Smart TV Privacy Risks and Protection Measures

Smart-TV Datenschutz- und Privatsphärenrisiken und Schutzmaßnahmen
Zur Erlangung des akademischen Grades Doktor-Ingenieur (Dr.-Ing.)
genehmigte Dissertation von Marco Ghiglieri, M.Sc. aus Hadamar
Tag der Einreichung: 28. Februar 2017, Tag der Prüfung: 25. April 2017
Mai 2017 — Darmstadt — D 17

1. Gutachten: Prof. Dr. Michael Waidner
2. Gutachten: Prof. Dr. Melanie Volkamer

TECHNISCHE
UNIVERSITÄT
DARMSTADT

Fachbereich Informatik
Fachgebiet
Sicherheit in der Informationstechnik

Smart TV Privacy Risks and Protection Measures
Smart-TV Datenschutz- und Privatsphärenrisiken und Schutzmaßnahmen

Genehmigte Dissertation von Marco Ghiglieri, M.Sc. aus Hadamar

1. Gutachten: Prof. Dr. Michael Waidner
2. Gutachten: Prof. Dr. Melanie Volkamer

Tag der Einreichung: 28. Februar 2017
Tag der Prüfung: 25. April 2017

Darmstadt — D 17

Erklärung zur Dissertation

Hiermit versichere ich, die vorliegende Dissertation ohne Hilfe Dritter nur mit den angegebenen Quellen und Hilfsmitteln angefertigt zu haben. Alle Stellen, die aus Quellen entnommen wurden, sind als solche kenntlich gemacht. Diese Arbeit hat in gleicher oder ähnlicher Form noch keiner Prüfungsbehörde vorgelegen.

Darmstadt, den 02. Mai 2017

(Marco Ghiglieri)

Danksagung

An erster Stelle danke ich meinem Doktorvater, Prof. Dr. Michael Waidner, der mir die Möglichkeit gegeben hat, in seinem Fachgebiet zu promovieren. Er hat mich bei meinem Vorhaben unterstützt und große Freiräume für das wissenschaftliche Arbeiten gewährt. Michael, vielen Dank für alles!

Ein großer Dank geht auch an meine Zweitbetreuerin, Prof. Dr. Melanie Volkamer, die mich im letzten Teil meiner Promotion mit voller Energie unterstützt hat. Die Gespräche und Diskussionen, trotz der manchmal weiten Entfernung, haben mich sehr weiter gebracht. Vielen Dank, Melanie!

Ich möchte mich recht herzlich bei den Mitgliedern meiner Prüfungskommission bedanken: Prof. Christian Bischof, Ph.D., Prof. Dr. Johannes Fürnkranz und Prof. Dr. Max Mühlhäuser.

Ein großes Dankeschön geht an Karina Köhres, Birgit Blume und Stefan Frey, die mich tatkräftig bei der Organisation unterstützt haben. Vielen Dank möchte ich auch Erik Tews, Golriz Chehrazi, Hervais Simo, Karen Renaud, Martin Stopczynski, Philipp Holzinger und Stefan Triller sagen.

Ein ganz großer Dank geht an Andrea Püchner und Christoph Krauß, die bei Problemen immer ein offenes Ohr für mich hatten. Es war mir eine große Freude mit euch zusammenzuarbeiten.

Ich danke meinen Eltern dafür, dass sie mir den Weg geebnet haben, diesen Karriereweg einzuschlagen und dass sie in jeder Situation meines Lebens rückhaltlos hinter mir standen. Ich bedanke mich auch bei meinen Schwiegereltern für die Kraft und Motivation, die sie mir gaben.

Ich entschuldige und bedanke mich zugleich bei meiner Tochter Kate, die oftmals durch diese Arbeit zu kurz kam. Vielen Dank geht auch an meine Schwester Tamara, die in schwierigen Zeiten immer für Kate und mich da war.

Meiner Ehefrau Jane möchte ich an dieser Stelle aus tiefstem Herzen danken. Es war eine lange und manchmal mühsame Zeit. Herzlichen Dank für die unermüdliche Unterstützung und die Kraft, die du mir jeden Tag gegeben hast, um diese Arbeit fertigzustellen.

Zusammenfassung

Die Verbreitung von Smart-TVs stieg in den letzten Jahren stetig an. Smart-TVs sind keine gänzlich neue Geräteklasse. Sie sind vielmehr eine Erweiterung der traditionellen Fernsehgeräte und bieten neben dem Empfang des Broadcastsignals zusätzlich die Möglichkeit, über das Internet zu kommunizieren. Durch die zusätzliche Internetverbindung werden verschiedene Internetfunktionen auf Smart-TVs möglich. Zum Beispiel sind dies Facebook, verschiedene Mediatheken sowie Online-Spiele. Einige Funktionen können die in vielen Smart-TVs eingebauten Mikrofone oder Kameras nutzen. Auch Web-Anwendungen, wie zum Beispiel Onlinebanking, können über die integrierten Web-Browser genutzt werden. Weiterhin unterstützen fast alle seit 2015 verkauften Smart-TVs die herstellerunabhängige Funktion HbbTV (Hybrid broadcast broadband TV). Diese Funktion ermöglicht es, Internetinhalte mit dem (traditionellen) Fernsehen zu verbinden. Sie ist standardmäßig aktiviert. HbbTV bietet dem Konsumenten programmabhängige Funktionen, wie beispielsweise die Anzeige von Live-Informationen aus dem Internet, angepasste Werbung, direkte Unterstützung beim Kauf von Teleshopping-Produkten oder auch senderabhängige Mediatheken.

Auf den ersten Blick erscheinen die Internetfunktionen eines Smart-TVs so, als würden sie nur Vorteile für die Konsumenten bieten. Allerdings bringt die Verbindung des Smart-TVs mit dem Internet, wie bei anderen internetfähigen Geräten auch, Gefahren mit sich. Smart-TVs können somit Ziel verschiedener Angriffe werden, die es ermöglichen auf das Smart-TV und auf dessen Daten unlegitimiert zuzugreifen. Forscher zeigten, dass es möglich war, über einen verwundbaren Mediaplayer im Smart-TV Zugriff auf das Smart-TV und dessen Mikrofon sowie Kamera zu bekommen.

Bei sensiblen Daten, wie zum Beispiel beim Onlinebanking, könnte es für Angreifer bereits wertvoll sein, die übertragenen Daten lesen zu können und sie dann zu manipulieren oder zu missbrauchen. Das Smart-TV sollte somit überprüfen, dass die Verbindungen so sicher sind, wie der Betreiber der Web-Anwendung es vorsieht. Wird die Überprüfung der Verbindung nicht oder nicht korrekt durchgeführt, sind die Daten der Konsumenten in Gefahr und es kann ein sozialer oder finanzieller Schaden für Konsumenten entstehen.

Sender und Hersteller haben ebenfalls Interesse daran, verschiedene Daten von Smart-TVs zu erhalten, die dafür genutzt werden können, um ein genaues Nutzungsprofil des Smart TVs zu erhalten. Dies kann für Produkt- oder Programmoptimierung sowie gezielte und personalisierte Werbung genutzt werden. Heutzutage beauftragen Sender Unternehmen wie die GfK, die mit Hochrechnungen aus repräsentativen Haushalten die Nutzerzahlen hochrechnen. Aus technischer Sicht ist die Erhebung dieser Nutzungsdaten auch direkt am Smart-TV mit Internetverbindung keine Herausforderung. Sender könnten die Daten mit HbbTV erheben und Hersteller könnten sie direkt von den Smart-TVs geschickt bekommen. Diese Daten würden deutlich genauere Informationen über den Konsumenten preisgeben. Beispielsweise wann und wieviel das Smart-TV genutzt wurde oder auch die Vorlieben bei der Programmwahl. Es kann dann eine Gefahr darstellen, wenn diese Daten in einem anderen Kontext oder zu einem anderen Zweck genutzt werden als der Konsument erwartet oder durch den Gesetzgeber erlaubt ist.

Die aufgezeigten Gefahren werden mit zunehmender Verbreitung von Smart-TVs wichtiger, da diese immer mehr Menschen betreffen. Das dreigeteilte Ziel dieser Thesis ist daher:

- Smart-TV bezogene Datenschutzgefahren zu identifizieren und diese zu verstehen,
- das Wissen und die Haltung der Konsumenten gegenüber Smart-TV bezogenen Privatsphäre- und Datenschutzgefahren zu erforschen,
- und Maßnahmen zur Sensibilisierung der Konsumenten sowie technische Schutzmaßnahmen für Smart-TV bezogene Privatsphäre- und Datenschutzgefahren zu entwickeln.

Im ersten Teilziel wurden in zwei umfangreichen Analysen erhebliche Datenschutzgefahren für Konsumenten aufgedeckt:

Wir entdecken in unseren *Analysen der HbbTV Funktionalität* ernstzunehmende Datenschutzgefahren für Konsumenten. In 2013 veröffentlichten wir als erste Publikation auf diesem Gebiet, dass Datenübertragungen vom Smart-TV zu verschiedenen Zielen im Internet bereits stattfanden, wenn ein Sender mit HbbTV-Unterstützung am Smart-TV eingeschaltet wurde. Dies alles, ohne dass der Konsument HbbTV aktiv nutzte, d.h. bevor er auf den *Red Button* seiner Fernbedienung drückte, um HbbTV zu nutzen. Die Ziele dieser Datenübertragungen waren unter anderem die Server der Sender und auch Diensteanbieter wie Google Analytics, die dafür bestimmt sind, Nutzungsdaten über den Konsumenten zu erheben. Die Nutzungsmöglichkeit dieser Daten reicht von Produktverbesserung zu personalisierter Werbung bis hin zu Überwachung durch Hacker, falls die Daten beim Sender in falsche Hände geraten. In dieser Veröffentlichung machten wir Empfehlungen zur Reduktion der Gefahren für Konsumenten. Diese wurden teilweise in den HbbTV Standard aufgenommen. Nach Vorstellung der Veröffentlichung folgte eine sehr hohe Medienwirksamkeit und es wurde in Radio, TV, Zeitschriften und Zeitungen davon berichtet. Um die technische Entwicklung von HbbTV weiter zu untersuchen, führten wir weitere Analysen im Jahr 2014 und 2015 durch, die 2014 und 2016 veröffentlicht wurden. Es wurden zusätzlich zu den TV-Sendern noch Radiosender, die über Satellit übertragen wurden, mit HbbTV Signal gefunden. Diese wiesen die gleichen Gefahren wie die TV-Sender in 2013 auf. Der Konsument müsste über diese Gefahren aufgeklärt werden, um es bei Unbelieben abzuschalten.

Weiterhin entdeckten wir in einer systematischen *Sicherheitsanalyse* von sieben Smart-TVs im Zeitraum von 2012 bis 2016, dass die Überprüfung von sicheren Verbindungen zu Web-Servern nicht korrekt durchgeführt wurde. Dies ist teilweise heute noch der Fall. Daten von sicheren Web-Anwendungen, wie zum Beispiel Onlinebanking, die auf dem Smart-TV aufgerufen wurden, konnten von Angreifern unbemerkt abgehört oder sogar manipuliert werden. Diese Schwachstelle wurde im Web-Browser und bei anderen Internetfunktionen wie zum Beispiel HbbTV des Smart-TVs nachgewiesen. In 2012 waren wir die ersten, die diese Schwachstellen aufdeckten und an den Hersteller meldeten. Erst in 2014 wurden diese schwerwiegenden Schwachstellen behoben. Einige Samsung Smart-TVs sind heute noch anfällig, da das Update bei diesen Modellen über USB geschieht und es keine Konsumenteninformation bisher gab.

Im nächsten Teilziel analysierten wir die Annahme, dass die meisten Konsumenten keine Kenntnis von Datenschutzgefahren sowie Schutzmaßnahmen bei Smart-TVs haben. Da zu diesem Thema noch keine Forschungsergebnisse veröffentlicht wurden, konzipierten und führten wir eine Umfrage mit 200 Teilnehmern durch. Nur ein geringer Anteil der Teilnehmer kannte Smart-TV spezifische Gefahren und Schutzmaßnahmen. Wir analysierten die Einstellung der Teilnehmer gegenüber Datenschutzgefahren genauer, indem wir ihnen Gefahren zeigten und sie baten, diese bezüglich wie kritisch sie diese sehen, zu bewerten und ihre Bewertung zu begründen. Aus diesen Begründungen leiteten wir verschiedene Faktoren, die ihre Haltung gegenüber den Gefahren sowie ihre Bewertung beeinflussten ab. Diese Faktoren waren wichtig, um gezielte Sensibilisierungsmaßnahmen zu entwickeln.

Im letzten Teilziel wurden Sensibilisierungsnachrichten und deren Auswirkung auf Konsumenten sowie technische Schutzmaßnahmen prototypisch entwickelt und evaluiert. Da auch für die von uns gesuchten Sensibilisierungsnachrichten sowie die technischen Schutzmaßnahmen für Smart-TVs keine Forschungsarbeiten existierten, gingen wir wie folgt vor:

Aus den ermittelten Faktoren wurden verschiedene Sensibilisierungsnachrichten in einer Vorstudie evaluiert. Das Ergebnis war, dass Sensibilisierungsnachrichten Schaden kommunizieren müssen, aber dieser darf nicht zu konkret sein (z.B. Hauseinbruch), da die Nachricht sonst als unglaubwürdig von den Teilnehmern eingestuft wird.

Zwei der evaluierten Nachrichten wurden in einer weiteren Studie mit 155 Teilnehmern untersucht. Wir konnten durch diese Nachrichten eine Sensibilisierung feststellen, dennoch stuften die meisten Teilnehmer die Internetfunktionalität ihres Smart-TVs wichtiger ein als den Schutz ihrer Daten.

Zusätzlich zu den beiden Sensibilisierungsnachrichten boten wir den Teilnehmern in einer weiteren Studie mit 169 Teilnehmern technische Schutzmaßnahmen an, die mit Kosten und/oder Zeitaufwand verbunden waren. Sensibiliserungsnachrichten und technische Schutzmaßnahmen, auch wenn sie Kosten oder einen erhöhten Zeitaufwand bedeuten, wurden von den Teilnehmern angenommen, sodass die meisten Teilnehmer sich für eine Schutzmaßnahme entschieden.

Basierend auf den Ergebnissen entwickelten wir die erste prototypisch implementierte Schutzsoftware, den *Smart TV Protector*, der die Daten des Konsumenten schützt und dabei möglichst alle Internetfunktionalitäten beibehält. Der *Smart TV Protector* ist das erste Schutzsystem speziell für Smart-TVs und kann dadurch Smart-TV spezifische Eigenheiten, wie zum Beispiel HbbTV, gesondert behandeln. Weiterhin stellen wir eine theoretische Erweiterung zum *Smart TV Protector* vor, die auch die Interessen von Herstellern und Sendern beachtet. Dieses Konzept kann, wenn alle Stakeholder die Idee umsetzen, für alle Parteien vorteilhaft sein, da die Datenqualität steigt und Hersteller sowie Sender weiterhin die benötigten Daten erhalten.

Abstract

Smart TVs have been becoming more popular in recent years. They are not entirely new devices, they are rather traditional TVs with current technology and increased functionality. In addition to streaming traditional broadcast content, Smart TVs facilitate access to Internet content and services. Thus, different Internet functionality on Smart TVs is available. For instance, Facebook, different video on demand services or online games. Some Internet functionality can access and utilize the integrated microphones and cameras. Smart TVs can also be used to browse on web applications that processes sensitive data such as online banking. Furthermore, the vendor independent functionality HbbTV (Hybrid broadcast broadband TV) has been available on almost all new Smart TVs that have been sold in Germany since 2015. This functionality combines the traditional broadcast content with Internet content. It is activated by default. Examples for the content are program-dependent functionality such as infotainment from the Internet, targeted advertisements, direct support for consumers while teleshopping and channel-dependent video on demand services.

At the first glance, the Internet functionality of Smart TVs appears to deliver distinct value, as compared to traditional TVs. However, Smart TVs are also, as known from other Internet enabled devices, exposed to different risks due to the Internet connectivity. They could be subject to different attacks that aim to access the Smart TV or the stored data unauthorized. Researchers have shown that it was possible to gain access to the Smart TV and its microphone over a vulnerable media player.

For hackers it could already be of value to read sensitive data for example from online banking in order to manipulate or misuse this data afterwards. Therefore, Smart TVs have to validate whether the connection is as secure as the web application provider intends. If the connection is not or not correctly validated, the consumer's data is under risk and it could cause social or financial losses for consumers.

Broadcasters and vendors are also interested in Smart TV data to establish usage profiles of Smart TVs. This usage data can be used to improve their products, program schedule or targeted advertisements. Nowadays, broadcasters acquire usage data from specialized companies such as GfK that extrapolate the viewing figures from a specific representative amount of households to the population. From a technical perspective, it is not a challenge for broadcasters to collect usage data directly from the Smart TVs using HbbTV. Vendors could get the data directly from the Smart TVs. This usage data would reveal more precise data of consumers. For example, when and how much is a Smart TV used and which channels consumers prefer. It could be a risk when the data is used in another context or purposes than expected by consumers or permitted by law.

The presented risks are becoming more and more important as the distribution of Smart TVs increases. Thus, our primary goal of this work was as follows:

- identify and understand Smart TV related privacy risks,
- research consumers' knowledge and attitudes of Smart TV related privacy risks,
- and develop a combination of appropriate awareness and technical protection measures.

We revealed severe privacy risks for consumers in two extensive analyses in the first aspect of the goal:

Severe privacy risks in the *HbbTV functionality analyses* for consumers were revealed. In 2013, we published, as the first paper in this area, that data transfers to different servers already started when a channel was selected that supported HbbTV. This happened without that the consumers actively used the HbbTV functionality, i.e., the data transfer started without pressing the *Red Button* on the remote control. The destinations of this data were among others the broadcasters and third parties like Google Analytics that are specialized to profile consumers. This data can be used to improve products, targeted

advertisement and hackers could steal the data from broadcasters in order to misuse them. In this publication we also recommended some countermeasures to reduce the risk for consumers. It was partly added in the HbbTV standard. Media and press immediately reported about our results. Afterwards, TV and interviews with different magazines were conducted. In order to analyze the evolution of HbbTV, we conducted further analyses in 2014 and 2015 and published the results in 2014 and 2016. In addition to the results in 2013, we found radio channels that supported HbbTV. Those had the same characteristics as the analyzed TV channels in 2012. The consumers must be aware of this risk to be able to disable HbbTV.

Moreover, in a systematical security analysis of seven Smart TVs in 2012 to 2016, we revealed that the validation of secure connections is not performed correctly. This issue still exists in some subsystems of the Smart TVs. Data of secure web applications, e.g. online banking, could have been eavesdropped or manipulated. This vulnerability was not limited to the web browser, but also other functionality (e.g. HbbTV) of the Smart TV was affected. In 2012 we, to the best of our knowledge, were the first researchers who revealed this vulnerability and communicated it to the vendor. It was patched in 2014. Some Samsung Smart TVs are still vulnerable since the update has to be performed over USB, but consumers have not been informed about that issue yet.

In the second aspect of the goal we analyzed the assumption that consumers are not aware of Smart TV related privacy risks as well as of countermeasures. We were, to the best of our knowledge, the first researchers that conducted a survey with 200 participants to research it. We explored that consumers are not aware of privacy risks or appropriate countermeasures. Only a small number of participants mentioned privacy risks or countermeasures. Additionally, we presented four different scenarios motivated by occurred privacy issues that should be rated by the participants. We asked them to justify the ratings. Based on these, we identified factors that potentially impacted the consumers' attitudes towards privacy risks and their ratings. This factors were essential to develop further awareness-raising messages.

In the last aspect of the goal we analyzed awareness and technical measures. To the best of our knowledge, we conducted the first research work that evaluated awareness-raising messages and technical protection measures for Smart TVs. We proceeded as follows: Based on the factors, we developed different awareness-raising messages that we evaluated in a pre-study. We concluded that privacy-related awareness could best be prompted by messages that avoid being too specific about a potential misuse. Being too specific (e.g. burglary) is likely to be judged as low risk as it is considered as too unlikely in this context.

Two of the evaluated messages were further evaluated in another study of 155 participants. The result was that most consumers would willingly sacrifice their privacy to benefit from Smart TV functionality. This analysis indicated that awareness-raising messages can increase awareness however messages alone do not show the desired effect on consumers.

Additionally, we combined the above mentioned awareness messages with feasible protection measures and evaluated them in a study with 169 participants. Our result is that consumers would spend time and/or money on protecting their privacy when the Smart TV's Internet functionality is retained.

Based on the previous results, we tailored a prototypical solution, the *Smart TV Protector*, which shows the feasibility of an appropriate technical protection measure. The *Smart TV Protector* is the first technical protection measure for Smart TVs.

Furthermore, we theoretically outlined an extension for the *Smart TV Protector* that respects broadcasters' and vendors' interests. We developed an approach that uses methods to keep the privacy protected while aiming to reach a high stakeholder acceptance. This approach is only feasible if all stakeholders accept the rules.

List of Publications and Press

Conferences and Workshops

M. Ghiglieri, M. Volkamer, and K. Renaud, "Exploring Consumers' Attitudes of Smart TV Related Privacy Risks," *Human Computer Interaction Conference 2017*, 2017, to be published (accepted).

M. Ghiglieri and M. Stopczynski, "SecLab: An Innovative Approach to Learn and Understand Current Security and Privacy Issues," in *Proceedings of the 17th Annual Conference on Information Technology Education*, ACM, 2016, pp. 67–72.

M. Ghiglieri, "PriMSED-Privacy-friendly measurement of Smart Entertainment Devices," in *Consumer Communications and Networking Conference (CCNC), 2015 12th Annual IEEE*, IEEE, 2015, pp. 65–70.

M. Ghiglieri and J. Müller, "Datenschutzfreundliche Erfassung von Nutzungsdaten bei Smart Entertainment Geräten," in *14. Deutscher IT-Sicherheitskongress*, Bundesamt für Sicherheit in der Informationstechnik, May 2015.

M. Ghiglieri and F. Oswald, "SSP – Ansatz zur garantierten Durchsetzung von Web Sicherheitsmaßnahmen auf dem Client," in *14. Deutscher IT-Sicherheitskongress*, Bundesamt für Sicherheit in der Informationstechnik, May 2015.

M. Ghiglieri, "I Know What You Watched Last Sunday – A New Survey Of Privacy In HbbTV," *Workshop Web 2.0 Security & Privacy 2014 in conjunction with the IEEE Symposium on Security and Privacy*, 2014.

M. Ghiglieri and E. Tews, "A Privacy Protection System for HbbTV in Smart TVs," in *Consumer Communications and Networking Conference (CCNC), 2014 IEEE 11th*, IEEE, 2014, pp. 357–362.

M. Ghiglieri, L. Kalabis, and D. Kelm, "Events Around Me - Ein datenschutzfreundlicher Veranstaltungskompass," in *13. Deutschen IT-Sicherheitskongress*, Best Student Award, Bundesamt für Sicherheit in der Informationstechnik, May 2013.

M. Ghiglieri, F. Oswald, and E. Tews, "HbbTV – I Know What You Are Watching," in *Informationssicherheit stärken – Vertrauen in die Zukunft schaffen*, Bundesamt für Sicherheit in der Informationstechnik, May 2013, pp. 225–238.

M. Stopczynski and M. Ghiglieri, "Smart Home Dashboard–Das intelligente Energiemanagement," in *VDE-Kongress 2012*, VDE VERLAG GmbH, 2012.

Journals and Magazines

M. Ghiglieri and M. Waidner, "HbbTV Security and Privacy: Issues and Challenges," *IEEE Security Privacy*, vol. 14, no. 3, pp. 61–67, May 2016, ISSN: 1540-7993. DOI: 10.1109/MSP.2016.54.

M. Ghiglieri and J. Fürnkranz, "Learning to recognize missing e-mail attachments," *Applied Artificial Intelligence*, vol. 24, no. 5, pp. 443–462, 2010. DOI: 10.1080/08839514.2010.481499. eprint: http://dx.doi.org/10.1080/08839514.2010.481499. [Online]. Available: http://dx.doi.org/10.1080/08839514.2010.481499.

Technical Reports and Other Publications

M. Ghiglieri, M. Hansen, M. Nebel, J. V. Pörschke, and H. S. Fhom, "Smart-TV und Privatheit - Bedrohungspotenziale und Handlungsmöglichkeiten," Forum Privatheit, Tech. Rep., Feb. 2016.

M. Ghiglieri, L. Benjamin, H. Simo, and M. Waidner, "Security und Privacy bei SmartTV: Bedrohungspotential und technische Lösungsansätze," *Digitale Schwellen - Privatheit und Freiheit in der digitalen Welt*, p. 67, 2015.

M. Ghiglieri, “HbbTV – aktueller Stand 2014,” Deutsch, in *FKT - Die Fachzeitschrift für Fernsehen, Film und elektronische Medien*, Schiele & Schön, Ed., vol. 11/2014, Nov. 2014.

M. Ghiglieri, “Incorrect HTTPS Certificate Validation in Samsung Smart TVs,” Technical Report, 2014.

M. Ghiglieri, F. Oswald, and E. Tews, “HbbTV: Neue Funktionen mit möglichen Nebenwirkungen,” Deutsch, in *FKT - Die Fachzeitschrift für Fernsehen, Film und elektronische Medien*, Schiele & Schön, Ed., vol. 10/2013, Oct. 2013, pp. 563–566.

Press and Media Coverage

Schwäbische Zeitung: ”Nutzer wissen nicht, was mit ihren Daten passiert”, 08.07.2016, *Zeitung*

NDR Service:Zuhause, Besser fernsehen - so geht’s!, 16.04.2016, *TV*

think ING. kompakt 03|2016 – Digitale Sicherheit, 03.2016, *Zeitschrift*

Westdeutsche Allgemeine Zeitung, Fernseher als Datenkrake, 30.10.2015, *Zeitung*

WDR service:zuhause, Schutz vor Datenklau im Fernsehen, 30.08.2015, *TV*

Netzpolitik.org, Der Smart-TV als Abhörwand, 19.06.2015, *Online-Nachrichten*

Frankfurter Allgemeine, Sieh einer an, der neue Fernseher spioniert uns aus, 17.06.2015, *Zeitung*

heute.de, IT-Sicherheit in Deutschland, Nur bedingt abwehrbereit, 10.04.2015, *Online-Zeitung*

mex, hr Fernsehen, 11.03.2015, *TV*

Nordbayerischer Kurier, Smart TV: Sie wissen, wer du bist und was du wann guckst, 15.02.2015 , *Zeitung*

VDI Nachrichten, Zähes Ringen um mehr Datenschutz bei Smart-TV, 05.09.2014, *Online-Nachrichten*

WDR Servicezeit, Datenschleuder Smart-TV, TV 18.03.2014, *TV*

Der Spiegel, Glotze glotzt zurück, 17.02.2014, *Zeitschrift*

hr info, Spion Smart-TV, 27.01.2014, *Radio*

WDR markt, Smarte ”Datenschleudern”, 20.01.2014, *TV*

Mannheimer Morgen, Fernseher späht Daten aus, 14.12.2013, *Zeitung*

Technology Review, Was guckst du ?, 12.2013, *Zeitschrift*

Hannoversche Allgemeine, Smart-TV unter Schnüffelverdacht, 22.11.2013, *Online-Nachrichten*

heise, HbbTV: Spion im Wohnzimmer 21.11.2013, *Online-Nachrichten*

Märkische Onlinezeitung/Augsburger Allgemeine, Smart-TVs von LG senden Daten über TV-Nutzung nach Südkorea, 21.11.2013, *Online-Nachrichten*

Frankfurter Rundschau, LG gesteht TV-Spionage, 21.11.2013, *Online-Nachrichten*

stern, Sie wissen, was du guckst, 11.07.2013, *Zeitschrift*

Deutschlandfunk, Manuskript: Fahndungsoffensive, 30.06.2013, *Online-Nachrichten*

hoch3 #4/2013 TU Darmstadt, Der Spion im Wohnzimmer, 26.06.2013, *Zeitschrift*

Spiegel Online, HbbTV: Smart TV: Ihr neuer Fernseher lässt sich hacken, 07.06.2013, *Online-Nachrichten*

tagesschau nachtmagazin, Der Spion im Wohnzimmer, 23.05.2013, *TV*

ARD Mittagsmagazin, Smart-TV: Spione im Wohnzimmer, 23.05.2013, *TV*

heise, TV-Sender könnten wissen, was Smart-TV-Besitzer schauen, 17.05.2013, *Online-Nachrichten*

Darmstädter Echo, Spione im Wohnzimmer, 16.05.2013, *Zeitung*

Echo-Online, Spione im Wohnzimmer, 16.05.2013, *Online-Nachrichten*

Contents

List of Figures

List of Tables

1 Introduction

The term *Smart TV* was first mentioned in 1990 by an article in the journal "Popular Science" [1]. About 15 years later, between 2005 and 2008, the first Smart TV was marketed. Literature has not agreed on a specific date yet, so different dates in these three years are mentioned [2, 3]. However, the latest date found publicly available is the first Smart TV manufactured by Samsung, which was introduced in 2008 [4]. In the following years, Smart TVs became more popular. The worldwide shipments of Smart TVs were rising from 52 million in 2011 [5] to 100 million units in 2015. Forecast Smart-TV shipments are 134 million by 2020 [6]. While the distribution of Smart TVs were increasing, many Smart TV related security and privacy risks were revealed in academia and media.

This chapter serves as an introduction in this thesis. After presenting the motivation in Section 1.1, we discuss the goal and the contributions of this work in Section 1.2. Finally, in Section 1.3 we present the outline.

1.1 Motivation

Smart TVs have been becoming more popular over the last years. They are not entirely new devices, they are rather traditional TVs with current technology and increased functionality. In addition to streaming traditional broadcast content, Smart TVs facilitate access to Internet content and services. These capabilities enable broadcasters and vendors to provide services such as real time information for the running TV program, video on demand, games, TV shopping and infotainment. Providing real time information to consumers has always been possible even with traditional TVs, but being able to provide customized information to a Smart TV over the Internet is new. The only exception here has been teletext, which could be used in a way that consumers can pick information they are interested in. Teletext is a way to transport text and other symbols over the broadcast channel to the TVs [7]. Smart TVs can also be used to browse on web application that processes sensitive data such as online banking. For this purpose it is essential that Smart TVs secure the data on the way to the servers properly. If not, the data can be eavesdropped and/or manipulated without consumer's notice.

The Smart TV vendors implement functionality to download and execute applications similar to smart phone apps (called apps) that extend the Smart TV functionality, e.g., Facebook, web browser, e-mail. The vendors' platforms, e.g. Samsung's SmartHub, are not standardized, i.e., these platforms and the applications differ from vendor to vendor and Smart TV to Smart TV. Some Smart TV applications are pre-installed by the vendors. Additionally, most vendors deliver Smart TV firmware and software updates over the Internet. Usually they are performed automatically over the Internet or manually over USB. Only a few vendors stick to a USB only update method.

Broadcasters have two options to deliver content to the Smart TVs. First, they provide an app that can be installed on the Smart TVs. Thus, the broadcasters must ensure that it is tested and usable on many different Smart TV models. Second, they bring content with Hybrid Broadcasting Broadband TV (HbbTV) to the consumers. HbbTV is a standardized technique that is implemented by most Smart TV vendors. In Germany, 97% of the Smart TVs sold in 2015 supported the HbbTV functionality [8]. It covers video on demand and information services for Smart TVs. Web technologies like HTML[1], CSS[2] and JavaScript are used for HbbTV. Technically, a web site with transparent background over the current channel is delivered to the Smart TVs. According to the Smart TV working group of the German TV-Platform [9], a worldwide usage of HbbTV is being contemplated. Thus, the topic is relevant for all countries that

[1] Hypertext Markup Language
[2] Cascading Style Sheets

already have or will introduce HbbTV. Europe has the highest coverage of HbbTV supported devices as of today.

According to the gfu Consumer & Home Electronics [10], 70% of the 18M Smart TVs in Germany are connected to the Internet in 2015. Only those Smart TVs which are connected to the Internet can use the provided Internet functionality. As widely known, if a device is connected to the Internet, it could be a target for attacks. For Smart TVs, criminals could try to break into the Smart TV in order to gain access to functionality and/or stored data. Thus, Smart TVs have to be tested thoroughly to identify security vulnerabilities before brought to the consumers.

Michéle *et al.* [11] showed that an outdated or unpatched media player is sufficient to gain access to any subsystem of the Smart TV. Indeed, in Metro [12], a newspaper, it was reported that a couple was recorded in an intimate situation by hackers. The recorded video was published. Thus, severe privacy consequences could be caused through security vulnerabilities in the implemented Smart TV functionality and protocols.

Broadcasters are interested in detailed viewing figures of their channels in order to optimize their content so that more consumers watch their channels. They can increase their revenues when selling time slots for advertisement, since the price is calculated through the viewing figures that state how many consumers watched a channel at a specific time. Nowadays, broadcasters acquire the data from companies such as GFK or Nielsen-Ratings. Since the Nielsen-Ratings and the GFK method are an extrapolation from a specific representative amount of households to the population, the viewing figures are often imprecise [13]. A Smart TV functionality that can be used to gather viewing figures by broadcasters is HbbTV. It is enabled by default on most Smart TVs and starts to load data before the consumer actively requested to use HbbTV by pressing the *Red Button*. Due to these background activities, it is likely that most consumers are not aware of this functionality and its side effects.

Vendors are also interested in detailed viewing figures and usage data of sold Smart TVs. This usage data could support the vendors to identify issues and improve their products effectively. But, the data for vendors is not collected with the traditional audience measurement methods. Vendors can gather the usage data directly over the Smart TVs. If the collected data is passed on by vendors or broadcasters to advertisement companies, those companies could use the usage data to tailor better advertisements in order to improve their revenues. Therefore, precise viewing figures and consumers' usage data are valuable for broadcasters and vendors as well.

However, both, the vendors and broadcasters, should inform consumers about the collection of usage data, the purpose they use the data and the data collection should be compliant to data policy rights. According to the German Bundesdatenschutzgesetz a data collection without consumer consent is not permitted. Long privacy policies, which states that vendors transfer data, have to be accepted when the Smart TV is installed the first time. However, even if consumers have accepted these privacy policies, they do not expect an extensive data transfer while watching traditional TV since they are used that this functionality works without Internet. Thus, it is likely that consumers do not see the need to protect themselves.

Therefore, this research project is important to develop effective protection and awareness measures for Smart TV consumers that are not used to privacy risks and those caused by security vulnerabilities. They should have a chance to take informed decision whether to use a Smart TV with all risks coming from the technology before taking severe financial or social consequences.

1.2 Goal and Contributions

In this section, we describe our goal, the challenges and contributions of this work. Based on the motivation and the Smart TV related risks the overall goal of this work was to

- identify and understand Smart TV related privacy risks,
- research consumers' awareness and attitudes towards Smart TV related privacy risks,
- and develop a combination of appropriate awareness and technical protection measures.

To reach this goal, we identified several challenges that have to be addressed. In the remainder of this section, we explain these challenges for the above mentioned goal's aspects and how we solved them as well as our contributions.

Identify and understand Smart TV related privacy risks. At the beginning of our research in 2012, we were, to the best of our knowledge, the first researchers who were analyzing Smart TVs in regards to consumer' privacy. We were only aware of one publication (see Mulliner *et al.*[14]) in the field of Smart TV security. Thus, no systematic method to analyze Smart TVs' privacy risks were available. The information we found about different attack vectors for Smart TVs were limited. Therefore, we did many analyses and much research before we could start to deepen our analysis in the following fields:

- We analyzed the Hybrid Broadband Broadcast (HbbTV) functionality regarding the following three aspects: (1) How much and which kind of data is sent to broadcasters and/or vendors? (2) Which information is provided to consumers before the Smart TV starts sending HbbTV data? (3) Which privacy risks emerge for consumers?
- We analyzed different Smart TVs regarding the following aspects: (1) Which security vulnerabilities that causes privacy risks can be identified in Smart TVs? (2) Which privacy risks emerge for consumers?

Our academic and social contributions are as follows:

- We identified privacy risks in the Smart TV functionality Hybrid Broadcast Broadband TV (HbbTV) for which the broadcasters are responsible. Our work [15] was cited by many TV news, newspapers and magazines. We were asked to give TV and radio interviews and write articles for several highly relevant print magazines for TV professionals. Those activities raised the interest of data policy officers, e.g. from the Bayerischen Landesamt für Datenschutzaufsicht (BayLDA). We were invited to meetings to discuss this issue, e.g. Landesanstalt für Medien Nordrhein-Westfalen (LfM).
- We published the first academic paper about privacy in HbbTV [15] in 2012 and further analyses results in 2014 [16, 17] and 2016 [18]. In 2014 and 2016 we observed that HbbTV is also deployed on satellite radio channels. Furthermore, we published articles in magazines [19, 20] and a technical report [21].
- We recommended different countermeasures in [15]. Parts of our recommendations and many other information about privacy risks and how to avoid them have been integrated in the HbbTV standard 2.0 [22].
- We identified severe security vulnerabilities that causes privacy risks in the implementation of the HTTPS certificate validation processes in Samsung Smart TVs in 2012 [23]. It was possible to manipulate secured connections. Some Smart TVs have been patched in 2014 and others are still vulnerable since the update has to be performed over USB manually, which is not likely if consumers have not been made aware of the issue. In 2016, we again identified security vulnerabilities

causing privacy risks in HTTPS validation processes of Samsung and LG Smart TVs [24]. It is likely that other vendors' Smart TVs are also affected.

The outcome clearly states that there is a need for appropriate protection measures. In order to research whether consumers see also a need for these measures, we evaluated whether Smart TV consumers are aware of Smart TV related privacy risks as well as countermeasures.

Research consumers' awareness and attitudes towards Smart TV related privacy risk. We assumed that consumers are not aware of these risks and thus cannot take informed decisions whether to connect the Smart TV to the Internet or deploy appropriate countermeasures for protecting against privacy risks. The challenge was to clarify our assumption and to get insights in consumers' attitudes and therefore help us to develop appropriate countermeasures. We were, to the best of our knowledge, the first who researched the consumers' attitudes towards Smart TV related privacy risks. We carried out the following research:

- We conducted a survey that explored whether consumers are aware of Smart TV related privacy risks and proper protection measures. Additionally, we presented four different scenarios motivated by occurred privacy issues that should be rated in terms of criticality by the participants. We asked the participants to justify their ratings as free text responses. From these responses we derived factors that influenced participants' attitudes and ratings.

Our contributions are as follows:

- We explored that consumers were not aware of potential privacy risks or appropriate countermeasures. Only a small number of participants mentioned privacy risks. Also countermeasures were rarely mentioned by participants.
- Based on the participants' free text justifications, we identified the following factors that potentially impacted the attitudes towards privacy risks: the party who gathers the data; the type of data; awareness of the fact that (usage) data is collected; being aware that collected data can be misused; personalized advertising being considered beneficial, or not; basic attitudes. These contributions are very valuable to develop awareness messages that make consumers aware of Smart TV related privacy risks.
- We have published these contributions in [25].

Based on these results, we developed awareness-raising messages that are evaluated in the next challenge of this work.

Develop a combination of appropriate awareness and technical protection measures. Both awareness and technical protection measures for Smart TVs were not widely available. Obviously, it is always possible to disconnect the Smart TV. But, all Smart TV's Internet functionality would be lost. We assumed that functionality is one of the reasons consumers buy a Smart TV so a solution without technical protection measures would not be accepted by consumers. First, we researched whether awareness-raising messages that make Smart TV consumers aware of privacy risks are sufficient for most consumers to disconnect their Smart TV from the Internet to protect their privacy. To the best of our knowledge, we conducted the first research that evaluated awareness-raising messages for Smart TV related privacy risks. We carried out this research in three steps that we published in [25]:

- First, in a pre-study we tested a range of messages covering a combination of different influential factors isolated in the last challenge. Some included concrete consequences other were more high level; some referred to hackers, others to vendors and broadcasters.

  We concluded that privacy related awareness could best be prompted by messages that avoid being too specific about a potential misuse. Being too specific (e.g. burglary) is likely to be judged as low

risk as it is considered as too unlikely in this context. Consumers need to be able to visualize the particular scenario and believe that it could happen, i.e. it is realistic.

- Second, based on the observation in the pre-study we tailored two awareness-raising messages for privacy risks. Then, we presented them to consumers and analyzed whether consumers would reconsider their decision to connect or disconnect their Smart TV. We did not offer further options to protect their privacy.

  Our contribution is the result that most consumers would willingly sacrifice their privacy to benefit from Smart TV functionality, since they would not disconnect their Smart TVs when made aware of privacy risks. The results of this study indicated that awareness messages alone do not show the desired effect on consumers. However, we could show that if awareness messages are deployed, it is essential to communicate consequences, e.g. harm.

- Third, we combined these two awareness messages from the second step with three additional technical protection measures to protect privacy while retaining the Internet functionality and analyzed whether it increased the effect that consumers reconsider how they connect their Smart TVs to the Internet. In the same study we determined whether consumers would willingly spend time and/or money for these technical protection measures.

  Our result is that consumers would spend time and/or money on protecting their privacy when the Smart TV retains the Internet functionality.

We identified in the previous research steps that a combination of awareness and technical protection measures are essential in order to protect consumers' privacy. Most of the participants would not disconnect their Smart TV and select a technical protection when made aware of the privacy risks. Thus, we did the following research:

- We tailored a prototypical technical solution, the *Smart TV Protector*, which protects consumers against Smart TV related privacy risks. We implemented two approaches: (1) the *Smart TV Protector* blocks and filters the network traffic that causes privacy risks and (2) the *Smart TV Protector* provides information for consumers to configure their Smart TVs more privacy protecting.

- We outlined a theoretical extension of the *Smart TV Protector* that respects broadcasters' and vendors' interests. We developed an approach that uses methods to keep the privacy protected in order to reach a high stakeholder acceptance. However, this approach is only feasible if all stakeholders accept the rules.

Our contributions are as follows:

- The *Smart TV Protector* is the first technical protection measure for Smart TVs that is based on our research about Smart TV related privacy risks and consumers' attitudes. We published the *HbbTV Privacy Protector* in [16, 17]. It is integrated in the *Smart TV Protector* and greatly extends its capabilities.

- The *Privacy Protecting Collector* is an extension for the *Smart TV Protector* that could help to satisfy the needs of all stakeholders. We published it in a more general version for smart entertainment devices (including Smart TVs and others) in [26, 27].

1.3 Outline

This thesis is structured in 11 chapters. Chapter 2 serves as an introduction to HbbTV. This chapter is not necessary to follow the story line. Our contributions are discussed in Chapter 3 to Chapter 10. Chapter 11 summarizes the most important contributions of this work and discusses further research challenges.

Our contribution chapters are as follows:

We present our HbbTV analyses in Chapter 3. We analyzed over 122 TV channels including 58 radio channels in over three years analysis time. We showed that HbbTV sent data to the broadcasters without consumer's consent. We further analyzed each channel and evaluated the privacy risks, which differed in the amount of data and the sent content. Privacy statements from broadcasters could not be found. Moreover, we describe in detail how HbbTV can reveal consumer's behavior in an encrypted Wi-Fi network.

In Chapter 4, we discuss our result that the HTTPS certificate validation on Samsung and LG Smart TVs were vulnerable for different attacks. That could cause different privacy risks: (1) Illegitimate people were able to eavesdrop private data, (2) criminals could manipulate data, (3) criminals could manipulate Smart TV's firmware in order to harm the consumers, e.g. enable the microphone unnoticed. Further, we present our result that a firmware on a LG Smart TV could be downgraded to a vulnerable version.

In Chapter 5, we present our research whether consumers are aware of Smart TV related privacy risks and countermeasures. Further, we wanted to understand consumers' attitudes towards these privacy risks. At the end of this section, we deduced factors that influenced consumers' attitudes towards different privacy risks.

In Chapter 6, we discuss how we developed awareness-raising messages and evaluated whether they can be used for raising consumers' awareness. We isolated two messages that are used in the next chapter.

In Chapter 7, we show our evaluation whether consumer's intention to not connect their Smart TV to the Internet can be influenced by making them aware that usage data is collected and analyzed. We researched whether this influence can be strengthened when making them aware that the collected and analyzed data could potentially be misused to cause harm if accessed by criminals.

In Chapter 8, we present our research about the evaluation to which extend consumers who are aware of the privacy risks and the potential harm are willing to spend time and/or money on protecting their privacy when retaining the Internet functionality.

In Chapter 9 we present the *Smart TV Protector*, which protects consumers against Smart TV related privacy risks.

A discussion of a trade-off solution between privacy and interests of all stakeholders (broadcasters, vendors and consumers) can be found in Chapter 10. We propose a solution that prevents privacy risks but can share usage data in a privacy protecting way.

2 Introduction to Hybrid Broadcast Broadband TV (HbbTV)

The HbbTV standard is developed by the HbbTV association. It is a global initiative with the aim to harmonize the broadcast and broadband delivery of entertainment to the end consumer through Smart TVs and other set-top boxes [28]. The broadcasters are responsible for the content. HbbTV is vendor-independent and supported by most Smart TVs.

This chapter serves as an introduction to HbbTV and is not necessary to understand the contribution of this work. We introduce the HbbTV 1.5, 2.0 and 2.0.1 standard in Section 2.1. In Section 2.2, we present the HbbTV appearance for consumers and show the typical lifecycle of an HbbTV application.

2.1 HbbTV Standard

The European Telecommunications Standards Institute (ETSI) approved the HbbTV 1.5 standard in November 2012 [29]. The standard specifies the technical framework for HbbTV applications and how the HbbTV components should be implemented in Smart TVs and set-top boxes. The technical requirement for presenting and executing HbbTV applications on a Smart TV is a customized web browser (HbbTV browser) which supports HTML, CSS and JavaScript. The HbbTV browser presents its content as an overlay over the regular TV program. It remains invisible for consumers until a trigger (e.g. an URL) is received by the HbbTV browser through the DVB[1] stream. A customized JavaScript interpreter in the Smart TV can perform action on the Smart TV itself, e.g. changing the visibility of the HbbTV browser. If the content that is available under the URL includes such a JavaScript command to show the HTML content, the Smart TV will overlay the regular TV program. Two different methods of delivering the HbbTV data to the HbbTV browser are available:

1. **Entire HbbTV application through DVB.** Any HbbTV content is delivered over the DVB stream and no Internet access is required.

2. **URL in the DVB stream to an HbbTV application.** An URL to an Internet resource is provided and the HbbTV browser automatically loads the HbbTV content from the Internet. It is required that the Smart TV is connected to the Internet.

The selection of either of one of the above mentioned delivery methods limits the level of interactivity the HbbTV application can provide, i.e., HbbTV applications delivered entirely by DVB cannot be personalized individually for each Smart TV, since the same DVB stream is broadcast to all devices. Combinations of both methods are feasible. As soon as the HbbTV notification, which indicates that a HbbTV application is ready to be used, is shown, the consumer can interact with the HbbTV application by pressing the *Red Button* on the TV remote control (see Figure 2.1).

The HbbTV 2.0 standard was approved in October 2015 by ETSI [22] and includes some new features and a chapter about consumers' privacy. It now includes tracking preference expression (DNT)[2], managing third party cookies, blocking tracking websites, managing persistent storage (cookies, web storage) and a short section of "Respecting Privacy in Applications". The "Do Not Track" specification explains which technical implementation the Smart TV should provide in order to enable HbbTV applications to

[1] Digital Video Broadcast - The DVB project is an Alliance of many companies worldwide. It defines specifications for digital media delivery [30]. In this context, a DVB stream is a data stream that transports radio or TV signals via satellite (DVB-S), cable (DVB-C) or terrestrial (DVB-T) to the end devices.

[2] `https://www.w3.org/TR/2014/WD-tracking-dnt-20140424/`

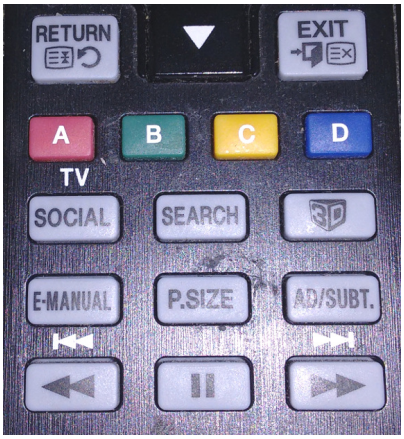


Figure 2.1.: Red button on Samsung's remote control.

respect consumers' preferences. Smart TVs may block all third party cookies or if possible give the consumer an option to enable or disable them. The Smart TV vendor is responsible for the blocking mechanism of tracking services. The section about respecting privacy in applications state that three options exists for protecting consumer's privacy: (1) delivering application via DVB, (2) using TLS to encrypt exchanged data and (3) use of cookies to record consumer's consent. They also mention that tracking before the consumer uses the HbbTV functionality may be illegal.

Further, the standard includes support for synchronization of content between different screens. In particular, it adds support for communication between other devices like smart phones or tablets. HbbTV applications can ask for an application to be launched on a mobile device and vice versa. The synchronization of different devices is specified. Support for delivering files containing audio and video content to connected storages for later consumption has been added. First devices with HbbTV 2.0 support should be available since 2016.

The newest not yet ETSI approved HbbTV standard is version 2.0.1 [31] with an additional section in the privacy chapter about the unique device ID that can identify a device. The unique device ID should be provided by default. But, consumers should be able to disable it and if necessary generate a new one. Some minor errors in HbbTV 2.0 were corrected.

2.2 HbbTV for the Consumer

The HbbTV applications differ from channel to channel. For one broadcaster it is only a replacement for teletext, for another it is a portal to deliver a variety of additional services such as media libraries or the possibility to watch previous content. The broadcasters are in all cases responsible for the content they provide via HbbTV.

Figure 2.2 outlines the typical lifecycle of an HbbTV application that is presented to consumers. First, the regular TV program is provided via DVB (1). After a short period of time the HbbTV notification is shown on the Smart TV screen (2). The HbbTV notification (called prompt in the specification) notifies the consumer that an HbbTV application is ready to be started by the consumer. Usually, it can be started by pressing the *Red Button* on the remote control of the Smart TV. If the *Red Button* is pressed, the HbbTV application can start in full screen mode (3). That is one possible way to start an HbbTV application. Different other possibilities are mentioned in the HbbTV specification:

- A digital teletext application can be started by pressing the TEXT button on the remote control.
- A broadcast-independent application can be started through the TV platform.

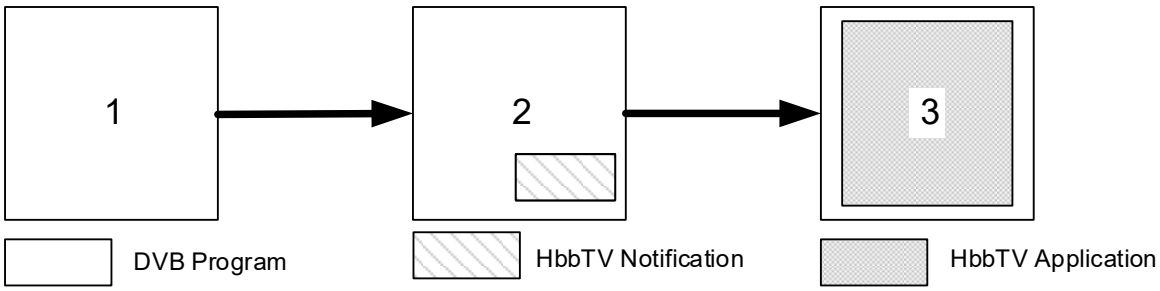


Figure 2.2.: Lifecycle of an HbbTV application presented to the consumer.

- Another device starts an HbbTV application (called companion screen in the HbbTV specification).
- Another running application links to an HbbTV application.
- Autostart applications start in full-screen mode.

The HbbTV notifications can differ depending on the channel. Examples are depicted in Figure 2.3.

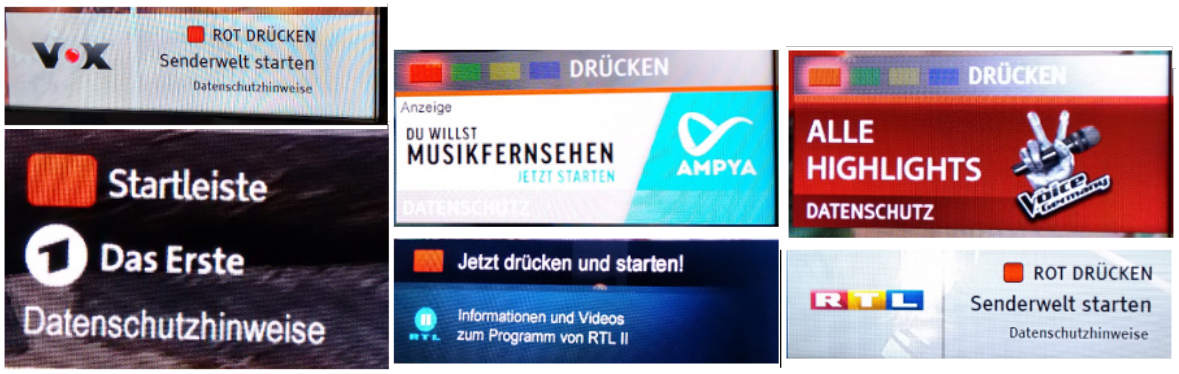


Figure 2.3.: Examples of HbbTV notifications from 2016.

We focus in this work on those HbbTV applications that are broadcast-dependent and either be starting automatically or started by pressing the *Red Button*.

3 Privacy Risks of Hybrid Broadcast Broadband TV

HbbTV is a standardized technique that is implemented in almost all Smart TVs [8]. It provides similar functionality as known from the traditional teletext, but the data is mostly transferred over the Internet.

In this chapter, we present our HbbTV analyses where we analyzed over 122 channels including TV and radio channels. First, we explain the attacker model in Section 3.1 for HbbTV. Then, we describe our methodology used to perform the HbbTV analyses in Section 3.2. The results of the analyses are reported in Section 3.3. We describe an attack on HbbTV that we discovered that helps criminals only receiving an encrypted Wi-Fi signal to profile consumers in Section 3.4. We list related work in Section 3.5. In Section 3.6, we discuss and summarize our results. Further background information about HbbTV can be found in Chapter 2. We published parts of this chapter in [15–18].

3.1 Attacker Model

We describe the attacker model for the Hybrid Broadcast Broadband TV analyses, which we focus on in this chapter. Figure 3.1 outlines the model. The Smart TV is connected to the Internet over a router with LAN or Wi-Fi. Over this infrastructure the broadcaster (service provider) communicates with the Smart TV over the Internet (WAN). The broadcaster provides the HbbTV content to the Smart TV and can collect usage data over HbbTV. The broadcaster has no access to local data and cannot manipulate any data.

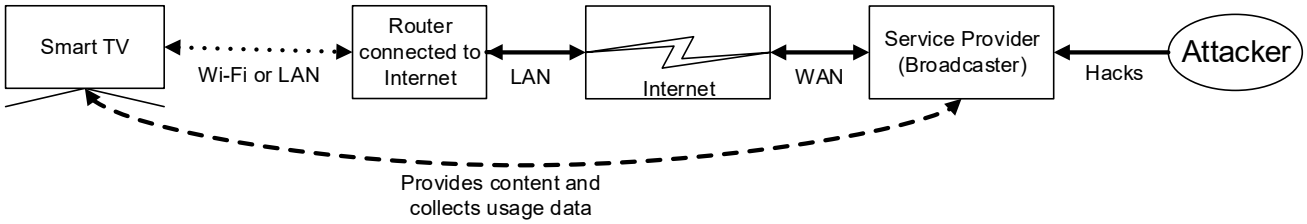


Figure 3.1.: Attacker model for HbbTV.

The broadcaster could analyze the usage data and improve their channels or increase the revenue, i.e., it could generate profiles for each Smart TV. If additionally an attacker gains access to the stored usage data at the broadcaster, the data could be stolen and misused.

3.2 Methodology

In this section, we explain the used methodology in order to analyze the HbbTV traffic for privacy risks systematically.

We set up a test environment that could monitor all traffic between a Smart TV and the Internet. The test environment is outlined in Figure 3.2.

The Smart TV was connected to a broadcast signal (satellite, cable or terrestrial) and an analyzing computer. The computer was connected to the router which was Internet connected. The Smart TV communicated with the broadcasters over the Internet (WAN). This test environment enabled the computer to monitor all traffic from and to the Smart TV. Based on that environment, we describe in detail how we analyzed HbbTV, which hardware and software we used for the analyses and how the Smart TV and the

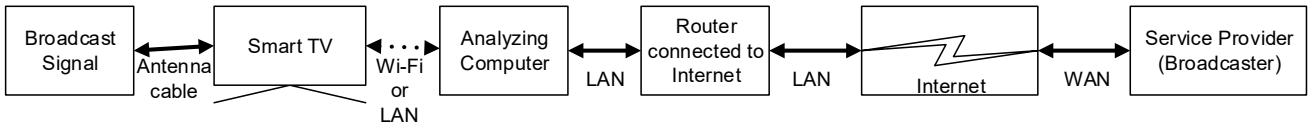


Figure 3.2.: Test environment for the HbbTV analyses.

radio environment were set up. Table 3.1 summarizes the details.

Hardware and software	Standard hardware / Linux, Wireshark
Broadcast signal reception	DVB-S, DVB-C, DVB-T
Tested scenarios	Smart TV, Digital Satellite Radio
Tested Smart TVs	Samsung (UE40D6200, UE40ES6300, UE40JU6580), LG (42LN5758, 47LB650V,32LF6309)
Tested Set-up Box	Invento Scena 6m IDL6651N

Table 3.1.: Overview of the test environment

Hardware and software for the analyzing computer. We used standard hardware for capturing packets between the Internet and the Smart TV, e.g., a laptop and a Wi-Fi router. The software Wireshark[1] on Linux and standard packet routing (iptables) that are integrated in Linux, were used. We captured the data without transport encryption, i.e. the analyzing computer could capture all traffic in plaintext.

Broadcast signal reception. The traffic of the HbbTV channels was captured with different broadcasting methods: satellite (DVB-S), terrestrial (DVB-T) and cable (DVB-C). The position of the satellite was Astra 19.2E and the terrestrial and cable signals were received in the Frankfurt Rhine-Main region of Germany.

Next, we present the test setup for our analyses of HbbTV on Smart TVs and set-top boxes for radio reception.
Smart TV test setup. The Smart TV test setup consisted of three components: the Smart TV, Internet connection via home network and a DVB signal coming from different sources (DVB-S, DVB-T or DVB-C). As shown in Figure 3.3 the DVB signal was received by satellite or terrestrial and was connected to the built-in receiver of the Smart TV. The Smart TV was connected to the Internet and the home network via LAN or Wi-Fi. We had three Samsung Smart TV models (UE40D6200, UE40ES6300, UE40JU6580) and three LG Smart TV models (42LN5758, 47LB650V and 32LF6309) that we analyzed.

Digital satellite radio test setup. The digital satellite radio setup had four components (see Figure 3.4): a set-top box with Internet connection, DVB satellite signal, connection to a Hi-Fi system. The set-top box was connected to the satellite and had a connection to the Internet and the home network. The Hi-Fi system got its audio signal over a direct cable connection to the set-top box. The set-top box could have been additionally connected to a (conventional) TV, which was however not relevant for our configuration. The digital radio signal with HbbTV was only transmitted by DVB-S. Thus, other broadcasting methods have not been analyzed. We used a set-top box from Invento model Scena 6n IDL6651N.

Analysis methodology. The analyses were performed in three steps:

1. **Pre-Analysis.** The pre-analysis provided a rough draft how HbbTV is designed and how it transfers data from the broadcasters' servers to the Smart TVs. We report the results in Section 3.2.1.

[1] `http://www.wireshark.org/`

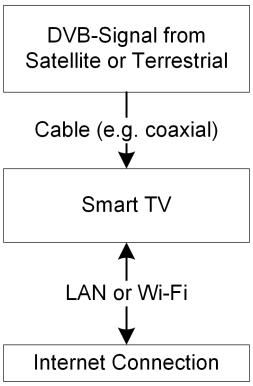


Figure 3.3.: Smart TV configuration

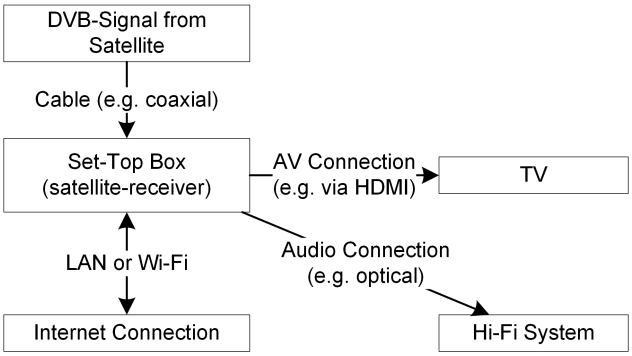


Figure 3.4.: Set-top box configuration

2. **Identify analysis characteristics.** Based on the last step, we extracted characteristics which can be used for systematical analysis of HbbTV channels. This characteristics are grouped in privacy risk groups according to the potential privacy risks in Section 3.2.2.

3. **Privacy risk analyses.** In Section 3.3, HbbTV channels are analyzed according to the identified characteristics. They are assigned to one of the privacy risk groups introduced in the second step.

3.2.1 Pre-Analysis Results

With the described methodology we observed the behavior of the Smart TVs and the produced network traffic. We filtered network traffic that were produced by HbbTV[2]. We divided the time where HbbTV packets are exchanged in different time phases (see Figure 3.5):
Phase 1: Time between switching to a channel and the HbbTV notification is shown,
Phase 2: Time between displaying the HbbTV notification and when the *Red Button* is pressed by the consumer and
Phase 3: Executing the HbbTV application after pressing the *Red Button*.

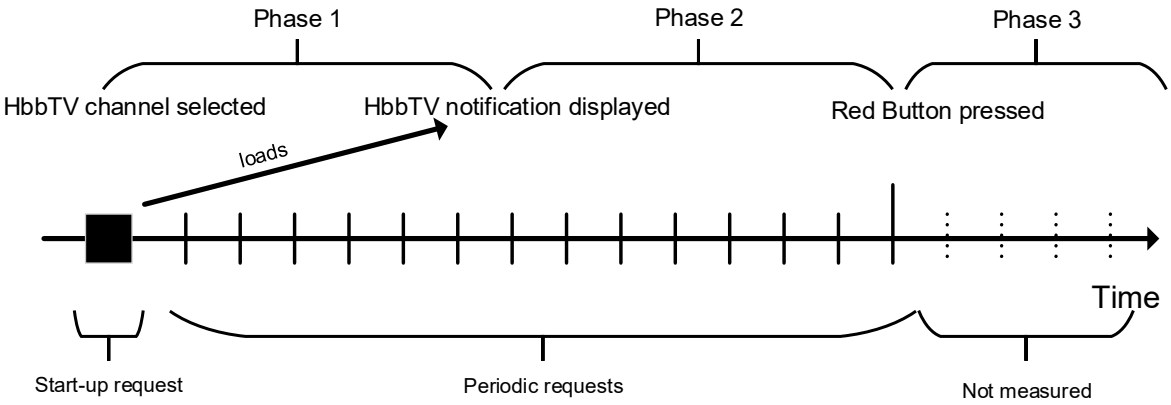


Figure 3.5.: HbbTV traffic flow.

Two different HbbTV traffic behaviors were detected. We spotted HbbTV channels that transferred data in phase 1, but not in phase 2. On some channels data transfer were measured in phase 1 and periodically in phase 2. All data transfers were performed between the Smart TV and the broadcasters. In both behaviors, we did not observed any data transfer between HbbTV channel and vendor.

[2] Our analysis of Smart TV related traffic can be found in Chapter 4.

The measured behavior of HbbTV in three phases will be the basis for the further analysis steps. We found different requests in the phases that we call characteristics and are explained in Section 3.2.2. Note, all results focus on phases 1 and 2, in which the consumer did not intentionally activate the HbbTV application, i.e., the consumer did not press the *Red Button*. Phase 3 was out-of-scope and therefore not measured.

3.2.2 Identified HbbTV Characteristics

From the pre-analysis results, characteristics were extracted that can be used to group channels with similar characteristics. The extraction process of characteristics was basically split in two steps: (1) Saving a capture of the network traffic of about 120 seconds and (2) analyzing the capture by manually check the requests and responses. The identified characteristics are listed below:

HbbTV application. We consider a channel provides an HbbTV application, if we gathered data while on a channel and a notification has been shown to the consumer. If the notification has not been shown and data has been collected, we further analyzed this behavior in order to find the purpose of the data transfer. If no HbbTV application was available, no URL in the DVB stream was provided and no further action was performed by the Smart TV. In the remainder of this work, we call a channel that provides an HbbTV application an HbbTV channel.

Start-up request. When switching to an HbbTV channel (Phase 1), the broadcaster has provided a URL within the DVB stream to load the first HbbTV notification showing that an HbbTV application was available (see Figure 3.5). In background, a variety of scripts, images and other resources were loaded. We call the first requests that loads the mentioned resources a *start-up request*.

Periodic requests. In addition to the start-up requests, we measured on some[3] channels periodic requests after the HbbTV notification has been displayed (Phase 2). The time between each request differed from one to 15 minutes depending on the channel. These requests were made before the consumer actively started the HbbTV application by pressing the *Red Button* (Phase 3). Thus, we assumed that consumers were not aware of these background transfers. Figure 3.5 shows the relation between start-up requests, periodic requests and the phases on a time line.

Data transferred to third parties. We considered all data transfers that were not sent to the broadcaster's server as third parties. If the broadcaster used a data center for its services, we did not consider that as third party.

Counting pixel. A counting pixel is a request of an image or other resource that is used to count visitors and page impressions of a web site. In HbbTV, it can be used to count the consumers on a specific channel. If a counting pixel is only used for counting the start time of an HbbTV channel, periodic requests are not needed. If the counting pixel should be used to measure the time a consumer is on a channel, periodic requests are performed.

Tracking. Tracking mechanisms are deployed to collect consumers' usage data to get a more accurate profile. Tracking mechanisms are more complex than counting pixels. They are usually deployed in scripts that can collect a variety of information, e.g. detect display resolution, measure time without periodic requests.

[3] More details can be found in Section 3.3.

Personalized advertisement. The HbbTV notification for the consumers can be modified by broadcasters so that it delivers personalized advertisement.

Cookies. Cookies can be set on Smart TVs as well as on other devices with web browsers. They can store different values on a Smart TV, e.g., identification numbers, login information. We did not consider them in the following channel grouping since it can be deployed for different reasons and therefore not be adduced for a risk assessment.

Characteristics/Group	Low Privacy Risk w/o HbbTV	Low Privacy Risk	Moderate Privacy Risk w/o HbbTV	Moderate Privacy Risk	High Privacy Risk w/o HbbTV	High Privacy Risk	Severe Privacy Risk	Not Available
HbbTV Application	-	x	-	x	-	x	x	x
Start-Up Request	x	x	x	x	x	x	x	x
Periodic Requests	-	-	-	-	x	x	(x)	?
Counting Pixel	-	-	x	x	x	x	x	?
Tracking	-	-	x	-	-	(x)	x	?
Data transferred to third parties	-	-	-	-	-	-	(x)	?
Personalized Advertisement	-	-	-	-	-	-	(x)	?

Table 3.2.: Assigned characteristics to each group

Legend: - not included, + included, (+) sometimes included, ? not known

In order to structure the analysis results we grouped the seven characteristics in five groups: *Low Privacy Risk*, *Moderate Privacy Risk*, *High Privacy Risk*, *Severe Privacy Risk* and *Not Available*. Table 3.2 shows the assignment from characteristics to groups. We decided for group names that directly indicate the potential privacy risk for consumers; *w/o HbbTV* denotes that a start-up request was measured but no HbbTV application was available. Cookies were not listed since they can be used for both, privacy protecting methods and increasing the potential privacy risk. We discuss them in more detail in the results section.

We explain the groups and how we grouped the characteristics in more detail:
Group Low Privacy Risk w/o HbbTV: Channels in this group performed a start-up request. However, no HbbTV application could be measured.
Group Low Privacy Risk: Channels performed a start-up request and an HbbTV application was delivered. Channels in both Low Privacy Risk (w/o HbbTV) groups have the lowest privacy risks since they only transferred necessary data needed for HbbTV.

Group Moderate Privacy Risk w/o HbbTV: Channels in this group performed a start-up request. Instead of an HbbTV application, we measured counting pixels and tracking scripts that were delivered from the broadcasters.
Group Moderate Privacy Risk: Channels in this group sent an HbbTV application where different counting pixels were embedded.

In the *Moderate Privacy Risk* groups the privacy risk is higher compared to the group *Low Privacy Risk* since broadcasters deploy methods to measure consumers' behavior on a channel.

Group High Privacy Risk w/o HbbTV: Channels in this group performed a start-up request. No HbbTV application could be measured. But, periodic requests to the broadcasters' servers were found.
Group High Privacy Risk: Channels assigned to this group sent periodic requests in a rate of one second to 15 minutes. They also deployed counting pixels and some of them tracking scripts. The potential privacy risk for consumers is high, since with the periodic requests, the corresponding broadcaster can determine viewing time, i.e., how long did a consumer watch a specific channel.

Group Severe Privacy Risk: Channels assigned to this group transferred data to third parties or personalized advertisement were directly shown on the Smart TV. Periodic requests could be measured on some of these channels.

Group Not Available: Channels in this group could not be measured with our test Smart TVs because of compatibility reasons. But we could find information that they should deliver HbbTV applications on other Smart TVs.

We refer to this grouping in the following section.

3.3 Results of HbbTV Privacy Risks Analyses

Before we give a overview of the results, we refine the methodology for the analyses that were performed in 2012, 2014 and 2015:

- HbbTV analysis in 2012: The analysis were performed on DVB-S (satellite), DVB-C (cable) and DVB-T (terrestrial) from June to December 2012 (see our publications [15, 16]).
- HbbTV analysis in 2014: The analysis were performed on DVB-S and DVB-T in January and February 2014 (see our publication [17]).
- HbbTV analysis in 2015: The analysis were performed on DVB-S and DVB-T in June 2015 (see our publication [18]).

In 2012, we assigned HbbTV channels to five groups: A,B,C,D,Z. They indicated the privacy risk (A lowest and D highest; Z not available). In the analyses from 2014 and 2015 we extended that scheme up to eleven groups: A^+,A,A^-,B^+,B,B^-,C^+,C,D,D^-,Z. In this work we reduced and unified the groups to five due to readability. The mapping from the old groups to the current groups is depicted in Table 3.3.

Current Group	Group in 2012	Group in 2014	Group in 2015
Low Privacy Risk w/o HbbTV	-	A^+	A^+
Low Privacy Risk	A	A	A
Moderate Privacy Risk w/o HbbTV	-	-	B^+
Moderate Privacy Risk	-	A^-	A^-
High Privacy Risk w/o HbbTV	-	-	B (without HbbTV Application)
High Privacy Risk	B	B,B^-	B,B^-
Severe Privacy Risk	C,D	C,D	C^+,C,D,D^-
Not Available	Z	Z	-

- no equivalent group

Table 3.3.: Channel group mapping

Note, the analyses results are representations of at that time measurable HbbTV channels on our test devices, i.e., it could be possible that we did not measure some HbbTV channels because of temporarily unavailable HbbTV applications. We focused on broadcast dependent HbbTV applications, i.e., HbbTV applications that are loaded by turning to a channel with HbbTV signal in the DVB stream. Channels without HbbTV were not analyzed because we were not aware of a privacy risk. They did not produce any data transfers.

Next, we give a summary of the results: Our first analysis in 2012 started with 28 channels that were only TV channels providing HbbTV functionality and one channel with data transfer but no HbbTV. In 2014, we found 44 TV channels and 54 digital radio channels with HbbTV. One year later, in 2015, we found 56 TV channels, 8 channels with data transfer but no HbbTV and 58 radio channels. Clearly, the HbbTV channel coverage has grown with each passing year (see Table 3.4).

	2012	**2014**	**2015**
TV Channels w/ HbbTV application	28	44	56
w/o HbbTV application	1	1	8
Radio channels w/ HbbTV application	0	54	58
w/o HbbTV application	0	0	0
Total number of analyzed channels	29	99	122

Table 3.4.: Number of analyzed channels

In Table 3.5, the number of channels assigned to each group is shown. In 2012, most channels were in the group *High Privacy Risk*, which had periodic requests. In the 2014 and 2015 analyses we saw a move to group *Low Privacy Risk* and *Moderate Privacy Risk*, which reduced the potential privacy risk for consumers. However, a privacy risk for consumers still existed in the last analysis and it is likely that will exist in the future.

Group	**Low Privacy Risk w/o HbbTV**	**Low Privacy Risk**	**Moderate Privacy Risk w/o HbbTV**	**Moderate Privacy Risk**	**High Privacy Risk w/o HbbTV**	**High Privacy Risk**	**Severe Privacy Risk**	**Not Available**
Results 2012	1	4	0	1	0	17	6	2
Results 2014	1	20	0	66	0	0	12	0
Results 2015	1	24	6	74	1	1	15	0

Table 3.5.: Channels assigned to each group.

Note, the channel classifications were done with traffic that had been captured before consumers started the HbbTV application, i.e., consumers did not press the *Red Button* (Phase 1 and 2).

The following traffic flow was common for channels assigned to group *Low Privacy Risk* to *Severe Privacy Risk* (excluding *Low Privacy Risk w/o HbbTV*, *Moderate Privacy Risk w/o HbbTV* and *High Privacy Risk w/o HbbTV*): The HbbTV browser on the Smart TV was triggered by the initial HbbTV URL in the DVB stream[4]. The URL was then automatically extracted and the start-up request was sent via Internet. In

[4] Details, how the HbbTV URL is transported in the DVB stream can be found in the HbbTV standard [31].

return different resources were delivered. If the start-up request had been performed successfully, an HbbTV notification was displayed that the application was ready and could be activated by pressing the *Red Button* on the TV remote control.

We present our results of the HbbTV analyses of TV Channels and Radio Channels in more detail in Section 3.3.1 and Section 3.3.2.

3.3.1 TV Channels

In this section we report the results of our privacy risk TV channel analyses. We assigned each channel to a group mentioned in Table 3.2, we analyzed the traffic flow accordingly. Figure 3.6 illustrates the number of channels assigned and how it increased over the time. A more detailed representation can be found in Table 3.6. We grouped channels of a broadcaster, i.e., ARD Group consists of 17 measured channels, bmt Group of 15 channels and Sky Group of 6 channels. All of them had the same characteristics.

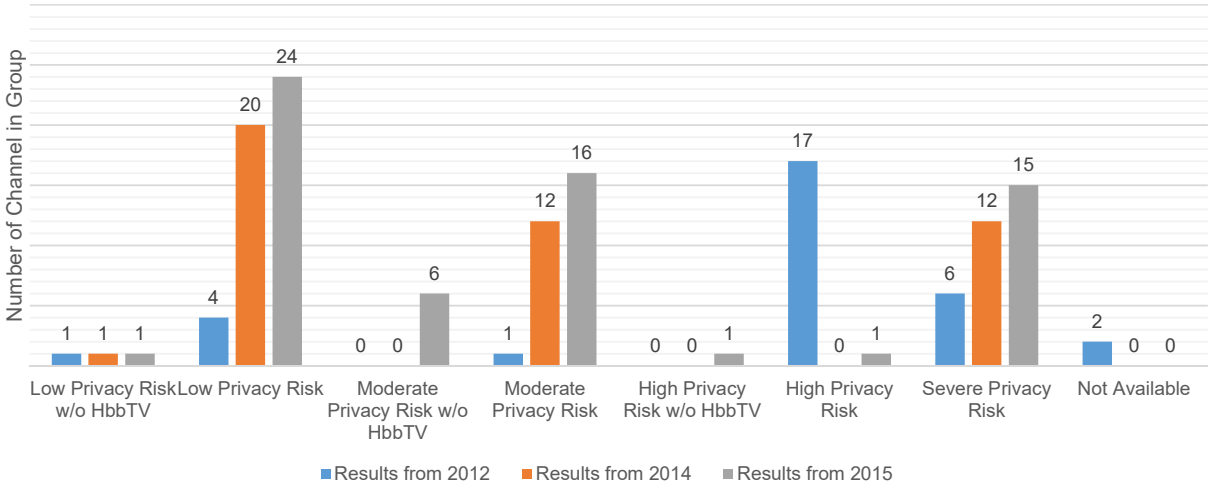


Figure 3.6.: Number of TV channels assigned to each group.

In the remainder of this section we discuss the results for each group:
Group Low Privacy Risk w/o HbbTV: 2012: The channel *N-TV* was assigned. 2014 and 2015: The channel *Super RTL* was in this group.
Group Low Privacy Risk: 2012: The channels *Bibel TV*, *Dr. Dish TV*, *QVC* and the channels of the *ZDF group* were in this group. 2014: *Bibel TV* disabled HbbTV; we could not measure any start-up request of this channel. The *bmt Group*, *Arte*, which was formerly in group *Moderate Privacy Risk*, *Eurosport* and *France 24* were measured in this group. *France24* did not send the start-up request over the Internet; it sent the notification via DVB without any Internet traffic. *HSE 24*, *N-TV*, formerly in group *Low Privacy Risk w/o HbbTV*, and channels of *ORF* were assigned. The two channels *ORF 1* and *ORF 2* were encrypted and could not be watched without an appropriate smart card. Nevertheless, the HbbTV applications were loaded and could be started by pressing the *Red Button*. The *bmt Group* started its HbbTV application in full screen when turning to the channel. The consumer did not need to press the *Red Button*. The channel *ARTE* also moved to this group since the tracking service Google Analytics, which was measured in 2012, had been removed. 2015: Some channels were added.

Group Moderate Privacy Risk w/o HbbTV: 2012 and 2014: No channels were measured. 2015: The channels of the *Sky Group* implemented a tracking method without available HbbTV application. In particular, the HbbTV application was entirely invisible to consumers. The start-up request included the

Group	2012	2014	2015
Low Privacy Risk w/o HbbTV	N-TV	Super RTL	Super RTL
Low Privacy Risk	Bibel TV, Dr. Dish TV, QVC, ZDF Group	bmt Group, Arte, Eurosport, France 24, HSE 24, N-TV, ORF1, ORF2, ZDF group	3Sat, bmt Group, Arte, Eurosport, France 24, HSE 24, HSE 24 Extra,ORF1, ORF2, ORF3, ZDF Group
Moderate Privacy Risk w/o HbbTV	-	-	Sky Group
Moderate Privacy Risk	-	ARD Group	ARD Group
High Privacy Risk w/o HbbTV	-	-	Servus TV AT
High Privacy Risk	ARD Group	-	Servus TV DE
Severe Privacy Risk	Anixe, Arte, Kabel 1, Pro Sieben, Puls 4 Austria, Sat 1, sonnenklar.tv	Anixe, Kabel 1, Pro Sieben, Puls 4 Austria, QVC, RTL, RTL2, RTVE, Sat 1, Sixx, Sonnenklar.tv, VOX	Anixe, Kika, Bibel TV, Kabel 1, N-TV, Pro Sieben, Puls 4 Austria, QVC, RTL, RTL2, RTL Nitro, Sat 1, Sixx, sonnenklar.tv, VOX
Not Available	RTL, VOX	-	-

Table 3.6.: List of TV channels in each year.

analytics tool Piwik[5]. A privacy policy could not be found. Although all channels of *Sky Group* were encrypted (=Pay-TV) the invisible HbbTV applications were transferred.
Group Moderate Privacy Risk: 2012: No channels could be measured. 2014 and 2015: *ARD group* moved to this group. The broadcaster disabled periodic requests and added a fall-back implementation of HbbTV over the DVB stream. No Internet connection was required to deliver a non-customized HbbTV application to the Smart TVs. But, if an Internet connection had been available, the channels used it and customized the HbbTV application (e.g. the channel logo).

In the group *Moderate Privacy Risk w/o HbbTV* we found counting pixels that were in the following format:

```
1 http://hbbtvserver.com/stat/p.png?redir=1&app=1&sid=28479&sub=-1&delivery=11&uid=5
      aab3ecd0cad34153b2c83cd1031d0ab&d=84305.1393622531075
```

These requests could be categorized as counting pixel since the response was an image with 1x1 pixels. We could not clarify the meaning of the parameters `redir`, `app`, `sub`, `delivery` and `uid`. `Redir`, `app`, `sub` and `delivery` never changed in our analysis. However, `uid` changed from one device session to another, i.e., if the Smart TV was turned off and turned on, the `uid` changed.

Group High Privacy Risk w/o HbbTV: 2012 and 2014: No channels were measured. 2015: The Austrian channel *Servus TV AT* did not deliver an HbbTV application. But, the German version of this channel did. Thus, the behavior looked like an implementation error. Periodic Requests could be found.
Group High Privacy Risk: 2012: The channels of the *ARD group* deployed a mechanisms that performed periodic requests. 2014: No channel were measured. 2015: The channel *Servus TV DE* deployed periodic

[5] `http://piwik.org/`

requests. All channels from 2012 and 2015 in this group included all characteristics of the mentioned lower channel groups. In addition, periodic requests before the consumer had pressed the *Red Button* could be measured. The time intervals of these requests were between 20 and 70 seconds.

Group Severe Privacy Risk: 2012: The channel *Anixe* showed an advertisement every 15 minutes over the current running program (see Figure 3.7). The customer had no option to disable that overlay. Even

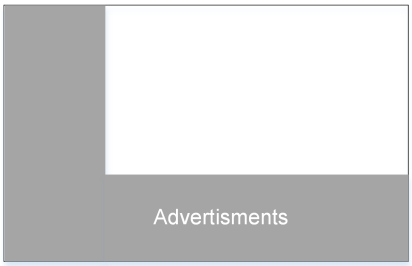


Figure 3.7.: Advertisements of channels in group Severe Privacy Risk.

if the channel had been broadcasting an ad, the HbbTV ad was additionally shown. At this point, we were not aware if the ads were personalized. But, we got different ads on our test devices. *Arte, Kabel 1, Pro Sieben,Puls 4 Austria, Sat 1* and *sonnenklar.tv* used Google Analytics for consumer tracking. Furthermore, we found the analytics services *Chartbeat* and *Webtrekk*. Moreover, *Kabel 1, Pro Sieben* and *Sat 1* deployed a periodic counting method. The periodic requests were in the following format:

```
1 http://hbbtvserver.com/?c=Channel&seq=1&open=1&sid=3729871
```

The parameters `seq` and `open` were parameters that counted up every request and `sid` seemed to be a session identifier. Parameter `c` indicated the name of the channel. This request returned a JavaScript command that did not provide any function. With this technique it was possible to determine the time a consumer had been on a specific channel. 2014: Google Analytics and other tracking services have been removed from *Pro Sieben, Kabel 1, Sat 1* and *Puls 4 Austria*, but were still sending data to third parties. *Sixx* deployed HbbTV and had a similar behavior as the aforementioned channels. The two channels *RTL* and *VOX* that were formerly in the group *Not Available* moved to group *Severe Privacy Risk*. They provided an HbbTV application to all consumers of a device that supported HbbTV. Periodic requests could not be measured on this two channels.

In summary, in this group we found channels that sent data to third parties like INFOnline[6], IVW[7], Google Analytics[8], etracker[9] and ScorecardResearch[10]. These services are services, which can be used to track a consumer accurately. As in all other groups the consumers were not able to avoid sending data to such services. 2015: The channel *Kika*, which is part of the *ARD Group* sent data to xiti[11]. On the other channels we found Google Analytics, ioam, webtrekk, xiti.com, adform.net, etracker.de and the self-hosted analytics solution Piwik.

Cookies. In 2015, we analyzed the usage of cookies in HbbTV. Many cookies were set with identifying numbers and an expiration date with 30 days up to 1 year. Thus, they remained on the devices for many days. Webtrekk was used on *Sat.1, Pro Sieben and Kabel 1*. This tracking company have used Evercookie, a mechanism to create extremely persistent cookies. Its goal is to identify a device even after removal of standard cookies (see [32]). Our test devices did not provide any functionality to delete cookies.

6 https://www.infonline.de/
7 http://www.ivw.eu/
8 http://www.google.com/analytics/
9 http://www.etracker.com/en.html
10 https://www.scorecardresearch.com
11 http://xiti.com/

3.3.2 Radio Channels

We discuss over 50 digital satellite radio channels that used HbbTV (see Table 3.7). They were provided by the same broadcaster. The characteristics of the traffic could be assigned to group *Moderate Privacy Risk*, which means that a start-up request and a counting pixel have been measured. Furthermore, images with the radio channel logo were requested.

Group	Moderate Privacy Risk
Results 2012	0
Results 2014	54
Results 2015	58

Table 3.7.: Radio channels assigned to each group.

On all radio channels we observed that the privacy protecting method via DVB was enabled. Therefore, if an Internet connection had not been established, the HbbTV application was available via DVB and the radio channel logos were not customized, i.e., just the logo from the radio station (e.g. general logo for ARD group) were shown on all HbbTV notifications. The radio channels that used HbbTV are listed in Table 3.8.

Group	2014	2015
B	Bayern 1, Bayern 2, Bayern 3, Bayern Plus, BR Klassik, BR Puls, HR 1, HR 2 Kultur, HR 3, HR 4 Rhein-Main, HR Info, MDR 1 Radio Sachsen, MDR Figaro, MDR Info, MDR Jump, MDR Klassik, MDR Radio Sachsen-Anhalt, MDR Sputnik, MDR Thüringen, NDR 1, NDR 2, NDR 90.3, NDR Blue, NDR Info, NDR Infor Spezial, NDR Kultur, SWR 1, SWR 2, SWR 3, SWR 4, SWR info, WDR 1, WDR 2, WDR 3, WDR 4, WDR 5, WDR Event, You FM	Bayern 1,Bayern 2, Bayern 3, Bayern Klassik, B5 aktuell, Bayern Plus, Bayern Heimat, hr 1, hr 2, hr 3, hr 4, you fm, hr-info, MDR 1 Sachsen, MDR 1 Sachsen-Anhalt, MDR 1 Thüringen, MDR figaro, MDR jump, MDR Sputnik, MDR info, NDR 2, NDR kultur, NDR info, N-Joy, NDR 90,3, NDR 1 WN, NDR 1 MW, NDR 1 NS, NDR info spezial, Bremen Eins, NW Radio, Bremen Vier, Inforadio Rbb, Kulturradio rbb, Antenne Brandenburg, radio berlin, radio eins, Fritz, SR1, SR2, SR3, SWR 1, SWR 1 RP, SWR 2, SWR 3, SWR 4 BW, SWR 4 RP, Das Ding, SWR Info, Eins Live, WDR 2 klassik, WDR 3, WDR 4, WDR 5, WDR Funkhaus Europa, Eins Live Diggi, KIRAKA, WDR Event

Table 3.8.: Radio channels in 2014 and 2015.

In 2014 we found cookies, which had a long life time – over 20 years. In 2015, the life time was reduced to one year. The cookies were set before the consumer had the possibility to disable it. An option to disable it was available after starting the HbbTV application with the *Red Button*. However, without awareness of the consumers, it is unlikely that they search for the option.

We did not find periodic requests or analytics services, so the time a consumer is on a channel could not be gathered accurately. Only the selection time of a radio channel was reported to the broadcasters.

3.4 Consumer Tracking in Encrypted Wi-Fi Networks

The previous sections were focused on privacy risks of HbbTV caused by broadcasters. This section focuses on a side channel attack of HbbTV, which we revealed while analyzing the HbbTV channels. We are not aware of any other publication that found this vulnerability. The transferred data packet sizes of the HbbTV notifications were unique for a channel, i.e. each channel requested many resources where the requests and responses had characteristic packet sizes for this channel. Those packet sizes could also be analyzed in an encrypted Wi-Fi network since the used Wi-Fi encryption did not change the packet sizes. It added a small overhead to the packets that could be calculated. This enabled criminals or neighbours to analyze the usage behavior of Smart TVs when these Smart TVs were connected over a Wi-Fi network to the Internet. The criminals or neighbours did not need to be a member of the Wi-Fi network, i.e. they did not need the pass-phrase of the network. Capturing of the encrypted data was sufficient.

We describe the methodology of this analysis in Section 3.4.2. In Section 3.4.3, we report on our results. We published the results in [15, 16].

3.4.1 Attacker Model

The attacker model in this section differs from the attacker model shown in Section 3.1. Here, we have an external attacker (e.g. criminals or neighbours) that is not connected to the encrypted Wi-Fi network. The attacker receives the Wi-Fi signal but cannot communicate with other devices in the network since it is not member of the network. If the network is encrypted, the attacker only sees encrypted data. The only exception is the meta data (e.g. source MAC, destination MAC) that are needed to communicate in a Wi-Fi network. If it is not encrypted, the attacker sees plain text. The entire model is depicted in Figure 3.8. The attacker does not manipulate any traffic.

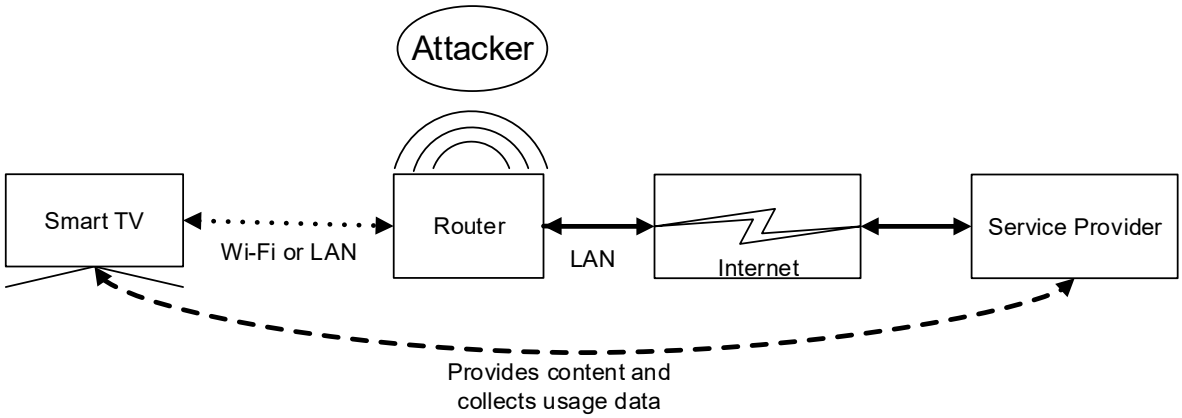


Figure 3.8.: Attacker model for consumer tracking in encrypted Wi-Fi networks.

3.4.2 Methodology

We analyzed the fact that the characteristics of the HbbTV notifications differed from channel to channel and were unique for a channel. For that, we setup the following test environment as outlined in Figure 3.9. Note, it was similar to a real setup in a household with a Smart-TV and a Wi-Fi connection to the Internet over a router.

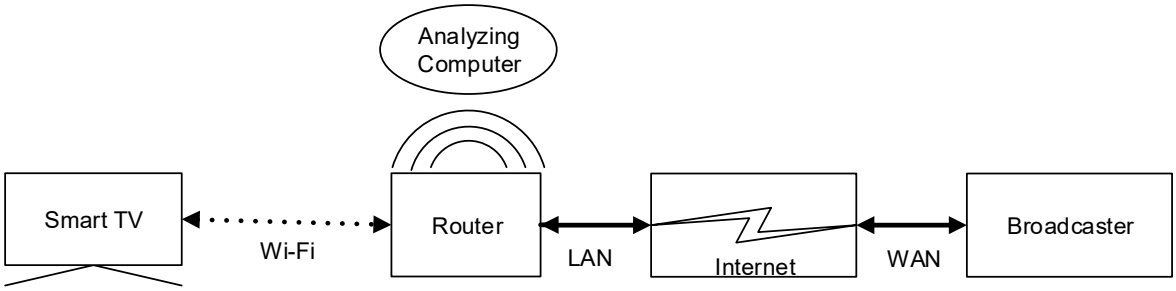


Figure 3.9.: Test environment for the consumer tracking in encrypted Wi-Fi network analysis.

The Smart TV was connected via Wi-Fi with the Internet gateway (e.g., a Wi-Fi router) and the computer that is equivalent to the attacker from the attacker model snooped on this connection. The computer was not member of the Wi-Fi network so that it only see the encrypted network traffic. Meta information that can be read in an encrypted network without further difficulties are packet sizes as well as the MAC addresses and the time a packet was sent. In an encrypted Wi-Fi network, the IP addresses cannot be determined.

As WPA2 (Wi-Fi Protected Access 2) is the standard for Wi-Fi encryption, we enabled it for all our tests. There are two different modes: WPA2-Personal and WPA2-Enterprise. We used the WPA2-Personal version, where one shared secret is entered in each device that should be member of the network.

We reviewed how the encryption in WPA2 modified a plain packet. In WPA2, AES-CCMP or TKIP is used to encrypt the network packets. In both methods (and WEP) the plain text is being encrypted with a stream cipher (RC4 with WEP and TKIP, AES with Counter-Mode in AES-CCMP). Additionally, a block with fixed length to protect the integrity is appended. A padding, as used for example with block ciphers masking the real length of a data packet, is not used. Even the MAC address of the sender resp. the recipient of the packet is transmitted unencrypted. Thus, it is possible to identify the vendors of all devices in an encrypted Wi-Fi network, and the length of the plain text packets of the encrypted data packets with a specific overhead [33].

3.4.3 Results

We observed that all channels with HbbTV applications had requests and responses where the combination of packet sizes were unique for the channel. In detail, they pre-loaded parts for the HbbTV application itself, which did not change very frequently: configuration and script files. Files that depended on the current program changed very frequently. The data was usually transferred via HTTP which enabled us to see the packets in the original sizes in our test environment as depicted in Section 3.2.

On the Smart TV side, the start-up and periodic requests differed in the URL that was requested. In return to these requests the server's content had mostly the same size. The amount of received data and the size of each data packet differed from channel to channel. In order to detect the HbbTV channel over the encrypted Wi-Fi network we used the following technique:

1. We created a list of all HbbTV channels. This list contained the typical transferred packet sizes. It was important that the computer monitoring these packets was member of the network (not the analyzing computer). Thus, we saw all packets in plain text. Packet sizes found on more than one channel, were ignored. Packets belonging to data that was usually cached by the browser were filtered and removed, e.g. pictures.

2. We then captured the whole encrypted data stream of the Smart TV with the analyzing computer. It was not possible to determine if the encrypted data was from HbbTV or other data traffic from the Smart TV due to the encryption. However, it was possible to select the traffic of the Smart TV

by filtering with the Smart TV's MAC address. Another filter removed all data packets, which had full MTU (maximum transmission unit) length. With a sliding window method all packets were captured that were within a time interval of ten seconds, i.e., packets of the previous ten seconds were analyzed. If most captured data packet sizes were contained in the list created in 1., it was very likely that this was a specific channel running on the Smart TV.

In step 2., packets with full MTU were removed, since they could be not used for the analysis. Full packets could be produced by (1) overlong data, (2) padding of shorter data. Both could not be distinguished. Only different packet sizes increased the accuracy.

In our experiments we had no false positives, however, sometimes instead of identifying the individual channel, the channel group was identified, e.g. ARD. The reason was that some broadcasters deployed the same application for all their operated channels. Only the logos differed in the start-up and periodic requests. This behavior was always tested live on the channels listed in table 3.6 and only the packet sizes, which were unique for the TV channel, were extracted from saved data.

Some limitations of this approach exist:

- A channel being turned on for only a few seconds turned out to be a problem. The HbbTV data was only partially loaded and our test script was not able to recognize the channel.
- If the Internet connection was established over DSL with PPPoe or VPN and the Smart TV could not use the full packet size of 1500 bytes, the list of packet sizes had to be modified, so that the characteristics were aligned to the new MTU size.
- A possible extension of the attack technique would be to add timing information and response information to the analysis. However, we did not implemented this extension, since we had a high probability to recognize the right channel or channel group in our analysis.

The source code of this prototypical implementation is attached in Appendix B.

3.5 Related Work

We report on different types of related work that were published about security vulnerabilities causing privacy risks and privacy risks.

The first categories are directly related to HbbTV:
Privacy risks of HbbTV. To the best of our knowledge, we were not aware of any other academic work related to privacy in HbbTV except our own articles published in 2013 [15], 2014 [16, 17] and 2016 [18]. After our first investigations, other authors such as Jaritz *et al.* [34] and Sachs *et al.* [35] also did traffic analyses and found similar issues in HbbTV.
Security risks in HbbTV. In recent years, some security vulnerabilities of HbbTV were published. Oren *et al.* [36] showed an attack on the DVB stream that outlines a large-scale attack, in which many devices receive malicious URLs or content. Since an overlay over the current running program is supported by the HbbTV standard, a phishing attack covering the whole screen with malicious content is possible. Even a large-scale attack of underlying components based on software vulnerabilities is a realistic scenario. Michéle *et al.* [11] showed an attack to execute system commands on outdated media players implemented in Smart TVs using a USB stick. Vulnerable media players that were also used in the HbbTV browser of Smart TVs could also be exploited by malicious video streams.

The next two categories are related to privacy risks that occurred due the implementation of the next mentioned Smart TV functionality:

Privacy risks due to vendor's data collection. An Internet blog "DoctorBeet" [37] revealed that LG models sent usage data even when the functionality that data should be sent to the vendor was deactivated. Furthermore, the blog authors revealed that LG also collected the names of files stored on external media devices that were connected to those Smart TVs. The Daily Mail [38] reported that Vizio Smart TVs also profile consumers in order to sell the collected data to advertisers.

Privacy risks of the voice recognition functionality. Many Smart TVs have integrated sensors such as microphones and cameras. Functionality such as voice-based control is facilitated thereby. For this functionality, the entire audio stream needs to be analyzed to extract the Smart TV commands. But, the performance capacity and internal storage of Smart TVs is often limited, so that only a few commands can be directly processed on the Smart TV when it is not connected to the Internet. If the device is connected to the Internet the voice recognition is often carried out by the vendor's server or an external service. According to their privacy policies, Samsung shares its voice recognition information with Nuance [39] and LG shares with unspecified third parties [40]. This functionality could lead to serious surveillance issues as reported in CNET [41] or the Daily Beast [42]. Additionally, Lodge [43] revealed that some Samsung Smart TVs transferred voice data without any encryption. In newer generations of Smart TVs this functionality is only activated by pressing a button on the remote control.

3.6 Discussion and Summary

In this chapter, we analyzed over 122 channels that supported HbbTV. This includes 64 TV and 58 radio channels. In over three years analysis time, we showed that HbbTV sent data to the broadcasters and third parties without consumer's consent.

The results presented in this work are snapshots of specific time periods. Thus, it is likely that new HbbTV analyses would lead to other results. In this work we did not analyze the entire HbbTV application, since they are similar to web applications. We analyzed data that was transferred before the consumer intentionally started the HbbTV application. From 2012 to 2015, we observed changes in the following characteristics: Number of HbbTV channels, transferred content, HbbTV standard and the privacy risk of channels. No privacy risks for consumers could be determined on HbbTV channels that transfer the HbbTV notification over the DVB stream; only one channel did so. All other measured channels were at least assigned to a low privacy risk group. Privacy statements that informed about the HbbTV notification could not be found outside the HbbTV application. While we were conducting our HbbTV analysis in 2012, suddenly the HbbTV functionality was turned on by a Smart TV update, so the privacy risk increased. On all newer tested Smart TV models the HbbTV functionality were enabled by default.

HbbTV channels that had transferred data without consumer interactions were a privacy risk for consumers. We assume that the technique was used to track and profile consumers in order to get more accurate viewing figures. This is supported by different observations in our analyses:

- **Periodic requests were detected.** We identified requests that were repeated in a specific rate. These requests included information that could be used to extract data such as the time a consumer watched a channel or consumer's channel selection behavior.
- **Counting pixels were found.** We measured counting pixels that could be used to count visitors and page impressions of a website. In the Smart TV context this information indicates how much consumers were watching a TV channel or listening to a radio channel.
- **Tracking scripts were found.** Many tracking scripts were found before the consumers actively started the HbbTV application. We found an increasing number of channels that deployed tracking scripts from 2012 to 2015. It was not limited to a specific tracking method. It is rather a variety of tracking services (self-hosted and external) that were used. All of them were developed

for collecting consumer data to get more accurate profiles; in this context viewing and listening behavior.

- **Cookies with unique IDs were detected.** Cookies with unique IDs and a lifetime of one or more years have been found. The values saved in the cookies could identify a Smart TV and be used to profile consumers. We do not know if the profiling was performed at server level, but a privacy risk exist.

- **Persistent cookies found.** In 2015, we analyzed the cookies set from HbbTV channels. We found long life cookies from one year to 20 years and additionally Evercookie, a mechanism to create extremely persistent cookies, on three HbbTV channels. With this technique and the missing cookie management functionality of most Smart TVs, it has been almost impossible to delete those identifying cookies for consumers. This is a very alerting fact.

Since our results reflect which data flow was going from the tested Smart TVs to the broadcasters or other third parties, we do not know how the gathered data was processed by them. Even the possibility to collect a variety of data has been a high privacy risk for consumers. The data could be used to gather consumer behavior in real time with more accuracy than ever before. Most Internet service providers in Germany assign an IP address to a household for 24 hours or longer, which makes the household unique and identifiable within that time period. Even afterwards, Smart TVs could be identified by using cookies with IDs. With such data it is easily possible to link a Smart TV with an already existing data set even after an IP renewal.

As we started our investigations in 2012 the HbbTV 1.5 standard did not state anything about privacy. After presenting our paper [15], we had a huge media coverage. In this publication, we mentioned the following recommendations to mitigate some privacy risks:

- **Adding privacy information to the HbbTV standard.** We recommended to add guidelines for privacy by design, e.g., list of functionality before pressing the *Red Button*, standardize the transfer of the HbbTV notifications and omitting tracking scripts in the HbbTV notifications.

- **Changes at the Smart TVs.** Smart TVs provide the HbbTV browsers. These browsers did not provide user interfaces to control cookies or enable tools like Adblock[12] or NoScript[13]. The Smart TV user interface should communicate more information about the revealed privacy risks to consumers. A more restrictive approach would be to forbid to transfer the HbbTV notification over the Internet.

- **Changes at the HbbTV applications.** We recommended that the HbbTV applications should be implemented as privacy protecting as possible.

A privacy section was added to a revised specification of HbbTV (see HbbTV 2.0 standard [22]). Some of our mentioned recommendations were incorporated.

In 2014 and 2015, we observed that security and privacy in HbbTV were more considered. The following findings indicate it:

- **DVB were used to transfer HbbTV by some channels.** We found a more privacy protecting method to transfer HbbTV applications. Broadcasters could provide HbbTV over DVB. Thus, no data have to be transferred over the Internet. We observed that it was used in two different ways: (1) Fall-back when the Internet connection was not available and (2) transferring the HbbTV notification without any request to the Internet. The most privacy protecting method to transfer the HbbTV notification entirely over DVB was less used. Instead, many channels used DVB when no Internet

[12] `https://adblockplus.org/de/`
[13] `https://noscript.net/`

connectivity was available. But if the Smart TV was connected to the Internet, it still transferred data to the broadcaster's server. We recommend to use the privacy protecting method for more channels.

- **HbbTV switched to HTTPS.** In 2015, we observed that more channels switched from HTTP to HTTPS for HbbTV applications indicating that security and privacy have been more considered. We expect a growing amount of channels switching to HTTPS in the future.

Furthermore, we showed that the usage behavior of a Smart TV that was connected over an encrypted Wi-Fi network could be profiled. We captured and then processed the collected data in such a way that we could detect which channels were watched. This attack was even possible when the network was secured with the current WPA2 standard. For the attacker it was not necessary to have the pass phrase for this network. We implemented a prototypical tool that could analyze the Wi-Fi network traffic and extract the information needed to determine the watched channel.

4 Privacy Risks Caused by Security Vulnerabilities in Smart TVs

In this chapter, we discuss different security vulnerabilities causing privacy risks that we revealed in Smart TVs. In Section 4.1, we give an introduction to HTTPS. We describe the corresponding attacker model in Section 4.2. In Section 4.3, we present our HTTPS certificate validation analysis in Samsung and LG Smart TVs. The result is that many Smart TVs were vulnerable for different attacks on the HTTPS validation. Another security vulnerability causing privacy risks is downgrading of Smart TV firmware, which we discuss in Section 4.4. Furthermore, we present other vulnerabilities in Section 4.5. Section 4.6 reports on related work. Finally, we give a summary and discuss our results in Section 4.7. We published parts of this Chapter in [17, 23].

4.1 Introduction to HTTPS

The mostly used protocol in the Internet is HTTP defined in RFC 2616 [44]. Data is transferred in plain text and no encryption is applied, a non-legitimate person could read and manipulate it. To overcome this, HTTP over SSL/TLS was introduced and called as HTTPS (see RFC2818 [45]).

Current web browsers on desktop and mobile devices support HTTPS and process requests fully transparent for users, i.e., the user does not need to take any additional action compared to HTTP requests. HTTPS guarantees confidentiality and integrity transparently on the route to and from the user. The encryption used for HTTPS is asymmetric; this means that the server has a private key and the client needs the server's public key to negotiate a symmetric key for HTTPS session initiation. An HTTPS certificate (SSL certificate or technically an X.509 certificate) is used to bind the public key to a specific subject, in this case a web server. The subject of an HTTPS certificate is usually the host name of the web server, e.g., ssl1.wsp.lab.sit.cased.de.

A registration authority (RA) is the entity that is responsible for the trusted binding of a specific subject to a public key. Before a certificate authority (CA) issues and cryptographically signs an HTTPS certificate, a RA must verify that the binding is legitimate, i.e., a trusted CA should never issue a certificate for which the legal owner of a host does not provide the public key. In order to ensure that only HTTPS certificates issued by trusted CAs are valid in web browsers, they are bundled with a list of trusted CAs. Therefore, the validation of these HTTPS certificates by the web browser is essential for the security of HTTPS. If a connection does not provide a trusted HTTPS certificate, a connection must be considered to be insecure by the web browser. Further information about certificates can be found in RFC 5280 and 6818 [46, 47].

It is important that the result of the HTTPS certificate validation process is presented to the user. In web browsers, the user usually gets a lock symbol next to the address bar of the browser (see Figure 4.1). Current browsers on desktop PCs notify the user whether a certificate is valid or not.

Valid certificates in web browsers: Figure 4.1 (b) shows a web site requested via HTTP and (a) a web site via HTTPS. Therefore, the green lock in the browser's address bar clearly indicates a secure connection, i.e., the HTTPS certificate is valid. The HTTP connection does not show the prefix **http://** nor a green lock symbol.

In both cases more information will be displayed when clicking on the symbol in front of the address. In the case of HTTPS the user can verify the certificate information presented. A manual HTTPS certificate check is possible by comparing the public key hash codes; but end users do often not do this. The integrated automatic validation is performed with the trusted list of CAs and is updated regularly since a malicious CA could lead to security issues and privacy risks. If a CA is not in the list, the certificate will not be marked as valid. However, users can always import their own certificates, which will then be considered to be secure only on their own system.

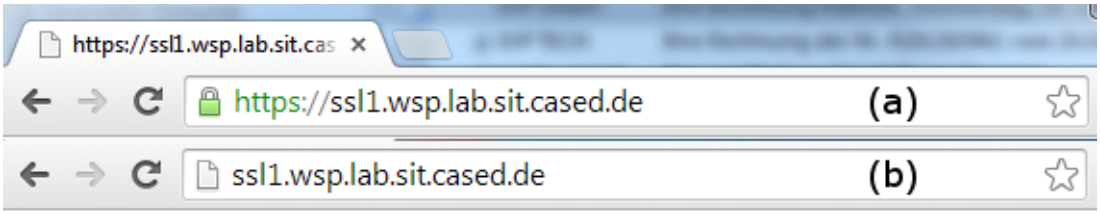


Figure 4.1.: Google Chrome Browser - (a) web site with valid HTTPS certificate; (b) web site with HTTP

The list of trusted CAs for certificates can be found in the browser options. In mobile devices it is located in the main settings. This option is essential for users to see which certificate authorities are trusted.

Invalid certificates in web browsers: There are different reasons why a certificate will be marked as invalid in the web browser. All current web browsers show qualified warnings in addition if a certificate is invalid. With this information the user can decide whether to trust the requested web site nevertheless.

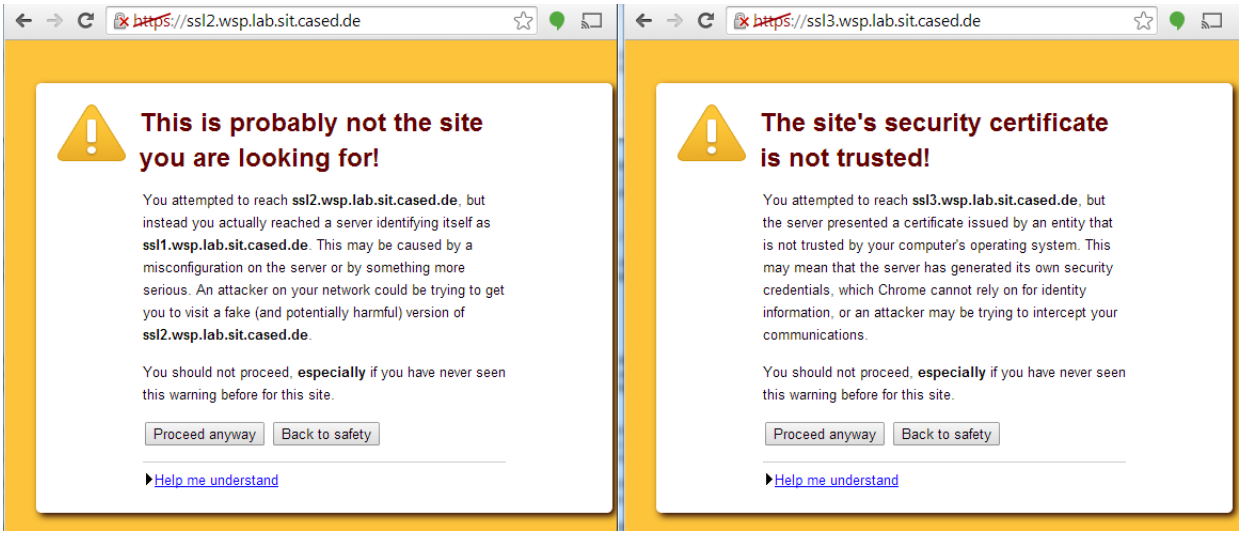


Figure 4.2.: Google Chrome - both certificates are invalid for the specific host

Figure 4.2 shows two different cases: (1) the subject (web server) in the HTTPS certificate does not match with the web server delivering the web site and (2) the HTTPS certificate is not trusted because it has been self-signed. Both warnings notify the user that these requested sites are considered to be insecure. The address bar additionally strikes out *https* and the text color is changed to red. This indication will remain even if the user clicks on *Proceed anyway*, so a user is always able to see if the connection to the web site is considered to be secure.

HTTPS on Smart TVs. Much functionality of Smart TVs communicates over the Internet, e.g. web browser, HbbTV, apps. Some functionality needs to transfer the data secured over the Internet. Internal services such as updating the Smart TV need HTTPS to secure the update transfer to the Smart TVs in order to protect the updates against manipulation during transfer. Hence, without HTTPS on Smart TVs much functionality cannot be guaranteed to be secure and without risks for consumers.

4.2 Attacker Model

The attacker model in this chapter is basically an attacker that is in between the connection, a so called man-in-the middle attacker. The attacker can manipulate and read all traffic between the Smart TV

and the service provider, e.g., an online-banking provider, broadcaster, vendor. Essentially, the data is transferred secured with HTTPS. If the Smart TV or its apps (e.g. web browser) does not check whether the provided HTTPS certificates are valid, the connection between service provider and Smart TV must be considered to be insecure. The Smart TV, as standard web browser also does, should notify consumers about this issue. Figure 4.3 outlines the attacker model. Note, if the connection is not secured with HTTPS, the attacker can manipulate exchanged data without any notice.

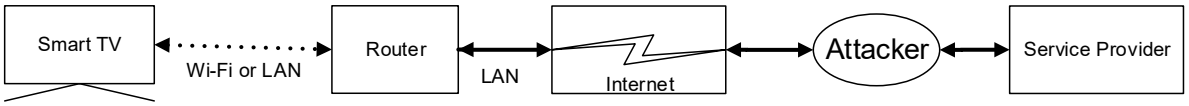


Figure 4.3.: Attacker model of the Smart TV vulnerabilities.

4.3 Vulnerabilities in the Smart TV Implementation of HTTPS

We describe the methodology of the analysis in Section 4.3.1. In Section 4.3.2, we discuss vulnerabilities in the validation process of HTTPS in Samsung and LG Smart TVs.

4.3.1 Methodology

We describe the methodology for the HTTPS validation analysis of our tested Smart TVs. Since we needed to analyze the entire network traffic from Smart TV to the Internet, we setup a similar test environment as described in the previous chapter (see Figure 4.4).

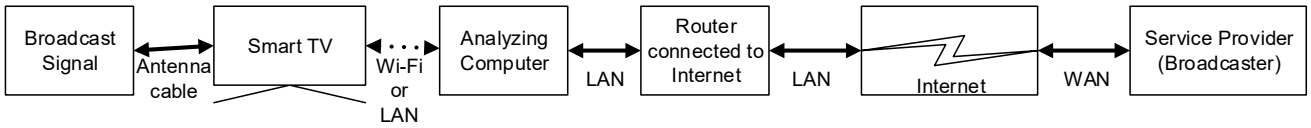


Figure 4.4.: Test environment for HTTPS validation analysis.

In order to analyze the behavior of our tested Smart TVs when a HTTPS certificate is manipulated, we monitored the network traffic while we actively changed the certificates. The monitoring were performed with Wireshark. Mitmproxy[1] were used for the manipulation of the certificates, i.e. we generated new certificates that copied the values from the original certificates. Thus, it breaks HTTPS on-the-fly and issues self-signed certificates that are sent to the recipient.

We performed two different tests for checking the HTTPS certificate validation:

- **HTTPS certificates on web sites.** We set up web sites with three different certificates that we call A,B,C. Two of them were invalid due to different reasons (see Table 4.1 for details); one was valid. This test could be used, when it was possible to enter the URL manually, e.g. in Smart TV's web browser. We expected that the Smart TV that requested the web sites with the invalid certificates B and C would warn the consumers. The web browsers that were implemented in our tested Smart TVs were non-standard browsers.

- **On-the-fly change of HTTPS certificates.** With the test environment outlined in Figure 4.4, the Mitmproxy could change the HTTPS certificates on-the-fly. Basically, the Mitmproxy read the original certificate and self-issued a new self-signed HTTPS certificate that contained all information

[1] `https://mitmproxy.org/`

Certificate	Description	Expected Behavior
Certificate A	Valid Certificate: It was issued for the correct host name	Device/browser should handle that as valid.
Certificate B	Invalid certificate: It was issued for a different host name	Device/browser should handle that as insecure.
Certificate C	Invalid certificate: It was self-signed.	Device/browser should handle that as insecure.

Table 4.1.: List of certificates that were used in the tests.

from the original certificate, so the only difference was the issuer of the HTTPS certificate and the corresponding keys. The Smart TV then requested HTTPS as usual. We expected that this change in the HTTPS certificate was detected and the request aborted with a consumer warning.

We tested the following Smart TVs with all available Internet updates[2]: Samsung UE40D6200, UE55D6500, UE40ES6300, UE46F6640, UE40JU6580 as well as the LG 32LF6309 and LG 42LN5758.

4.3.2 Results

We discuss wrongly implemented validation of HTTPS certificates in Samsung and LG Smart TVs. Since we did not have root access to these tested Smart TVs, we could not analyze in detail which subsystem of the Smart TVs caused these issues.

Wrong Validation of HTTPS Certificates on Samsung Smart TVs

We found different vulnerabilities in the HTTPS certificate validation process in Samsung Smart TVs. The Smart TV's web browser did not check HTTPS certificates correctly in 2012[3]. In 2013, we tested the validation of certificates in HbbTV, which was also not performed correctly. Finally, we showed a vulnerability in a Smart TV model from 2016.

Wrong HTTPS certificate validation in the web browser. We tested whether consumers get a warning if a web site with an invalid HTTPS certificate was requested on our tested Smart TVs. The web sites with the valid certificate A and the two invalid certificates B and C were requested in the Smart TVs' web browsers (see Table 4.1). The following Smart TVs did not warn consumers about the insecure connection to these web sites: Samsung UE55D6500, UE40ES6300, UE46F6640 in 2012 and 2013.
The details were as follows:
Certificate A (valid): As expected, all tested Smart TVs marked the HTTPS certificate as valid.
Certificate B and C (both invalid): The vulnerable Smart TVs marked the HTTPS certificates as valid without any security warning. As shown in Figure 4.5, the Smart TV models (a) and (b) displayed a lock symbol on the right side and Smart TV model (c) on the left side next to the address bar.

We tested these Smart TVs with the second test method (on-the-fly change of HTTPS certificates) and intercepted the traffic with Mitmproxy. As expected from the first test method, the self-issued certificates were not marked as invalid by the Smart TV browser. They were marked valid.

[2] Other updates that had to be manually flashed to the Smart TVs were not considered.
[3] Note, this was confirmed by Samsung's Smart TV security team.

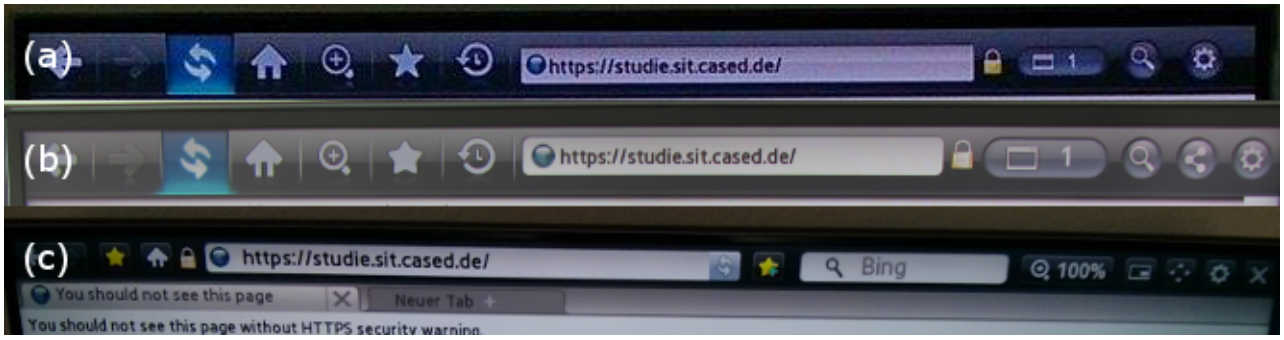


Figure 4.5.: Web browser screenshots of the Samsung Smart TV models (a) UE55D6300, (b) UE40ES6300 and (c) UE46F6640 after requesting the web site with certificate B.

Wrong HTTPS certificate validation in HbbTV. We analyzed the HTTPS validation process in HbbTV whether it warns the consumer about invalid HTTPS certificates. The following Smart TVs did not warn the consumers: Samsung UE40D6200, UE55D6500, UE40ES6300, UE46F6640.
In detail, we tested for all mentioned Smart TVs whether these Smart TVs warn the consumer when an HbbTV application with invalid certificate was requested. Since we were not able to enter URLs in HbbTV, we performed only the second test method (on-the-fly change of HTTPS certificates). The mentioned Smart TVs accepted self-issued certificates without any warning.

Wrong HTTPS certificate validation in time server client of the Smart TV. In 2016, while analyzing the Smart TV Samsung UE40JU6580 we detected one HTTPS connection that could be intercepted without warning. Since it was a background activity that was performed at boot time of the Smart TV, we were not able to enter URLs with our test HTTPS certificates. Thus, we tested the Smart TV with the second test method (on-the-fly change of HTTPS certificates). The invalid self-issued certificates were accepted by the Smart TV. We analyzed the content of this request and found that it was compatible with zic [48], a time zone compiler. According to the syntax, we manipulated the content in order to see a different behavior on the Smart TV. But, we could not detect any changes. We could not clarify how this vulnerability can be exploited, since we did not know how the under-laying operating system of the Smart TV was communicating with the system software of the Smart TV.

Wrong Validation of HTTPS Certificates on LG Smart TVs

In 2016, we found one HTTPS connection on boot time of the LG 32LF6309 Smart TV that did not validate the HTTPS certificate correctly. Since it was a background activity that was performed at boot time of the Smart TV, we were not able to enter URLs with our test certificates. Therefore, we performed the second test method (on-the-fly change of HTTPS certificates). We could perform a man-in-the-middle attack and self-issued our own certificate with Mitmproxy. The content of this request was a unique ID that we changed. But, we did not noticed any behavior changes on the Smart TV. We could not clarify how this vulnerability can be exploited, since we did not know how the under-laying operating system of the Smart TV was communicating with the system software of the Smart TV. Other HTTPS connections we analyzed on this TV were validated correctly and rejected our attack.

4.4 Firmware Downgrading

We analyzed the update mechanisms of all Smart TVs. We found that the LG 32LF6309 was vulnerable to downgrading attacks, i.e., the firmware of the LG 32LF6309 could be downgraded due to a vulnerable update mechanisms. Downgrading firmware could be misused to install an outdated and vulnerable

software version with known vulnerabilities that could be exploited. More details of this vulnerability is reported from Neidig [24].

We describe the methodology how this vulnerability were analyzed in Section 4.4.1. In Section 4.4.2, we report the results of the LG Smart TV analysis.

4.4.1 Methodology

For this analysis, we used the same architecture as outlined in Section 4.3.1. The computer that analyzed the issue was in between of the Smart TV and the Internet. Thus, we monitored the network traffic that was sent and received by the LG 32LF6309 Smart TV with Wireshark. We deployed Mitmproxy to manipulate data transferred on-the-fly, i.e. it was able to modify the content of transferred files.

4.4.2 Results

We found a request to LG's update servers that could be manipulated. The LG Smart TV requested a unencrypted resource with the URL `http://snu.leg.com/CheckSWAutoUpdate.laf` that responded with a XML file that included the firmware file (see Figure 4.6). We modified the response with Mitmproxy and the LG Smart TV downgraded to the version we specified in the XML response. Different possibilities exist to find a firmware that is outdated. In this case, the version was still available on the LG's update servers. Without a valid HTTPS connection the data is not secured against manipulation and can be changed in transit.

```
<RESPONSE>
<RESULT_CD>900</RESULT_CD>
<MSG>Success</MSG>
<REQ_ID>0000000000053900053603</REQ_ID>
<IMAGE_URL></IMAGE_URL>
<IMAGE_SIZE></IMAGE_SIZE>
<IMAGE_NAME></IMAGE_NAME>
<UPDATE_MAJOR_VER></UPDATE_MAJOR_VER>
<UPDATE_MINOR_VER></UPDATE_MINOR_VER>
<FORCE_FLAG></FORCE_FLAG>
<KE></KE>
<GMT>7 May 2016 13:16:40 GMT</GMT>
<ECO_INFO>01</ECO_INFO>
<CDN_URL></CDN_URL>
<CONTENTS></CONTENTS>
</RESPONSE>
```

```
<RESPONSE>
<RESULT_CD>900</RESULT_CD>
<MSG>Success</MSG>
<REQ_ID>0000000000053902082224</REQ_ID>

<IMAGE_URL>http://snu.lge.com/SWDownload.laf</
    IMAGE_URL>
<IMAGE_SIZE>698074204</IMAGE_SIZE>
<IMAGE_NAME>starfish -dvb-secured -m14tv -1.
    biscayne.m14tv -123-04.00.30-
prodkey_nsu_V3_SECURED.epk</IMAGE_NAME>
<UPDATE_MAJOR_VER>05</UPDATE_MAJOR_VER>
<UPDATE_MINOR_VER>00.30</UPDATE_MINOR_VER>
<FORCE_FLAG>Y</FORCE_FLAG>
<KE></KE>
<GMT>7 May 2016 13:28:59 GMT</GMT>
<ECO_INFO>01</ECO_INFO>
<CDN_URL>http://su.lge.com:80/GlobalSWDownloadCdn.
    laf?IMG=/201509/starfish -dvb-
secured -m14tv -1.biscayne.m14tv -123-04.00.30-
    prodkey_nsu_V3_SECURED.epk</CDN_URL>
<CONTENTS></CONTENTS>
</RESPONSE>
```

Left: Original XML response, Right: Manipulated XML response

Figure 4.6.: XML responses from the LG's update servers.

A downgraded firmware could recover vulnerabilities that were patched in newer version.

4.5 Further Results

We report on some vulnerabilities that we found while analyzing the Smart TVs. All of them cannot be exploited over the Internet. The attacker must be connected to the internal network or an additional device has to be connected to the Smart TV.

4.5.1 Attacker Model

The attacker model for the next privacy risk and security vulnerability comprises of internal attackers. Internal attackers are inside the local network. For example, devices that are controlled by other companies or software that is malicious could be internal attackers. We describe two different internal attackers:

- The attacker can record and manipulate any network traffic that is not secured. It can perform a man-in-the-middle attack and active attacks against the Smart TV.
- The attacker is directly connected to the Smart TV over HDMI. It cannot record network traffic. However, it could record data provided by the Smart TV over HDMI, e.g. audio or video. This attacker is often a device that is controlled by a company. A connection to the Internet is additionally established over Wi-Fi or LAN.

Figure 4.7 depicts both attackers that we considered.

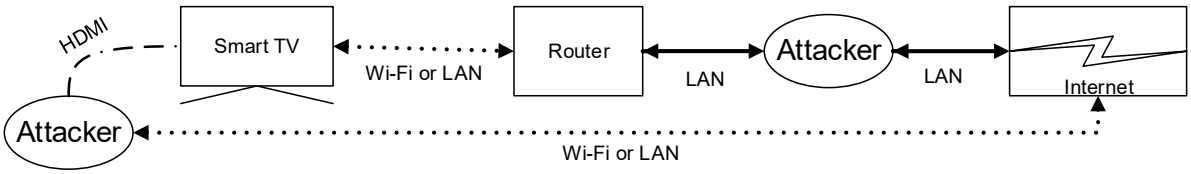


Figure 4.7.: Attacker model for the HDMI-ARC privacy risk and children protection vulnerability.

4.5.2 HDMI-ARC Privacy Risks

Most Smart TVs are equipped with one or more High-Definition Multimedia Interfaces (HDMI) with ARC (Audio-Return Channel) support. These interfaces are usually labeled as 'HDMI-ARC' or 'ARC'. The interfaces are specified in the HDMI specification [49]. ARC is a technique that enables HDMI devices to receive the audio signal of a Smart TV while the HDMI device outputs video and audio to the Smart TV. Connected HDMI devices could analyze the audio signal and guess the content that has been watched by the consumer remotely over the Internet. Thus, the vendors of such HDMI devices connected to the Smart TV can profile the consumer's viewing behavior. More details are reported from Neidig [24].

Methodology. The test environment is depicted in Figure 4.8. We connected the Smart TV's HDMI-ARC interface with an ARC splitter that extracted the audio signal that was sent over the ARC channel. The audio signal was then processed by the analyzing computer. The ARC splitter had a button to enable the extraction of audio. We analyzed how the Smart TV reacted to it and whether the consumer was notified. We tested the following Smart TVs with all available Internet updates: Samsung UE40JU6580 as well as the LG 32LF6309.

Results. If the ARC splitter was turned on, the Smart TV should deactivate the audio output with a consumer notification. The correct behavior could be shown on the LG Smart TV but not on the Samsung Smart TV. The Samsung Smart TV returned audio over ARC and the internal speakers of the Smart TV.

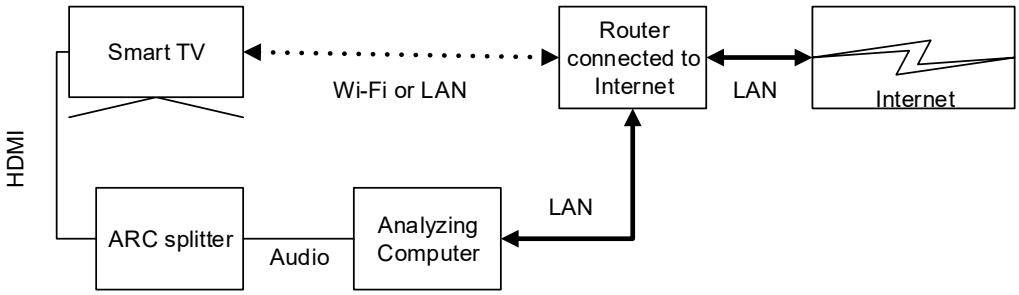


Figure 4.8.: Test environment for the HDMI-ARC vulnerability.

Therefore, it was possible for an external HDMI device to record the audio signal and process it and sent it over the Internet. The collected data could be used to profile consumers because audio data of TV channels revealed the viewing behaviors of consumers. As of now, we could not find a device that has already misused HDMI-ARC. To perform this test, we built up a test device that simulated an attacker.

4.5.3 Children Protection

Children protection on Smart TVs is important in order to protect children to watch inappropriate channels or use functionality that they are not allowed to. Furthermore, the functionality can also be used in show rooms where some functionality should be disabled or invisible for the customers.

While analyzing the UPnP functionality of the Samsung UE40ES6300 Smart TV, we found a vulnerability of the Smart TV that could be used to break the children protection.

Methodology. The analysis of the UPnP functionality was performed with Wireshark to monitor the network traffic and an UPnP browser that can be used to browse through the UPnP functionality of the Smart TV. First, all UPnP functionality was tested in order to produce traffic that could be captured by Wireshark. Then, some automated test scripts were written to exploit possible vulnerabilities.

Results. We found a vulnerability that was in the PIN code verification function of the Samsung Smart TV UE40ES6300. This UPnP functionality was not protected against unauthenticated requests and brute-force attacks. The PIN code had four digits. We developed a tool that brute-forced the PIN code of the children protection. We used a non-optimized approach to brute-force. We sent a maximum of 10.000 SOAP messages that were processed by the UPnP functionality of the PIN function. Each of the generated messages contained a different PIN code. Figure 4.9 shows the source code of our used script.

The script needs the library SOAPpy[4]. Once the Smart TV accepts the PIN code with an “OK” SOAP message we stop the execution and display the found PIN code. While attacking the Smart TV we did not see any reaction on the Smart TV. All Smart TV functionality could be used normally.

It was an implementation error since a PIN code should protect some functionality against unauthorized access. This vulnerability could be exploited in order to unlock the Smart TV, for example in show rooms or for inappropriate content for children.

A countermeasure would be to delay each attempt to enter the PIN code. It would lengthen the time needed to find the right PIN code. Additionally a notification on the Smart TV’s screen that has to be confirmed would make this attack unlikely.

[4] `https://pypi.python.org/pypi/SOAPpy`

```
from SOAPpy import SOAPProxy

namespace = "urn:samsung.com:service:MainTVAgent2:1"
url = "http://192.168.0.103:7676/smp_12_"
soapaction = "urn:samsung.com:service:MainTVAgent2:1#CheckPIN"

proxy = SOAPProxy(url, namespace=namespace, soapaction=soapaction)
proxy.config.debug = 0

for x in range(0,9999):
    while len(str(x))< 4:
        x="0"+str(x)
    output=proxy.CheckPIN(PIN=x)
    if not "NOTOK" in output:
        print x
        break
```

Figure 4.9.: Source code of the tool to brute-force the PIN code of the children protection.

4.6 Related Work

We report on security issues and vulnerabilities in the following two fields:
Vulnerabilities in using HTTPS. Niemietz *et al.* [50] showed in 2015 that HTTPS issues for some popular apps on Smart TVs such as Facebook existed. Lodge revealed that even voice recognition commands were transmitted in the clear without encryption [43]. Not only issues in implementing HTTPS correctly could cause severe privacy and security issues, also stolen or wrongly issued HTTPS certificates could lead to severe risks. Examples are stolen valid CA certificates to create new HTTPS certificates for known web sites [51] or Symantec issued fake Google SSL certificates [52]. If an attacker gets a valid certificate or gets the user to accept a wrong certificate, the attacker can collect sensitive data on a faked, so called phishing web site (see [53]).

Vulnerabilities in Smart TVs. Michéle *et al.* showed that an outdated and or unpatched media player is sufficient to gain access to any subsystem of the TV [11]. As an example for this issue, the Metro [12], an English online newspaper, reported that hackers filmed people having sex and they put the video on the Internet. Some other publications about vulnerabilities in Smart TVs have been published in the last years. Auriemma [54] reported a vulnerability where a Smart TV is not usable when it receives invalid data packets at a specific network port. More hacks for the underlying hardware or software were published by SeungJin researchers [55] and Mulliner and Michéle [14]. An overview and a notice from Kaspersky about security on Smart TVs can be found in [56]. Lately, ransomware infected LG Smart TVs [57].

4.7 Summary and Discussion

In this chapter we discussed different types of Smart TV security vulnerabilities that could cause privacy risks.

First, we presented our analyses that revealed severe issues in the implementation of HTTPS certificate validation in Samsung and LG Smart TVs. The web browsers of the Samsung Smart TV models UE55D6500, UE40ES6300 and UE46F6640 did not warn consumers that invalid HTTPS certificates were presented from our test web sites. In addition, HbbTV also did not validate HTTPS certificates correctly on the Samsung Smart TV models UE40D6200, UE55D6500, UE40ES6300, UE46F6640.

In 2012 as we started with our investigations, the consumers were not able to detect an invalid certificate delivered to these Smart TVs. We communicated this issue to Samsung in October 2012. The Samsung Smart TVs UE40ES6300 and UE46F6640 were patched in April 2014 by an online update. This patch changed the behavior so that consumers got a warning like the one shown in Figure 4.10.

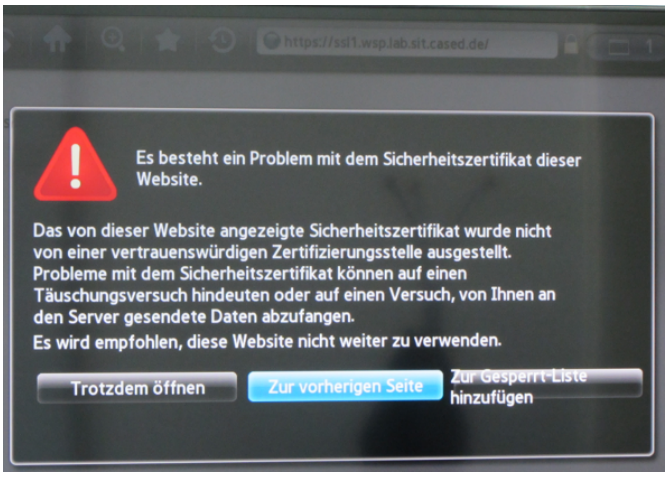


Figure 4.10.: Security warning on Samsung Smart TV UE40ES6300 (in German only).

This warning states that a problem with the HTTPS certificate has occurred. However, ignoring this warning by using the button *open anyway* (*Trotzdem öffnen*, left button) presented the web site as secure. The lock sign next to the address bar still did not indicate an invalid certificate. It is very important that the consumer is aware that these Smart TVs handle HTTPS connections that way.

The older Samsung Smart TV UE40D6200 had to be updated by USB. We were not aware of any online update for this Smart TV model or a communication to the consumers that gives information about the necessary USB update.

In our Samsung Smart TV UE40JU6580 and LG Smart TV 32LF6309 from 2016, we also found that HTTPS validation was on one HTTPS connection not correctly performed. We could not clarify if that issue could be exploited. However, the fact that there was an issue states that the implementation of HTTPS certificate validation was still not correct on some Smart TVs.

Wrongly implemented HTTPS certificate validation could lead to severe issues such as (1) illegitimate people are able to eavesdrop private data, (2) criminals could manipulate data, (3) criminals could manipulate Smart TV's firmware in order to harm the consumers, e.g. enable microphone unnoticed.

Second, we showed that it was possible to downgrade the LG Smart TV 32LF6309 to an older firmware. LG used an insecure HTTP connection to communicate with the LG's update servers. This issue could be used to install a vulnerable firmware version in order to misuse vulnerabilities that have been already patched in newer versions.

Furthermore, we showed that the HDMI-ARC functionality on Smart TVs could be misused to record viewing behavior of consumers when the HDMI device is malicious. The transmitted audio signal could be processed so that the watched content was revealed. Hence, profiling of consumers was possible over HDMI-ARC. The children protection was vulnerable on the Samsung Smart TV UE40ES6300. The corresponding PIN could be brute-forced.

Many issues on Smart TVs have already been patched. However, it is likely that more vulnerabilities are hidden and will be revealed in the future. This chapter impressively showed that security vulnerabilities in Smart TVs could have severe privacy risks for consumers. Hence, it is important that security updates are provided easily, e.g., updates via USB are not recommended for example. Furthermore, vendors

should test their Smart TVs for security and privacy risks since these devices affect a consumers' private lives.

5 Consumer Awareness and Attitudes

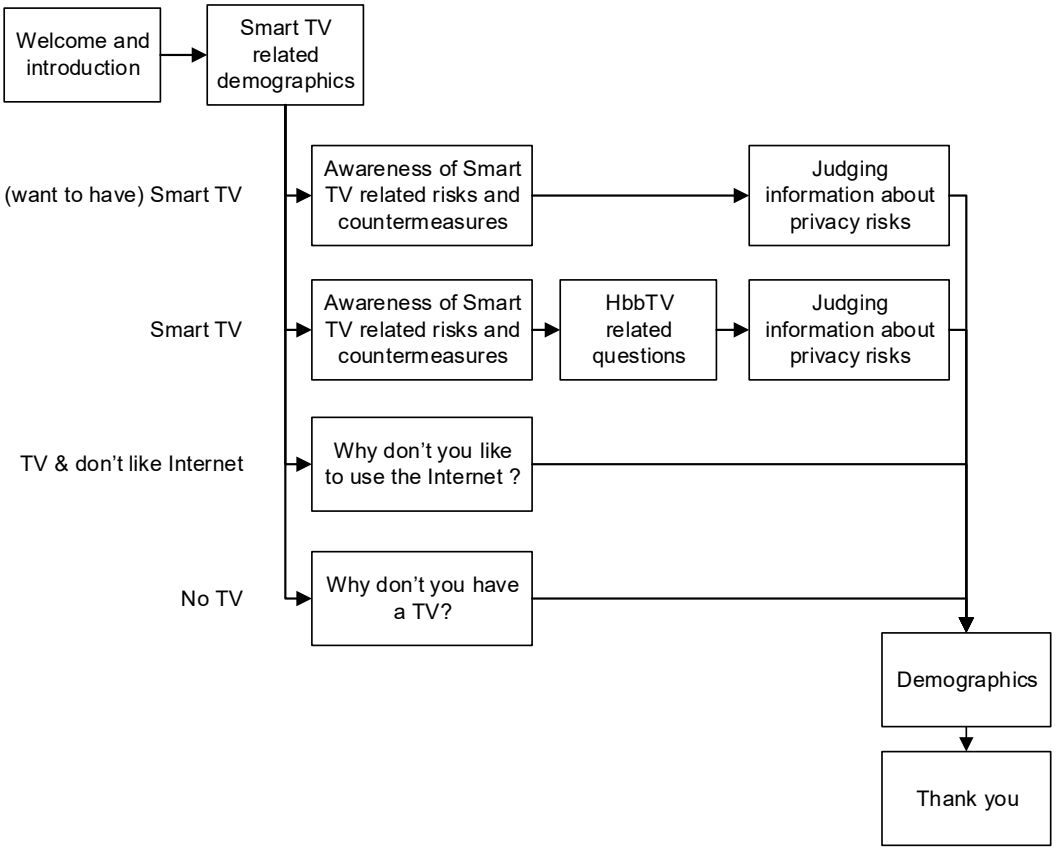
In this chapter, we discuss our research on consumers' awareness and attitudes towards Smart TV related privacy risks. In Section 5.1, we describe the methodology used. The results are presented in Section 5.2. We discuss our results in Section 5.3. Finally, we report on related work in Section 5.4 and summarize this chapter in Section 5.5. We published parts of this chapter in [25].

5.1 Methodology

We describe the study design in Section 5.1.1. The recruitment and ethics are presented in Section 5.1.2. In Section 5.1.3, we explain the evaluation methodology how we analyzed the participants' justifications.

5.1.1 Study Design

The study comprised seven phases that are depicted in Figure 5.1. The different paths depended on the responses the consumer gave in the *Smart TV related demographics* phase. Note, all questions and texts were translated into English. The original German questionnaire can be found in the Appendix C.



The texts represent the paths' names: (want to have) Smart TV, Smart TV, TV & don't like Internet and No TV.

Figure 5.1.: Study design of the online survey researching consumer awareness and attitudes.

These phases were as follows:
Welcome and introduction. First, participants were informed that the survey focuses on Smart TVs. They were not briefed about the exact focus of the survey as not to prime their responses. Information about the duration was provided, as well as the fact that there are no wrong answers. They were told that they could leave the survey at any point (only completed surveys earned the participant a monetary reward).

Smart TV related demographics. Participants were presented an information what a Smart TV is and they were asked whether they own a TV. Those who responded that they do not own a TV where asked for the reasons. Those who stated that they own a TV were asked whether their TV is a Smart TV. Those who did not own a Smart TV were asked whether they would like to have a Smart TV. Those who answered that they own a TV and do not want to use the Internet were asked about the reasons. Both, participants who do not own a TV or own a TV and do not like the Internet were forwarded to the *Demographics* phase immediately after the questions for the reasons.

Awareness of Smart TV related risks and countermeasures: Those who owned a Smart TV and those who do not (yet) own a Smart TV but would like to use the Internet on their TV were asked to tell us about privacy risks of Smart TVs they are aware of. Afterwards, they were asked to list countermeasures for those risks they mentioned.

HbbTV related questions: Those who owned a Smart TV were presented an information what HbbTV is and were asked whether they have already seen HbbTV notifications on the Smart TV's screen. We presented different pictures (see Figure 5.2) of HbbTV notifications, so that even participants that did not know HbbTV by name could answer the questions.

Afterwards, they were asked whether they know where those HbbTV notifications came from (Internet or antenna/cable). Then, we asked for privacy risks of HbbTV. Last, we asked whether they know how to disable HbbTV.

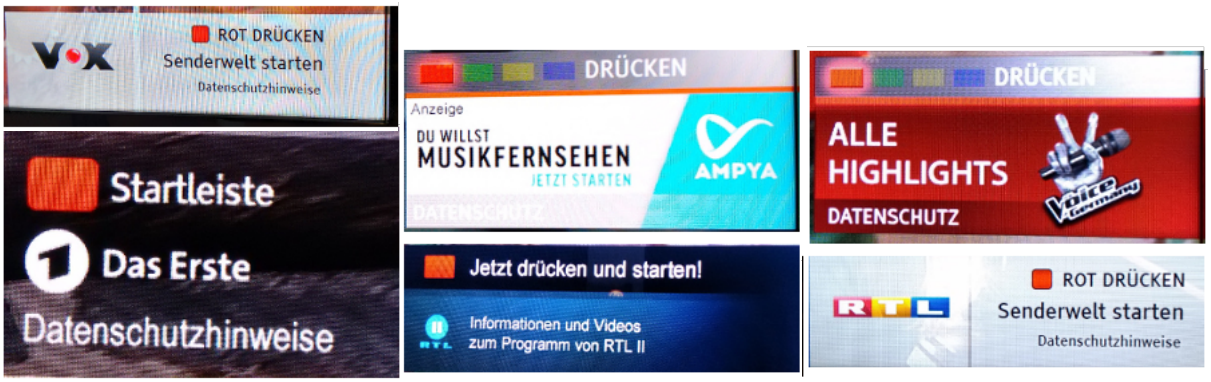


Figure 5.2.: HbbTV screenshots for the participants of the consumer awareness and attitudes study.

Judging information about privacy risks. Those participants that own a Smart TV or would like to have a Smart TV were given four different types of privacy risk scenarios to consider, one per page, in random order. For each, participants were asked to judge how critical it was with respect to privacy. Options ranged from 1 'not very critical' to 3 'neutral' to 5 'very critical'. The option 'don't know' was also available. They were asked to justify their ratings. The request for justification appeared on the same page as the scenario description. The scenarios were identified based on the privacy risks revealed in Chapter 3 and Chapter 4:

- The channel you watch gathers information about how long, and how often, you watch the channel. If a broadcaster offers multiple channels (e.g., Sat. 1 or Pro Sieben), it is possible that the information from different channels is combined.
- The Smart TV vendor gathers information about how you use the TV. For example, the vendor gets detailed information about which apps you use. Furthermore, it gathers information about how long, and how often, you use your TV.
- You can control your Smart TV with your voice. Your voice data is transmitted to, and analyzed, by the vendor's servers. It is entirely possible for other conversations in the room to be transmitted to the vendor's server for processing too.
- Your Smart TV is equipped with a microphone. Criminals can gain access to the Smart TV and can activate it and listen to all the conversations in your living room. You do not realize this.

Demographics. Participants were asked to provide information about gender and age.

Thank you. Finally, we thanked participants for their support and they received information on how to claim their monetary reward.

5.1.2 Recruitment and Ethics

The study was conducted in Germany in December 2015. SoSciSurvey[1] was used as platform for the survey. The participants were recruited via clickworker[2], a company paying people for doing small tasks, which is similar to Amazon Mechanical Turk but recruits in Germany instead of the USA. We paid each participant who completed the survey, and did not provide obvious nonsense answers, € 2 per participant on that platform. We estimated the right amount in the following way: we measured the average time with test participants. This was about twelve minutes. As Germany has a minimum wage of € 8.50 per hour € 2 was fair payment.

Guidelines on *ethical issues* regarding research involving humans are provided by the Technische Universität Darmstadt[3]. These guidelines were followed with respect to respondent consent and data privacy requirements were met. Participants first read an information page on which they were assured that their data would not be linked to their identity and that the responses would only be used for study purposes. Furthermore, using SoSciSurvey ensured that data was stored in Germany and thus subject to German data protection law. They were told that they could withdraw at any time. Moreover, they were told that all answers were valid: there was no such thing as a wrong answer.

5.1.3 Evaluation Methodology

An open-coding approach was used for all free text answers by the participants, i.e., we proceeded in the following way:

First, two researchers (the author of this work and another researcher) analyzed the free text answers independently and composed a list of codes. Furthermore, they clustered these codes in categories. Afterwards, the categories were discussed and the researchers agreed on one list of categories as well as a mapping from codes to category.

These codes were afterwards applied to the free text answers by the two researchers. It was possible to assign one answer to several categories. Then, the assignments were compared and discussed to agree on the codes to be assigned.

[1] http://www.soscisurvey.de
[2] http://www.clickworker.com/
[3] https://www.intern.tu-darmstadt.de/gremien/ethikkommisson/index.de.jsp

5.2 Results

We present the sample in Section 5.2.1. Section 5.2.2 reports on how aware consumers of Smart TV related privacy risks and countermeasures were. In Section 5.2.3 we show the results about the HbbTV related questions. The ratings of each scenario are shown in 5.2.4. The results of the ratings' justifications are reported in Section 5.2.5.

5.2.1 Sample

200 participants completed the survey. Eight were removed from the data set since they entered implausible values (e.g. data and rating did not match, empty free text fields all over the place). The survey group consisted of 104 females (54%) and 87 males (45%); one (1%) did not provide gender. The youngest participant was 19, the oldest 89 and the mean age was 38.9 years with a standard deviation of 12.41.

	total	**female**	**male**
# of participants	192*	104 (54%)	87 (45%)
# of participants own a TV	178*	98 (55%)	79 (44%)
# of participants own a Smart TV	127*	70 (55%)	56 (44%)
# of participants own a non-Smart TV	51	28 (55%)	23 (45%)
# of participants own a Smart TV or want to have a Smart TV	171*	97 (57%)	73 (43%)

Table 5.1.: Sample of consumer awareness and attitudes study.

* One did not provide gender

14 participants (7%) indicated that they did not own a TV. Participants selected the following reasons for their non-ownership: not interesting (7 participants), too expensive (3), no time to watch TV (2) and want to buy a TV (2). Four participants selected the option 'other reason' and explained:

> *"I watch online", "I can watch online", "bad for children", "no space for a TV".*

Out of the 178 remaining participants who owned a TV, 127 (71%) had a Smart TV and 51 (29%) owned a non-Smart TV. 44 (86 %) of those who did not own a Smart TV would like to have one but 7 (14%) did not. They gave the following reasons:

> *"too complicated", "it's too insecure", "using a laptop is more comfortable and easier", "it's unnecessary. Laptops are sufficient.", "it's too insecure from a privacy perspective", "I favor an external solution such as Apple TV that can be separately upgraded and replaced.","Have enough other devices.".*

A summary of the presented numbers is shown in Table 5.1. All participants who owned a Smart TV and those who wanted to have a Smart TV (171 participants) were considered for the main part.

5.2.2 Level of Awareness

We report on the privacy risks and countermeasures that were mentioned by the participants.

Mentioned privacy risks. We assessed whether participants knew about Smart TV privacy risks and which potential risks participants were aware of. In total, 60 individual text fields for risks were filled

by participants. The average number of risks per participant that mentioned at least one risk was 2.14; overall 0.16. 28 (16%) participants mentioned at least one risk. The summarized numbers are in Table 5.2.

	total	female	male
# participants asked for risks	171	97 (57%)	73 (43%)
# participants mentioned at least one risks	28	11 (39%)	17 (61%)
# risks mentioned	60	19 (32%)	41 (68%)

Table 5.2.: Number of participants that were asked for risks, that mentioned at least one risk, and the number of mentioned risks in total.

Next, we analyzed the 60 free text responses in terms of two aspects: 'potential actions' or 'consequences' of a risk (see Table 5.3). While analyzing these responses, we found that most participants that mentioned risks were describing the risk with potential actions. A potential action does not describe the consequence of a risk, but the action that could be performed on the Smart TV or with the data of the Smart TV. A consequence is a disadvantage or harm to consumers that could be caused by the risk. We distinguish between potential actions and consequences since the likelihood, for those participants that mentioned consequences, to take informed decisions is higher.

	total
Collecting Data	19
Access to Camera or Microphone	17
Access to Sensitive Data	4
Access to Network	3
TV Manipulations	2
# of participants	21

(a) Risks assigned to 'potential actions'.

	all
Personalized Advertising	7
Being Robbed	3
TV getting too slow	2
Child watches inappropriate content	2
TV does not work	2
Program could Change	1
# of participants	12

(b) Risks assigned to 'consequence'.

Table 5.3.: Aspects of privacy risks

The most often mentioned potential actions were 'Collecting Data' (19 participants) and 'Access to Camera or Microphone' (17). The other categories were 'Access to Sensitive Data' (4), 'Access to Network' (3), and 'TV Manipulations' (2). These aspects were mentioned by 21 participants.

The most often mentioned consequences of privacy risks were 'personalized advertising' (7) and 'being robbed' (3). The others were: 'TV getting too slow' (2), 'Child watches inappropriate content' (2), 'TV does not work' (2) and 'program could change' (1). These consequences were mentioned by 12 participants.

The results, both quantitative and qualitative, confirmed a general lack of awareness of privacy risks thereof.

Mentioned countermeasures. We assessed whether participants knew about countermeasures and which they were aware of. 22 (13%) participants mentioned at least one countermeasure and 42 countermeasures were mentioned in total. The average mentioned countermeasures per participant for those

who mentioned at least one was 1.95; 0.25 for all asked participants. The summarized numbers are presented in Table 5.4.

	total	female	male
# participants asked for countermeasures	171	97 (57%)	73 (43%)
# participants mentioned at least one countermeasure	22	5 (23%)	17 (77%)
# countermeasures mentioned	42	10 (24%)	32 (76%)

Table 5.4.: Number of participants that were asked for countermeasures, that mentioned at least one, and the number of mentioned countermeasures.

The mentioned countermeasures were: anti-virus scanner (10), firewall (9), disable Internet or disconnect device (7), disable camera/microphone (4), regular updates (3), disable other functions (e.g. motion sensor, updates) (3), protection software (2), child protection (1) and others (3).

The results confirmed a general lack of awareness of countermeasures for Smart TV related privacy risks.

5.2.3 HbbTV Results

The questions about HbbTV were answered only by participants that owned a Smart TV. Thus, 127 participants completed this phase.

56 (44%) participants said that they have seen HbbTV notifications on their Smart TV; 27 (21%) participants responded that they might have seen the HbbTV notification, but were not sure.

73 (58%) participants did not know whether the HbbTV notifications were received from the Internet or over the antenna/cable signal. 8 (6%) participants thought the HbbTV notifications were provided over the TV signal and not over the Internet.

87 (63%) participants did not know whether HbbTV causes any privacy risks. 13 (9%) participants mentioned that it could not have any privacy issues. Those of them who gave reasons said that it would be forbidden by law.

115 (91%) out of the 127 asked participants did not know how to disable HbbTV.

A general lack of understanding of the HbbTV functionality were confirmed. Participants were not aware that HbbTV could be deactivated.

5.2.4 Risk Scenario Ratings

We analyzed how critical participants rated the displayed privacy risk scenarios (see Section 5.1.1 for the description of the scenarios).

Table 5.5 provides, for each scenario, (1) the number of participants who answered 'I don't know', (2) the number of participants considered[4], (3) the mean value how critical the scenario is rated (available options were: from 1 'not very critical' to 3 'neutral' to 5 'very 'critical' and the option 'don't know') for all participants, all female/male participants, as well as those mentioning/not mentioning risks in the previous part of the survey. The 'broadcaster profiling' scenario was considered by most of the participants as the less critical one (light gray) and the 'surveillance audio' one as the most critical one (dark gray).

[4] Note, the total numbers differ as the number of people who answered 'I don't know' may differ as well as those who were set to 'not using' differs from scenario to scenario.

Scenario	I don't know	all	female	male	Risks	No Risks
Broadcaster Profiling	4	2.82 (164)	2.66 (95)	3.06 (68)	3.19 (27)	2.74 (137)
Vendor Profiling	2	3.46 (168)	3.52 (95)	3.42 (72)	3.50 (28)	3.45 (140)
Voice Recognition	10	3.97 (159)	3.99 (91)	4.00 (67)	4.07 (27)	3.95 (132)
Surveillance Audio	4	4.69 (166)	4.75 (95)	4.67 (70)	4.64 (28)	4.70 (138)
Total	20	3.74 (657)	3.73 (376)	3.79 (277)	3.85 (110)	3.71 (547)

most critical is filled dark gray and least critical light gray

Table 5.5.: Criticality rating of the scenarios.

5.2.5 Consumer Attitudes

In total 684 free text answers for the justifications, with more than 7,200 words, were examined using an open coding approach (see Section 5.1.3 for an explanation). We identified factors that potentially impact the consumer attitudes and therefore the ratings related to privacy risks. The different factors are explored in the following paragraphs:

Party who gathers the data is likely to be an influential factor because many participants consider vendors and broadcasters collecting data to be acceptable: e.g. "*Vendor may take the data as long as there is no abuse*", "*I consider broadcasters to be secure*". However, criminals would use data to harm them ("*On top of that there is a danger of data being abused by criminals*").

The **type of data** is also likely to be an influential factor. Some participants were not worried about the described privacy risk as they considered the addressed usage data to be unimportant, i.e. not worth protecting as compared to other types of data: "*Don't care about usage data*", "*Inspection of usage data is relatively uncritical as long as there is no inspection of personal data such as Skype conversations*", "*Don't mind as long as they don't have access to personal data such as passwords or banking details*", "*Inspection of usage data seems uncritical*","*I don't care about usage data*", "*The danger of abuse is minimal*", "*Information about my usage behaviour can be passed on*".

Being aware that usage data collection constitutes a privacy risk might have an influence or not. Some participants see no disadvantages ("*There is no disadvantage for me", "I think it has no negative effects on me*") or only consider the advantages to vendors and broadcasters of collecting and analyzing usage data:

- More reliable viewing figures: "*At least better than faked viewing figures*", "[..] *I don't really like it, but, on the other hand, it would be a real improvement in viewing figures*"

- Better products: "*Usage data is required in order to improve products*", "*It is important to support future development, because you can see which applications are used frequently and which not*".

On the other hand, other participants consider any collection of (usage) data a privacy invasion ("*I totally decline any data-gathering*", "*violates my privacy*", "*very bad, would violate my privacy a lot. If this*

happened,I would not feel very comfortable".) as well as with terms like surveillance ("*I don't want to be kept under surveillance*") and profiling ("*you can create a user profile*").

Even when they are aware of a privacy risk, **being aware of possible misuses** might have an influence. Those who are aware of possible misuse mentioned different types of misuse:

- Vendors generally misuse the data: "*data can be abused*", "*my voice could be used without my knowledge*". Note, the last quote actually addresses an interesting aspect: '*without my knowledge*'. However, this aspect was only mentioned very rarely.

- Vendors sell data: "*It is critical; I don't want the vendor to sell my data. It is a private affair*".

- Burglary: "*It invades definitely my privacy, no one may want that. Burglars can check if someone is at home or not. If yes, they can burglarize or check if burglary would be worth at all on the basis of information obtained . If that isn't critical enough, I don't know...*".

- Close a Deal: "*With my voice someone could fake phone calls to confirm orders or contracts. In addition, there is a risk that not only commands to the Smart TV are recorded, but also private or business conversations are recorded*".

- Espionage: "*I would feel spied on*", "*It isn't ok if I, as a customer, am spied on in this way. The legislature must do something*".

Most of these were only mentioned by one or two participants.

Considering **personalized advertising as beneficial** or **irritating** seems to be an influencing factor:

- Some like personalized advertising since it suggests items of interest: "*I'll benefit from the analysis of my usage behaviour as they provide me with tailored advertisements and special programmes for me personally*".

- Others consider this to be a nebulous attempt to misuse their data: "*Could be evaluated for personalized advertisement and programs -> data may be sold to other companies in the media group*".

People's **general privacy attitudes** may also have an influence. Those participants who have a negative attitude towards any type of privacy violation are, in general, more motivated to complain. Those who are more difficult to motivate are those that:

- use the 'nothing to hide' argument: "*I don't talk about important things I need to be concerned about*", "*There is nothing I have to hide*",

- have become accustomed to privacy risks: "*nowadays it is normal*" , "*You don't have to like it, but in a way it has been wildly implemented for some years now, hasn't it?*", "*It's the same problem with computers. If anybody wants to be a criminal, there will always be a way*", "*On the internet via computer or smartphone data is saved as well*"

- think it is unavoidable : "*You can't change it*",

In summary, the following factors influence consumer attitudes: the party who gathers the data; the type of data; awareness of the fact that (usage) data is collected; being aware that collected data can be misused; personalized advertising being considered beneficial, or not; basic attitudes.

5.3 Discussion

We had anticipated a general lack of awareness. Our study confirmed this. Only a small amount of participants in the study mentioned privacy risks and named concrete consequences of privacy risks. Additionally, consumers were not aware of countermeasures. Namely, they did not mention to disconnect the Smart TV in order to protect against privacy risks.

Furthermore, 44% of the asked consumers stated that they have seen HbbTV on the Smart TV. We revealed privacy risks of HbbTV in Chapter 3. However, only a very small number knew how to disable this functionality. Most of them did not know any privacy risks of HbbTV.

Participants rated the broadcaster profiling scenario as the less critical scenario although broadcaster could collect sensitive usage data that could be used to build profiles of consumers. We conclude that it is necessary to start consumer awareness-raising measures in order to enable consumers to decide whether to take the privacy risks or not.

In order to develop awareness-raising measures, we deduced factors that influence consumers' attitudes. With those factors we could develop awareness-raising messages that are likely to make consumers aware, change attitudes and thus bring consumers to think about their privacy protection.

Limitations. The study was conducted in Germany, where the population tends to be more attuned to privacy risks than citizens of other countries [58]. A study with Americans, for example, might well deliver different levels of awareness.

This study relied on self-report. We do not know whether expressed concerns were genuine nor do we know whether they actually act in a way that aligns with their concerns. Since participants were anonymous it is hard to see that many would feel the need to disseminate or to fabricate responses.

We tailored the survey to reflect the privacy risks found in Chapter 3 and 4. Different scenarios might well have revealed a different set of consumer attitudes and influential factors thereof.

5.4 Related Work

We are not aware of any work that researched levels of awareness or attitudes towards Smart TV related privacy risks. However, we report on works in related fields.

Mental models can influence people's attitude, so we list some work in this field. Mental models in the context of privacy and security have been studied from Camp [59], Dourish *et al.*[60] and Wash [61] as well as in different concrete areas, such as smartphones from Ophoff *et al.*[62], Volkamer *et al.*[63], Harbach *et al.* [64] and Elie [65], network security from Solove[66], firewalls from Raja *et al.* [67], secure communication from Friedman *et al.* [68], passwords from Weirich *et al.* [69], single sign on Gupta *et al.* [70], anonymous credentials from Wäslund *et al.* [71] and Harbach *et al.* [72], privacy settings from Debatin *et al.* [73], email encryption from Gaw *et al.* [74], Renaud *et al.* [75] and Clark *et al.* [76]. In these areas, security and privacy protection tools are increasingly available. The focus of these papers differs from this work, since the mental models of people should help to understand why the existing tools are not used. We tried to explore how consumers think about Smart TV related privacy risks in order to establish effective protection measures. However, there are parallels. Some reasons for not using security tools might be reasons that consumers do not complain if corresponding tools are not available or vendors and broadcasters collect usage data intentionally.

Asplund *et al.* [77] published that there is a lack of consensus on risks related to IoT (Internet of Things) security in critical societal services. We found the same issue in the Smart TV area.

5.5 Summary

In this chapter, we analyzed whether consumers were aware of Smart TV related privacy risks and any countermeasures. Further, we wanted to understand consumers' attitudes towards these privacy risks in order to deduce the influential factors that could be used to evaluate potential awareness-raising messages. We conducted an online survey with 200 participants to carry out this research. For our results, we only considered participants that owned a Smart TV or would like to own a Smart TV. Hence, 171 participants finished the main part of the survey. The results were:

- The study confirmed a general lack of awareness of risks. Only 28 of the 171 (16%) participants mentioned a privacy or security risk in their responses and only 12 (7%) were able to name concrete consequences of risks.
- The study confirmed a lack of knowledge and awareness of countermeasures. Only 22 of the 171 (13%) participants mentioned at least one countermeasure.
- Those participants that owned a Smart TV (127 participants) were asked several HbbTV related questions. Although we revealed severe privacy risks of HbbTV in Chapter 3, most participants did not know how to disable HbbTV in the Smart TV settings. Out of 127 asked participants only 11 (9%) knew how to disable it.
- Participants rated the surveillance scenario that states that a criminal can access the Smart TV's microphone as the most critical. The less critical rated scenario is the one that explains that broadcasters can profile consumers. However, as we revealed in Chapter 3 Smart TV consumers are exposed to the second privacy risk at a daily basis, whereas the probability that the first scenario happens is very low.

Based on the consumers' attitudes, we deduced factors that can be used to develop awareness-raising messages in order to make consumers more aware and therefore value their privacy. The following factors influence consumer attitudes:

- the party who gathers the data,
- the type of data,
- awareness of the fact that (usage) data is collected,
- being aware that collected data can be misused,
- personalized advertising being considered beneficial, or not,
- and basic attitudes.

These factors are further evaluated in the next chapter.

6 Evaluating Messages

In the previous chapter, we confirmed a general lack of awareness of Smart TV related privacy risks and isolated factors that influence consumers' attitudes. In this chapter, we discuss our evaluation of a range of awareness-raising messages respecting the isolated factors in order to raise awareness towards Smart TV related privacy risks. We conducted an online study to research it.

We describe the methodology of the study in Section 6.1. The results are presented in Section 6.2. The discussion of the results is presented in Section 6.3. Finally, we summarize the chapter in Section 6.4. Note, this chapter serves as a pre-study for Chapter 7.

6.1 Methodology

We describe the study design in Section 6.1.1. The recruitment and ethics are presented in Section 6.1.2. In Section 6.1.3, we explain the evaluation methodology how we analyzed the participants' justifications.

6.1.1 Study Design

We designed the study as outlined in Figure 6.1. Note, the study was conducted in Germany and questions and quotes in German were translated. The original German questionnaire can be found in the Appendix D.

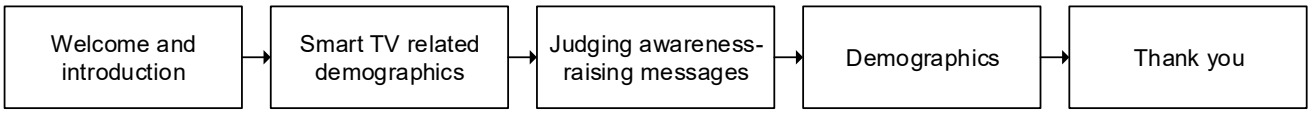


Figure 6.1.: Study design of the evaluating messages study.

The study comprised the following five phases:
Welcome and introduction. First, participants were informed that the survey focuses on Smart TVs. They were not briefed about the exact focus of the survey as not to prime their responses. Information about the duration was provided, as well as the fact that there are no wrong answers. They were told that they could leave the survey at any point (only completed surveys earned the participant a monetary reward).

Smart TV related information. Participants were presented an information what a Smart TV is and they were asked whether they own a TV.

Judging awareness-raising messages. Participants were given six messages to consider, one per page, in random order. For each, participants were asked to judge how critical the described situation was considered (i.e. how much reading this makes them worrying). Options ranged from 1 'not very critical' to 3 'neutral' to 5 'very critical' and the option 'I don't know'. Additionally, a mandatory free text field to justify the rating was provided. Participants were given the following messages:

- **Vendor & Broadcaster - Usage Data.** The Smart TV vendor and the broadcaster gather and analyze information about how, and how often, you use your Smart TV.
- **Vendor & Broadcaster - Personalized Advertisement.** The Smart TV vendor and the broadcaster gather information about how, and how often, you use your Smart TV. *This information is analyzed to deliver personalized advertisements directly to your TV screen.*

- **Vendor & Broadcaster - Usage Data & Harm.** The Smart TV vendor and the broadcaster gather and analyze information about how, and how often, you use your Smart TV. *It cannot be ruled out that the gathered information ends up in the wrong hands and abused in order to harm you.*

- **Vendor - Audio Stream & Harm.** The microphone of your Smart TV is always on in order to allow you to control your Smart TV with voice commands. Thus, the vendor has access to any conversation in the room. *It cannot be ruled out that the information ends up in the wrong hands and misused in order to harm you.*

- **Criminals - Audio Stream & Harm.** Smart TVs without security measures are more vulnerable to attack than laptops or smartphones. If you connect your TV without security measures, it may be possible for a hacker to gain access to your Smart TV and to enable the microphone without you realizing. *Thus, the hacker can collect audio stream data and potentially harm you.*

- **Criminals - Audio Stream & Burglary.** Smart TVs without security measures are more vulnerable to attack than laptops or smartphones. If you connect your TV without security measures, it may be possible for a hacker to gain access to your Smart TV and to enable the microphone without you realizing. *Thus, the hackers could figure out the best time to burglarize you.*

We developed the messages based on our analysis of consumer attitudes in Chapter 5.2.5. The factors that we isolated are summarized in Figure 6.1. We could not combine all possible factors and options since the amount of scenarios would be too large. We decided for the above mentioned one.

Factor	Options
Party who gathers the data	Broadcaster, Vendor, Criminals
Type of Data	Usage Data, Audio Stream
Consequences	no (gathered/analyzed), misuse, specific (e.g. personalized advertising, burglary)

Table 6.1.: List of identified factors.

General demographics. We asked the participants about gender and age.

Thank you. Finally, we thanked participants for their support and they received information on how to claim their monetary reward.

6.1.2 Recruitment and Ethics

The recruitment process was similar to the one described in Chapter 5.1.2. This survey was also conducted on SoSciSurvey in Germany in March 2016. The participants were recruited via clickworker. We paid each participant who completed the survey and who did not provide obvious nonsense answers €1.80. For ethical compliance see Chapter 5.1.2 as the same held for this study.

6.1.3 Evaluation Methodology

An open-coding approach was used for all free text answers by the participants. We proceeded in the same way as described in Chapter 5.1.3.

6.2 Results

We present the sample in Section 6.2.1. Section 6.2.2 reports the ratings of the awareness-raising messages and a comparison thereof. Based on the justifications of the ratings, in Section 6.2.3 we analyzed why some ratings were not as expected.

6.2.1 Sample

175 participants completed the survey. 24 participants were removed from the data set since they entered implausible values (e.g. justification and rating did not match, empty free text fields). The survey group consisted of 68 females (45%) and 82 males (54%); 1 (1%) did not provide gender. The youngest participant was 18, the oldest 70 and the mean age was 36.95 years with a standard deviation of 12.16.

73 participants (48%) indicated that they own a Smart TV. 151 participants completed the survey with the questions about the messages.

6.2.2 Ratings of the Awareness-Raising Messages

For each message we calculated the mean rating excluding those participants who answered 'I don't know'. We provide the numbers in Table 6.2. Over all messages, 'I don't know' was selected 51 times. 33 participants selected 'I don't know' at least once. Most of the selections were observed in the 'Criminals - Audio Stream & Harm' message.

Message	Considered participants	I don't know	Mean rating (M)	Standard deviation (SD)
Vendor & Broadcaster - Usage Data	143	8	3.22	1.44
Vendor & Broadcaster - Personalized Advertisement	146	5	3.16	1.41
Vendor & Broadcaster - Usage Data & Harm	142	9	3.64	1.28
Vendor - Audio Stream & Harm	142	9	4.15	1.16
Criminals - Audio Stream & Harm	136	15	4.08	1.15
Criminals - Audio Stream & Burglary	146	5	4.08	1.18

Table 6.2.: (Not) considered participants, mean ratings and the standard deviation of the evaluation of the awareness-raising messages.

The most critically rated message was "Vendor - Audio Stream & Harm" and the lowest rated one was "Broadcaster & Vendor - Personalized Advertising". We performed χ^2-tests to compare the ratings of the messages. Note that 'I don't know' answers were discarded. The preconditions for χ^2-tests were met: the variable was categorical (1 'not very critical' to 3 'neutral' to 5 'very critical'), the expected frequency count for each rating was at least 5. For all tests, we considered the following hypotheses
H_0 = there is no significant rating difference between both tested messages m_1 and m_2 and
H_a = there is a significant rating difference between both tested messages m_1 and m_2.

There was no significant difference between the "Broadcaster & Vendor" messages "Usage Data" (M=3.22; SD=1.44) and "Personalized Advertising" (M=3.16; SD=1.41); χ^2=1.587, df=4, p=0.811.

The statistical comparison of the "Broadcaster & Vendor" messages "Usage Data" (M=3.22; SD=1.44) and "Usage Data & Harm" (M=3.64; SD=1.28) did not show a significant difference; χ^2=10.825, df=4, p<0.05.

"Usage Data & Harm" (M=3.64; SD=1.28) message compared with "Vendor - Audio Stream & Harm" (M=4.15; SD=1.16) were significantly different; χ^2=14.498, df=4, p<0.05.

The messages "Vendor - Audio Stream & Harm" (M=4.15; SD=1.16) and "Criminals - Audio Stream & Harm" (M=4.08; SD=1.15) were not significantly different; χ^2=6.630, df=4, p=0.157.

The statistical test between both "Criminals" messages "Criminals - Audio Stream & Harm" (M=4.08; SD=1.15) and "Criminals - Audio Stream & Burglary" (M=4.08; SD=1.18) showed no significant difference; χ^2=2.011, df=4, p=0.734.

Note that no significant rating differences in each scenario emerged between males and females.

Figure 6.2.: Graphical overview of results.

A summary of the results is depicted in Figure 6.2. Equality means that we did not found significant different level of criticality, thus on average, participants were neither less nor more worried about both privacy risks. The less than sign shows that we found a significant smaller level of criticality.

6.2.3 Analysis of Messages.

In order to find out why the last messages did not significantly differ in the consumer rating, we analyzed the free-text responses related to these three messages. In total, 453 free text answers with more than 6,800 words were examined using the above mentioned open coding approach (see Section 6.1.3). We tried to find justifications that explains the equality of these messages. To do so, we assigned the following themes to the justifications, give for each theme some example quotes and show the amount of consumers assigned to each theme in Table 6.3:

No Harm. Participants could not imagine any harm audio stream data could cause:

> *"I don't see how one could harm me.", "I don't think that a hacker could gather much information from the microphone that could harm me".*

Not me. Participants thought the issue could happen but not to him/her:

> *"It would be possible, but it is unlikely that it would happen to me", "Microphone isn't used. TV is only used in the evening when no conversations are engaged in", "I'm not important enough for someone who wants to harm me", "I don't think that a hacker would compromise my TV.[...]", "Hackers are everywhere and scare every Internet user. A critical issue. But, I always assume that it won't happen to me".*

Nothing to Hide. Participants mentioned that they did not have anything to hide:

> *"Large-scale harvesting of such data wouldn't make much sense. Even if the conversations I have in my living room are published no severe harm could result."*.

Trust in Vendor. Participants thought that the vendor would not misuse this data and protect their Smart TVs properly:

> *"Not that critical, because I have a basic trust to the TV vendors. I think it's likely, since the function is implemented in Smart TVs.", "I don't rule out that it can happen, but I try to trust the vendor.","Cannot imagine that a vendor would do this. The vendor has no information that is important to me."*.

High Effort. Participants considered the effort required for an invasion to be unrealistic:

> *"Technical effort is too high to make abuse likely", "Required technical effort is too high. Protection software should help [to reduce the risk]", "I think it would be too much effort for a burglar", "Very high effort for something that could be achieved more easily"*.

Have not heard of that. This was the first time participants had heard about the described issue and they might have needed time to process the idea:

> *"I am aware that it could happen, but haven't heard of that possibility before", "So far, I haven't heard of such methods", "I don't know if such cases exist. However, it could quickly become very critical"*.

Hackers aren't Burglars. Some participants seemed to think that hackers operate differently from traditional burglars:

> *"Hackers usually don't burgle. They earn their money in other ways", 'Normally, hackers aren't burglars. They enrich themselves digitally, for example by using credit card data, instead of hacking into a Smart TV", 'A very unlikely scenario. Competent hackers would probably prefer to carry out credit card theft"*.

General Unease. Participants declined the scenario but did not provide concrete reasons for doing so:

> *"This risk is real and is unacceptable", "An absolute 'no go' that such vulnerabilities exist. At the moment I think it's unlikely"*.

Lack of Security/Privacy. Participants thought there was a paucity of security or privacy measures:

> *"The risk exists but who wants to listen to boring chit-chat for hours in order to find something important", "One can take precautions","Most vendors save money by not spending on protection measures for their devices. Hackers are years ahead and the need for economy does make the TVs"*.

Surveillance. Participants felt that they were under surveillance:

> *"No Smart TV without additional protection measures! This surveillance could be automated, stored and analyzed", "I do not want to be under surveillance", "The era of surveillance should be over. However, it's likely that a provider will use all channels to learn more about their customers", "I don't like my microphone to be on all the time"*.

Deactivate Feature Participants thought that they could deactivate the microphone as a sufficient precaution:

> *"I don't use voice control with my Smart TV and therefore have not activated the microphone", "Microphone is permanently off", "I don't need voice control. Thus, I wouldn't turn on the microphone"*.

It is possible. Participants considered the described issue to be feasible:

> *"Any mechanism can be used to spy on the consumer. Pretty likely", "Sounds plausible; sensitive conversations are overheard by third parties", "Hacks have shown that it is possible [to control a Smart TV by hackers] and the safety of users is at risk".*

Unlikely. Some participants considered the eventuality to be infeasible:

> *"unlikely, but the possibility is critical", "I don't think that could happen", "Sounds like James Bond".*

Table 6.3 shows which theme has been assigned to how many free text responses. The total row represents the number of assignments in that specific message.

	Vendor - Audio Stream & Harm	**Criminals - Audio Stream & Harm**	**Criminals - Audio Stream & Burglary**
Themes Leading to Low Criticality Levels			
No Harm	3	4	0
Not Me	7	21	0
Nothing to Hide	3	10	0
Trust in Vendor	6	0	1
High Effort	2	3	15
Haven't Heard	5	6	5
Hackers aren't Burglars	0	0	10
Themes Leading to High Criticality Levels			
General Unease	15	6	8
Lack of Security/Privacy	56	49	23
Surveillance	12	5	0
Themes Leading to All Criticality Levels			
Deactivate Feature	12	2	2
Is Possible	23	26	52
Unlikely	15	23	45
Total	159	155	161

Table 6.3.: List of themes and numbers of assignments in each message.

The most participants that justified their answers with *Unlikely* were in the 'Criminals - Audio Stream & Burglary' message. *Surveillance* were most mentioned in the 'Vendor - Audio & Harm' message. *Nothing to Hide* were most assigned in the 'Criminals - Audio Stream & Harm' message.

6.3 Discussion

Making people aware of usage data being collected for personalized advertisements is not worth the effort. Furthermore, making people aware that the data that is collected can be misused to harm them is worth the effort. Finally, the focus of the awareness messages should be on the potential misuse of application data such as audio data in order to be most effective.

The criminal-related awareness messages are not more effective than those related to the vendors (on audio data). Note, the criminal-related messages were not about getting the collected data from the vendors but from hacking into the Smart TVs or Wi-Fi networks. One possible explanation is related to personal attitudes as, on the one hand, in the group of 'criminals-audio stream & harm', more participants mentioned the nothing to hide argument. On the other hand, in the group of 'vendor - audio

stream & harm' more participants believe that by using some privacy-protection functionality protects them.

Note, we did not only select participants that owned a Smart TV, since we also wanted to address people that will buy a Smart TV in future.
We found that if the message becomes more specific, it will not make the message more effective. The open text field responses indicated that some participants considered the effort required of a miscreant to mount such an attack to be too high. They did not consider it possible that hackers and burglars would collaborate. Thus, what is really important is that the awareness message has to be believable. If messages were too specific for participants to be able to relate to, they failed to convince the participants that the threat was real.

Since vendors already deactivated the automatic recording of audio in their Smart TVs, we considered both 'Vendor & Broadcaster - Usage Data' for our further research:

- **Vendor & Broadcaster - Usage Data.** The Smart TV vendor and the broadcaster gather and analyze information about how, and how often, you use your Smart TV.
- **Vendor & Broadcaster - Usage Data & Harm.** The Smart TV vendor and the broadcaster gather and analyze information about how, and how often, you use your Smart TV. *It cannot be ruled out that the gathered information ends up in the wrong hands and abused in order to harm you.*

Limitations. The pre-study was conducted in Germany, where the population tends to be more attuned to privacy concerns than citizens of other countries [58]. A study with Americans, for example, might well deliver different awareness levels and responses to scenarios and/or messages.

This study relies on self-report. We do not know whether expressed criticality levels were genuine. Participants could have given false answers but since they were anonymous it is hard to see that many would feel the need to disseminate or to fabricate responses.

6.4 Summary

In this chapter we reported on a study with 175 participants to find out how privacy-related awareness messages ought to be formulated in order to ensure that they achieve two things: raise awareness of privacy risks of Smart TVs, and prompt a level of concern. This chapter serves as a pre-study for our further studies in this work. The result shows firstly that the messages must be accepted by the recipient, so that they do not reject it out of hand. But, secondly, even if acceptance is achieved, the message has to be compelling enough to raise concerns. Awareness without concern will mean that consumers are likely to accept the privacy risk and do not want to change anything.

For the following chapters we isolated these messages:

- **Vendor & Broadcaster - Usage Data.** The Smart TV vendor and the broadcaster gather and analyze information about how, and how often, you use your Smart TV.
- **Vendor & Broadcaster - Usage Data & Harm.** The Smart TV vendor and the broadcaster gather and analyze information about how, and how often, you use your Smart TV. *It cannot be ruled out that the gathered information ends up in the wrong hands and abused in order to harm you.*

These messages raised the level of criticality and are understandable in terms of consequences and risks. We did not select a scenario that enables vendors to record audio from Smart TVs since the vendors updated that functionality in newer Smart TVs so that the privacy risk is reduced.

7 Raising Awareness

In Section 6, we conducted a pre-study that evaluated different awareness-raising messages that were developed based on the consumer attitudes from Section 5.

In this chapter, we discuss our evaluation of two raising-awareness messages that we isolated in the pre-study in order to raise consumer awareness of Smart TV related privacy risks. In Section 7.1, we describe the methodology. The results are shown in Section 7.2. We discuss our results in Section 7.3. Finally, we summarize related work in Section 7.4 and the main results of this chapter in Section 7.5. We published parts of this chapter in [25].

7.1 Methodology

We show the study design in Section 7.1.1. The recruitment and ethical considerations are presented in Section 7.1.2. In Section 7.1.3, we describe the methodology how we analyzed the free text answers of participants.

7.1.1 Study Design

The study was split into five phases. Note, the study was conducted in Germany and questions and quotes in German were translated. The original German questionnaire can be found in the Appendix E. The phases were as follows (see Figure 7.1):

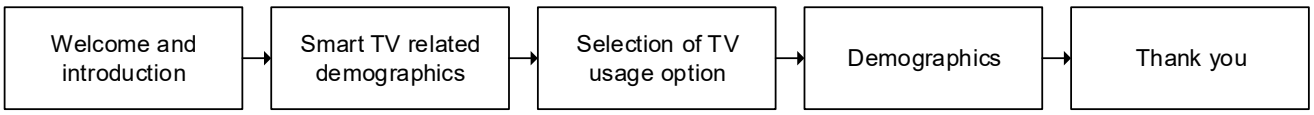


Figure 7.1.: Study design of the raising awareness online survey.

Welcome and introduction: Participants were informed that the study focuses on Smart TVs. They were not briefed about the exact focus as not to prime their answers. Information about the duration was provided (up to 10 minutes) as well as the fact that there are no wrong answers. They were told that they could leave the study at any point. However, only entirely completed studies earned the participants a monetary reward.

Smart TV related demographics: Participants were presented an information what a Smart TV is and they were asked whether they own a Smart TV or not. Afterwards, we presented an information about Internet functionality and gave them some examples what Internet functionality is. This information was provided on every study page. Then, we asked them to rate whether they use or would like to use Internet related functionality on their Smart TV on a regular basis. Options ranged from 1 'does not apply at all' to 5 'fully applies'.

Selection of TV usage option: Participants were randomly assigned to one of two groups. Each group was shown one of the two awareness messages that we isolated in Chapter 6 without the names in order to not prime them:

- **Simple awareness message.** The Smart TV vendor and the broadcaster collect and analyze usage data (e.g., information about how, and how often, you use your Smart TV).

- **Advanced awareness message.** In addition to the text from the 'simple awareness' group: It cannot be ruled out that the collected information ends up in the wrong hands in order to harm you.

Then, participants were asked which Smart TV usage option they would prefer. Because the only truly reliable privacy protection option is to not connect the Smart TV to the Internet the following two usage options were presented. The category names (privacy risk/protection) are only used for this work and were not communicated to the participants:

1. 'Privacy risk' option: The Smart TV will be connected to the Internet.
2. 'Privacy protecting' option: The Smart TV will not be connected to the Internet.

We asked them to justify their answer in a free text field.

Demographics: Participants were asked about gender and age.

Thank you: Finally, those who completed the study got information how to proceed for the monetary reward.

7.1.2 Recruitment and Ethics

The recruitment process was similar to the one described in Chapter 5.1.2. The study were conducted in June/July 2016 and SoSciSurvey was used as the platform. The participants were recruited over clickworker. We paid each participant who completed the studies and who did not provide obvious nonsense answers according to the minimum wage of Germany a fair monetary reward (i.e. 1.40€ for about 9 minutes). Furthermore, we made sure that each clickworker could only fill out one of our Smart TV related studies. For ethical compliance see Chapter 5.1.2 as the same held for this study.

7.1.3 Evaluation Methodology

An open-coding approach was used for all free text answers by the participants. We proceeded in the same way as described in Chapter 5.1.3.

7.2 Results

We present the participant's sample in Section 7.2.1. Section 7.2.2 reports on the effectiveness of the presented awareness messages. We analyzed the reasons why participants would not disconnect their Smart TV in Section 7.2.3.

7.2.1 Sample

155 participants completed the study (see Table 7.1). The study group consisted of 75 females (48%) and 79 males (51%); one (1%) participant did not mention gender. The youngest participant was 18, the oldest 65 and the mean age was 34.88 years with a standard deviation of 10.76.

106 (68%) participants owned a Smart TV. We only considered those participants who stated that they own a Smart TV and who rated that they use Internet functionality regularly at least with 3 (ranged from 1 'does not apply at all' to 5 'fully applies'). 82 (53%) participants owned a Smart TV and used Internet functionality regularly.

	total	female	male
# of participants	155*	75 (48%)	79 (51%)
# of participants own a Smart TV	106*	52 (49%)	53 (50%)
# of participants use Internet on their Smart TV	82	45 (55%)	37 (45%)

* one did not mention gender

Table 7.1.: Sample of consumer raising awareness study.

From these 82, 43 (52 %) were made aware that usage data is collected and analyzed, i.e. were assigned to the 'simple awareness' group. The remaining 39 (48%) were assigned to group 'advanced awareness' and were made aware that the collected and analyzed data can also be misused to cause harm if accessed by criminals. The youngest participant in the group 'simple awareness' was 18, the oldest 65 and the mean age was 32.63 years with a standard deviation of 10.21. The corresponding numbers for the 'advanced awareness' group are: the youngest 18, the oldest 57, mean age 35.05 and standard deviation 11.20.

7.2.2 Effectiveness of Awareness Messages

In the group 'simple awareness', 8 (19%) stated that they would not connect their Smart TV to the Internet anymore ('privacy protecting' option). 1 (5%) male decided for the privacy protecting selection; 7 (29%) females did. In the group 'advanced awareness', 15 (38%) participants selected this option; 6 (33%) males and 9 (43%) females did. For more details see Table 7.2 and Figure 7.2.

	Simple awareness group			Advanced awareness group		
	female	**male**	**total**	**female**	**male**	**total**
# (%) Privacy risk option	17 (71%)	18 (95%)	35 (81%)	12 (57%)	12 (67%)	24 (62%)
# (%) Privacy protecting option	7 (29%)	1 (5%)	8 (19%)	9 (43%)	6 (33%)	15 (38%)
Total	24	19	43	21	18	39

Table 7.2.: Effectiveness of both awareness messages.

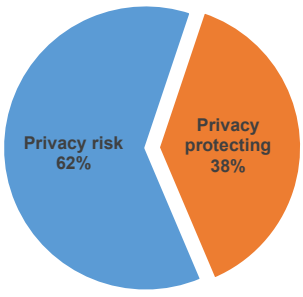


Figure 7.2.: Graphical representation of effectiveness results for the advanced awareness group.

For both groups we did the following χ^2-tests[1]:
A significant improvement in the selection behavior could be shown between the groups 'simple awareness' and 'advanced awareness'; χ^2=4.00, df=1, p<0.05.

Note, no significant difference could be found between males and females; 'simple awareness': χ^2= 4.51, df=1, p (exact) =0.06 and 'advanced awareness': χ^2=0.37, df=1, p (exact) =0.74.

[1] All preconditions are met.

7.2.3 Justifications

Table 7.3 shows the categories that we assigned to justifications for keep using the Internet in both awareness groups.

	Simple awareness group			Advanced Awareness group		
	female	**male**	**total**	**female**	**male**	**total**
Functionality is important	11	13	24	7	10	17
Don't mind	3	5	8	2	1	3
Resignation	2	1	3	1	2	3

Table 7.3.: Categories assigned to participants that keep using the Internet.

We extracted some example quotes that give more insights why participants decided for keeping the Internet connected:
Functionality is important: Participants said that the functionality they get when connecting the Smart TV to the Internet are important to them. Example quotes are:

> *"A Smart TV without Internet isn't useful" , "I don't need a Smart TV without Internet"*

Some participants balanced privacy against functionality and decided for functionality. Example quotes are:

> *"I think that the advantages that I get when it's connected to the Internet outweigh the disadvantages"*

Don't mind: Participants did not mind if usage data is collected and analyzed by broadcasters and vendors for various reasons. Example quotes are:

> *"I don't mind if my usage data is passed on" , "[..] I don't care if someone finds out that I watch porn."*

Resignation: Participants thought this happens everywhere and they cannot do anything against it. Example quotes are:

> *"Today, data is collected everywhere. The recording of TV usage behavior is relatively innocent.", , "The risk always exists that data ends up in the wrong hand, [..]."*

7.3 Discussion

This study's results demonstrate that significantly more consumers would disconnect their Smart TV when they are made aware of the risks with the advanced awareness message (with harm) as compared to the simple message (without harm). Thus, for further awareness studies it is essential to communicate the potential harm and not just the fact that data is collected and analyzed.

We also gained other insights into Smart TV consumer attitudes towards privacy risks. Many would willingly sacrifice privacy in order to make use of the Internet functionality of Smart TVs either because (1) functionality is more important, (2) consumers do not mind sharing usage data or (3) consumers are resigned to privacy risks. Note, most participants inhabited the first category.

Consequently, we were interested in whether the situation would change if privacy tools were made available. We wanted to evaluate the effectiveness of both messages in the presence of such a tool. In particular, we wanted to find out whether the advanced message was still more effective in this context.

Another issue could be that people's privacy attitudes often differ from the decisions they make. This inconsistency is called 'privacy paradox' . This issue has mostly been highlighted in the context of online privacy, e.g., from Trepte *at al.* and Dienlein [78–81]. In the context of Smart TVs, we experienced similar issues. Consumers claimed that privacy was important, but most of them also connected their Smart TVs to the Internet without any qualms.

Limitations. The research was conducted in Germany, where the population tends to be more attuned to privacy concerns than citizens of other countries [58].

Furthermore, the study relied on self-reports. We do not know whether expressed concerns were genuine nor do we know whether they actually act in a way that aligns with their concerns.

7.4 Related Work

We report related work that studied different methods of awareness raising:

Researchers have identified a lack of awareness (in particular of possible consequences) as one possible explanation for a low uptake of privacy protection mechanisms general, e.g. from Jensen *et al.* [82], as well as in specific contexts such as in social networks, e.g. from Acquisti *et al.* [83], and in mobile apps, e.g. from Kelley *et al.* [84], Felt *et al.* [85] or Harbach *et al.* [86]. A few approaches to address these observations have been studied such as nudging [87]. However, what has not been evaluated - to the best of our knowledge - whether making them aware of privacy risks and possible negative consequences actually has an influence at all and how much.

The privacy calculus theory is one way to explain users' privacy behaviour (referred to as privacy paradox). It states that people seek a balance between potential risks and benefits, e.g. in e-commerce from Dinev *et al.* [88], in online market places from Kim *et al.* [89] or from Lankton *et al.* in social networks [90, 91]. We discovered that, in the context of Smart TVs, functionality outweighs privacy concerns.

7.5 Summary

In this chapter we evaluated whether consumer's intention to not connect their Smart TV to the Internet can be influenced by making them aware that usage data is collected and analyzed. Additionally, we analyzed whether this influence can be strengthened when making them aware that the collected and analyzed data could potentially be misused to cause harm if accessed by criminals.

We conducted an online survey with 155 participants and 19% of the participants, who had their Smart TV connected to the Internet and who saw the simple awareness message, stated to disconnect their Smart TV from the Internet. The simple awareness message explained that the Smart TV vendor and the broadcaster gather and analyze usage data of the Smart TV.

Significantly more participants made this statement when showing them the advanced awareness message (compared to the simple). However, also with the advanced awareness message 62% of the participants would still not disconnect the Smart TV from the Internet. In addition to the simple awareness message, the advanced awareness message informed the participants that the gathered data could be misused in order to harm them.

Based on the justifications many participants do so because functionality is restricted when disconnecting the Smart TV.

8 Raising Awareness and Offering Alternatives for Connecting the Smart TV

The survey conducted in Chapter 7 resulted that most Smart TV consumer would not disconnect their Smart TV when functionality would be limited. In this chapter, we evaluate to which extend consumers who are aware of the privacy risks and the potential harm are willing to spend time and/or money on protecting their privacy when remaining the Internet functionality.

In Section 8.1, we describe the methodology used. The results in Section 8.2 state that many participants would deploy alternative options to connect their Smart TV when functionality is not limited. We discuss the results in Section 8.3 Finally, we summarize related work in Section 8.4 and the main results of this chapter in Section 8.5. Parts of this chapter are published in [25].

8.1 Methodology

We show the study design in Section 8.1.1. The recruitment and ethical considerations are presented in Section 8.1.2. In Section 8.1.3, we describe the evaluation methodology how we analyzed the free text answers of participants.

8.1.1 Study Design

The study were split into the same phases as the study shown in Chapter 7 (see Figure 8.1). We repeat them for completeness and readability. Differences are mentioned in the phase 'Selection of TV Usage Option'. Note, the study was also conducted in Germany and questions and quotes in German were translated. The original German questionnaire can be found in the Appendix F.

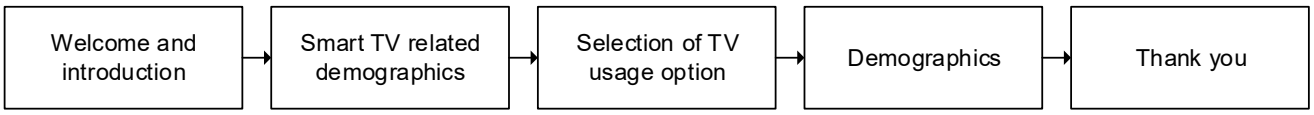


Figure 8.1.: Study Design of the raising awareness and offering alternatives study.

Welcome and introduction. Participants were informed that the study focuses on Smart TVs. They were not briefed about the exact focus as not to prime their answers. Information about the duration was provided (up to 10 minutes) as well as the fact that there were no wrong answers. They were told that they could leave the study at any point. However, only entirely completed studies earned the participants a monetary reward.

Smart TV related demographics. Participants were presented an information what a Smart TV is and they were asked whether they own a Smart TV or not. Afterwards, we presented an information about Internet functionality and gave them some examples what Internet functionality is. This information was provided on every study page. Then, we asked them to rate whether they use or would like to use Internet related functionality on their Smart TV on a regular basis. Options ranged from 1 'does not apply at all' to 5 'fully applies'.

Selection of TV usage option. The studies from chapter 7 and the one presented in this chapter differed in the options that could be selected by the participants. Additionally, there were also options to use the Smart TV with Internet functionality in a privacy protecting way. Resulting in the following connection

methods for Smart TVs; four of them were privacy protecting connection methods (names of these options were only introduced for this work and not shown to the participants):

1. 'Privacy risk' Option: The Smart TV will be used as bought and connected to the Internet.
2. 'Privacy protecting w/o Internet' Option: The Smart TV will not be connected to the Internet.
3. 'Effort' option: The Smart TV will not be connected to the Internet. Additionally, it will be used as an external monitor for a laptop.
4. 'Effort+costs' option: A privacy protection mechanism will be used to prevent the collection of usage data while still using the Internet functionality. It costs 20€ and one needs about 15 min to configure it.
5. 'Costs' option: A privacy protection mechanism will be used to prevent the collection of usage data while still using the Internet functionality. It costs 40€ and no additional configuring time is needed.

The privacy protection mechanisms with costs/effort have not been marketed as yet, but a prototype mechanism can be found in Chapter 9. The 'Effort+cost' option is supposed to be installed on an existing device (e.g., router) and the software should be purchased for 20€ similar to regular protection software for PCs[1]. The 15 minute configuration time is the average time a consumer may need to configure software (install it, choosing the preferences and select the right Smart TV Model). For the 'Costs' option, we considered a pre-configured bundle[2] with hard- and software which should be purchased for 40€.

Demographics. Participants were asked about gender and age.

Thank you. Finally, those who completed the study got information how to proceed for the monetary reward.

8.1.2 Recruitment and Ethics

The recruitment process was similar to the one described in Chapter 5.1.2. The study were performed in July 2016 after the study in chapter 7 and SoSciSurvey was used as the platform. The participants were recruited over clickworker. We paid each participant who completed the studies and who did not provide obvious nonsense answers according to the minimum wage of Germany a fair monetary reward (i.e. 1.40€ for about 9 minutes). Furthermore, we made sure that each clickworker could only fill out one of our Smart TV related studies. For ethical compliance see Chapter 5.1.2 as the same held for this study.

8.1.3 Evaluation Methodology

An open-coding approach was used for all free text answers by the participants. We proceeded in the same way as described in Chapter 5.1.3.

8.2 Results

We present the participant's sample in Section 8.2.1. Section 8.2.2 reports on the effectiveness of the presented awareness messages and the offered alternative options to connect a Smart TV.

[1] See e.g. `https://www.amazon.com/dp/B010P91LYY` (accessed 11 December, 2016).
[2] See e.g. `https://www.amazon.com/dp/B000BTL0OA` (accessed 11 December, 2016).

8.2.1 Sample

169 participants completed the study (see Table 8.1). The study group consisted of 84 females (50%) and 83 males (49%); Two (1%) did not mention gender. 121 (72%) participants owned a Smart TV.. As in the last section, we only report those participants who stated that they own a Smart TV and who rated that they use the Internet features regularly at least with 3 (ranged from 1 'does not apply at all' to 5 'fully applies'): 97 (53%) participants were considered as they own a Smart TV and use Internet functionality regularly.

	total	**female**	**male**
# of participants	169**	84 (50%)	83 (49%)
# of participants own a Smart TV	121*	58 (48%)	62 (51%)
# of participants use Internet on their Smart TV	97	48 (49%)	49 (51%)

** two did not mention gender; * one did not mention gender

Table 8.1.: Sample of consumer raising awareness and offering alternatives study.

From these 97, 45 (46 %) were assigned to the 'simple awareness' group and the remaining 52 (54%) were assigned to the 'advanced awareness' group. The youngest participant in the group 'simple awareness' was 18, the oldest 68 and the mean age was 36.44 years with a standard deviation of 12.08. The corresponding numbers for the 'advanced awareness' group are: the youngest 18, the oldest 67, mean age 36.80 and standard deviation 12.20.

8.2.2 Effectiveness of Messages

Table 8.2 reports the results for all participants that were presented five options. In both groups more than two third stated that they would be willing to spend time and/or money to get both - functionality and privacy ('simple awareness' group: 30 (67%); 'advanced awareness' group: 39 (75%)). From the three available options, the effort and/or cost options were the preferred ones, especially in the 'advanced awareness' group.

	Simple awareness group			**Advanced awareness group**		
	female	**male**	**total**	**female**	**male**	**total**
# (%) Privacy risk option	6 (27%)	8 (35%)	14 (31%)	4 (15%)	8 (31%)	12 (23%)
# (%) w/o Internet option	1 (5%)	0 (0%)	1 (2%)	1 (4%)	0 (0%)	1 (2%)
# (%) Effort option	3 (14%)	3 (13%)	6 (13%)	2 (8%)	4 (15%)	6 (12%)
# (%) Effort + costs option	7 (32%)	6 (26%)	13 (29%)	13 (50%)	12 (46%)	25 (48%)
# (%) Costs option	5 (23%)	6 (26%)	11 (24%)	6 (23%)	2 (8%)	8 (15%)
# (%) Costs and effort related options total	15 (68%)	15 (65%)	30 (67%)	21 (81%)	18 (69%)	39 (75%)
# (%) Privacy protecting options total	16 (73%)	15 (65%)	31 (69%)	22 (85%)	18 (69%)	40 (77%)
total	22	23	45	26	26	52

Table 8.2.: Effectiveness of new options.

In total, in the 'advanced awareness' group, 77% would change to a privacy protecting connection method; compared to 38% in the corresponding group in the first study with only one privacy protecting

option. The corresponding percentages for the 'simple awareness' are 69% versus 19%.

We did apply the same χ^2-tests as in the raising awareness study (see Section 7): No significant improvement could be shown between the selection behavior of the groups 'simple awareness' and 'advanced awareness'; χ^2=4.21, df=4; p(exact)= 0.373.

No significance could be found between males and females selection behavior; 'simple awareness': χ^2=1.53, df=4, p(exact)=0.96 and 'advanced awareness': χ^2=4.83, df=4, p(exact)=0.28.

8.2.3 Effectiveness of Offering Functionality

We observed a difference in the choosing behavior of Smart TV consumers comparing the study from Chapter 7 (two options) and this study (five options). We analyzed the differences between them. We found that an increased number of consumers demonstrated a preference for a privacy-protecting connection method.

For this analysis, we combined the groups 'w/o Internet' and all effort and/or cost groups from this study to arrive at two groups (see the graphical representation in Figure 8.2. The distribution after combining the four privacy-protecting options of this study looks, at first glance, like a random distribution, since 26 (27%) participants selected the 'Privacy risk' option and 71 (73%) a privacy-protecting option. A 20 to 80 distribution would be expected under random choice circumstances. In the two options study, 59 (72%) wanted to retain the connection to the Internet and 23 (28 %) wanted to disconnect the Smart TV. Thus, the choice behavior differed significantly from a random distribution (χ^2=15.80, df=1, p<0.001) with a clear lean towards the 'Privacy risk' option.

Therefore, we interpret the choice behavior in the second study as a positive effect. Proposing alternative options that protect the consumer's privacy while retaining Internet functionality seems the most promising approach.

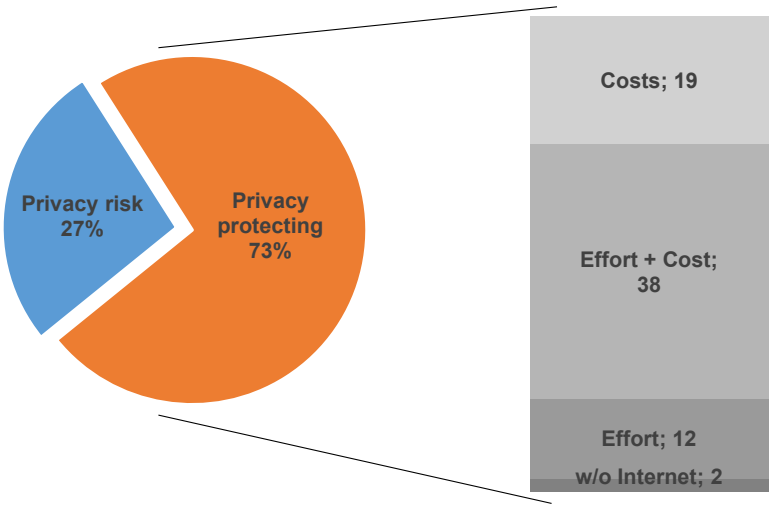


Figure 8.2.: Graphical representation of effectiveness of alternatives results for the advanced awareness group.

8.3 Discussion

In this study, we showed that Smart TV consumers were most likely to deploy a privacy protection measure on their Smart TV when the measure did not impair available functionality. They were willing to

commit time and/or effort to protect their privacy under these conditions. If functionality is restricted, on the other hand, they are unlikely to deploy a privacy-protection measure. Thus, corresponding usable technologies should be offered instead of purely making people aware of the privacy risks of current technologies such as Smart TVs.

Limitations. The research was conducted in Germany, where the population tends to be more attuned to privacy concerns than citizens of other countries [58].

Furthermore, the study relied on self-reports. We do not know whether expressed concerns were genuine nor do we know whether they actually act in a way that aligns with their concerns.

Additional to the two limitations also mentioned in the Chapter 7, we did not mention the exact costs or effort for the 'External Display' option. We assumed that consumers have an idea how much time is needed to connect a PC/Laptop with a Smart TV.

8.4 Related Work

We report related work related to the importance of adequate functionality:

Kulyk *et al.* [92] and Volkamer *et al.* [63] identified a sacrifice of functionality as a possible explanation for a low uptake of privacy protection mechanisms in the context of smart phones. Researchers have studied how to address this observation by developing privacy enhancing technologies (PETs) for various contexts, e.g. from Fawaz *et al.* [93] for protection location privacy. Furthermore, it has been studied whether people are willing to pay in general for more privacy, e.g. from Rose [94], from Grossklags *et al.* [95], Acquisiti *et al.* [96] , Tsai *et al.* [97]. However, what has not been evaluated - to the best of our knowledge - whether people would pay for privacy protection mechanisms that provide the functionality and protect their usage data.

8.5 Summary

In this chapter, we discussed an online survey with 169 participants that we conducted to evaluate different levels of awareness when offering alternatives for connecting the Smart TV to the Internet. We evaluated to which extend consumers who are aware of the privacy risks and the potential harm are willing to spend time and/or money on protecting their privacy when retaining the Internet functionality. We offered participants five alternatives: (1) use the Smart TV as recommended by the vendor, (2) disconnect the Smart TV, (3) use the Smart TV as external display for a laptop, (4) connect a pre-configured protection system to the Smart TV and (5) connect a protection system without configuration to the Smart TV. For the last two alternatives consumers must spend time and/or money.

We showed that Smart TV consumers most likely would change their mind regarding their connection method when it does not restrict the functionality; while they would spend time/effort on protecting their privacy. Thus, corresponding usable technologies should be depended instead of (purely) make people aware of the privacy implications of nowadays technologies.

Only 23% participants stated that they would not take any privacy protection methods (and keep using the Smart TV's Internet functionality as before participating in this study). From the remaining ones, 2% stated to disconnect the Internet and all others (75%) are willing to spend either money or time and money to protect their privacy.

9 Developing an Alternative to Connect the Smart TV

In this chapter, we present the *Smart TV Protector* that protects Smart TV consumers' privacy. It also protects Smart TVs against some security vulnerabilities. The *Smart TV Protector* is not a fully tested protection measure. It is rather a prototypical implementation which shows that it is feasible to establish a protection measure for Smart TVs.

In Section 9.1, we present the requirements for the *Smart TV Protector*. They are deducted from the risks mentioned in the previous chapters. In Section 9.2, we give an overview of the *Smart TV Protector* to introduce its three components: *Smart TV Protector Controller* (Section 9.3), *Core Protector* (Section 9.4) and *HbbTV Privacy Protector* (Section 9.5). We evaluate the *Smart TV Protector* in Section 9.6. We present related work in Section 9.7. Finally, we discuss and summarize the main results in Section 9.8. The *HbbTV Privacy Protector* presented in this chapter has been published in [16, 17].

9.1 Requirements

The development for the *Smart TV Protector* is driven by two aspects: privacy risks and consumers' attitudes. Both were explored in the previous sections of this work. We summarize the risks that the *Smart TV Protector* should cover in Section 9.1.1 and show countermeasures. Based on that, we formulate requirements in Section 9.1.2.

9.1.1 Considered Privacy Risks

Mainly, we wanted to protect Smart TV consumers against the privacy risks revealed in this work. We summarize them briefly in Table 9.1. In this table, we note potential actions that we found while analyzing these risks. The right column describes known countermeasures.

Risk	Potential Actions	Known Countermeasures
HbbTV tracking	Consumers can be tracked on channels with HbbTV by broadcasters.	Disable HbbTV for all or selected channels on the Smart TV.
Wrongly implemented HTTPS validation	Attacker can gain access to Smart TV, manipulate Smart TV software or eavesdrop on data.	The Smart TV should not perform vulnerable requests.

Table 9.1.: Summary of identified privacy risks.

HbbTV tracking can basically be deactivated by disabling HbbTV. Most Smart TVs offer an option in the menu to deactivate HbbTV. A more selective solution would be to disable HbbTV only on selected channels that can be chosen by the consumers. But, our tested Smart TVs did not offer this option. Based on our survey (Chapter 5) consumers are not aware how to disable HbbTV.

Privacy risks that are caused by security vulnerabilities such as the revealed issue *wrongly implemented HTTPS validation* are much harder to mitigate. These issues can only be detected when the Smart TV is regularly tested. If detected, the mitigation in most cases is to block malicious connections.

We further analyzed, which functionality can be disabled in the Smart TV settings:

- The HbbTV functionality can be deactivated on all our tested Smart TVs. But, for instance on Samsung Smart TVs the functionality was named 'Data Services'. Based on our survey in Chapter 5, we know that most consumers are not aware of how to deactivate HbbTV. Naming of settings in a non-intuitive way does not improve the consumers' ability to deactivate HbbTV. All our tested Smart TVs did not offer the option to disable HbbTV only for specific channels.
- Privacy risks caused by security vulnerabilities in Smart TVs cannot be disable by the Smart TV itself, only firmware updates can help to mitigate these issues.

9.1.2 Resulting Requirements

Based on our conducted surveys and the revealed privacy risks, we structured the requirements in the following two categories: (1) Protection against privacy risks and (2) consumers' attitudes.

Requirements for protection against privacy risks. These requirements discuss the type of privacy risks that should be detected and if possible mitigated by the *Smart TV Protector*:

- **HbbTV tracking.** As identified in Chapter 3, HbbTV can be deployed to collect consumers' usage data to profile consumers. In order to mitigate the revealed privacy risks, it is necessary to control the traffic of HbbTV. The following technical requirements are needed:
  - **Web technologies must be handled**. HbbTV and other Smart TV functionality (e.g. updates for the Smart TV) use web technologies like HTML, CSS and JavaScript. These technologies should be supported by the *Smart TV Protector*.
  - **Ability to detect the Smart TV model.** Each Smart TV vendor implements different functionality. In order to give consumers proper hints whether and how HbbTV can be deactivated in the Smart TV options it is essential to detect the Smart TV model.
  - **Need to offer a user interface.** No plugins or add-ons are supported by most of the available Smart TVs. The consumers need a possibility to interact with the *Smart TV Protector*.
- **Identification of wrongly validated HTTPS certificates.** The *Smart TV Protector* should detect wrongly validated HTTPS certificates. The traffic should be blocked and the consumer should be notified.

Requirements due to consumers' attitudes. These requirements are mainly deduced from the surveys in Sections 5-8 to get a consumer experience so that protection is not disturbing:

- **Costs/effort should be low.** Consumers do not want to spend much money and effort to use the *Smart TV Protector*. Thus, it should be easy to use.
- **Transparent for consumers.** Consumers do not want to do any additional actions. It should be as simple as possible and as hidden as possible.
- **Functionality matters.** Consumers want to use the functionality instead of avoiding privacy risks. They value the functionality more than privacy protection.
- **Graphical user interface.** An information which Smart TV services are found in the network and the current device status (blocked or allowed) should always be available. The logged and blocked information should be presented to the consumer so that the consumer can browse through the findings. For some findings – that can be mitigated by configuring the Smart TV – a detailed information how to disable or enable them should be displayed.

We want to use standardized soft- and hardware where possible. This reduces development effort and increases the prototype quality. We do not want to reinvent software that is already available and can be reused.

9.2 Overview of the Smart TV Protector

The overall purpose of the *Smart TV Protector* is to control the network traffic that is sent and received from the Smart TV in order to reduce risks. The *Smart TV Protector* is connected to the Smart TV and the Internet, so that the *Smart TV Protector* can monitor and manipulate all data sent or received by the Smart TV. This solution is transparent for the Smart TV, i.e., the Smart TV does not detect that the *Smart TV Protector* forwards all traffic to and from the Internet. In all our tests, the *Smart TV Protector* was installed on a computer with two network interfaces. We do not explain the hardware in further detail, since we used standard hardware with a Linux operating system.

The *Smart TV Protector* is split into three components: the *Core Protector*, the *HbbTV Privacy Protector* and the *Smart TV Protector Controller* (see Figure 9.1).

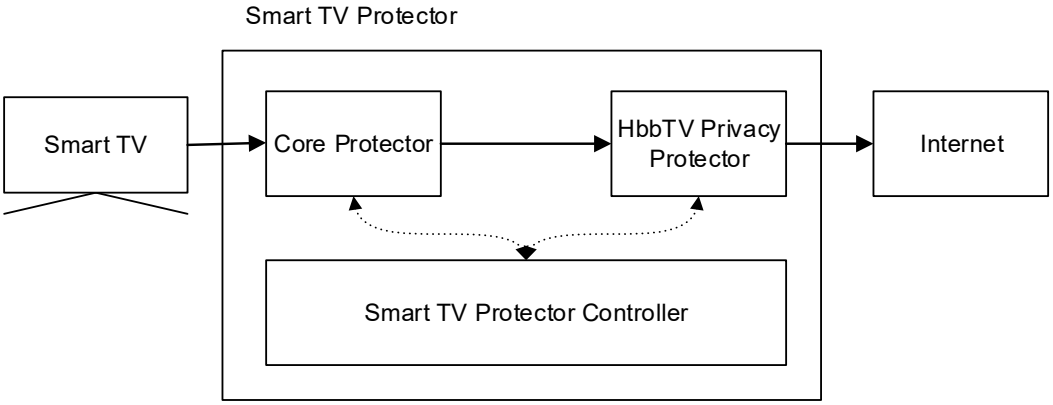


Figure 9.1.: Overview of the *Smart TV Protector*.

dotted line: configuration data; solid line: network traffic.

The *Core Protector* monitors network traffic sent and received by the Smart TV. It is able to block specific traffic based on rules. We describe the rules that fulfill the requirements later in this chapter. The *Core Protector* does not offer a user interface for consumers. It can be controlled by command line or over the *Smart TV Protector Controller*.

The *HbbTV Privacy Protector* is an HbbTV specialized component. It is able to allow or block HbbTV applications depending on consumers' decisions. Consumers can decide whether they want to load the HbbTV application. This decision can be performed directly on the Smart TV's screen. A customized notification is shown. The *Core Protector* cannot notify consumers directly on the Smart TV's screen due to technical reasons.

The *Smart TV Protector Controller* serves as a control unit that enables consumers to configure the *Core Protector* and the *HbbTV Privacy Protector* on a graphical user interface. It offers a web user interface that can be requested on any device with a web browser.

In the next sections, we explain the three components of the *Smart TV Protector* in more detail. We start with the *Smart TV Protector Controller* and explain high-level the functionality and the graphical user interface. Later, we describe the technical details of the *Core Protector* and the *HbbTV Privacy Protector*.

9.3 Smart TV Protector Controller

The *Smart TV Protector Controller* offers a user interface to configure the *Core Protector* and the *HbbTV Privacy Protector*. It provides a web based user interfaces that enables consumers to connect from every device with a current web browser. We give an overview of the *Smart TV Protector Controller* in Section

9.3.1. In Section 9.3.2, we introduce the user interface and explain the presented information and options. The database that is used for storing the data is explained in Section 9.3.3. Finally, we give some implementation details in Section 9.3.4.

9.3.1 Overview

The core functionality of the *Smart TV Protector Controller* is to serve as a configuration interface for the *Core Protector* and the *HbbTV Privacy Protector*. We did not implement any possible configuration option for all components, since the user interface would have too many options and thus would not be usable anymore.

Two different strategies supporting the consumer to reduce privacy risks are offered:

- Many Smart TVs offer options in their menus to deactivate or activate specific functionality. All our tested Smart TVs were not configured privacy protecting as possible by default. Therefore, the *Smart TV Protector Controller* has a functionality that shows consumers how to configure the Smart TV, if an information for this Smart TV model is available.
- The *Smart TV Protector* can control the network traffic in order to block Internet functionality, e.g., block traffic from HbbTV. Some settings can be set more fine-grained as in the settings of the Smart TV, e.g. block HbbTV only for channels instead for the entire Smart TV.

The *Smart TV Protector Controller* presents basically a list of events. These events are detected by the *Core Protector* or the *HbbTV Privacy Protector* e.g. HbbTV on channel A. If events are detected that could cause privacy risks, a user information is displayed, e.g., *HbbTV data transfer has been detected and enables the broadcaster to profile your usage behavior*. Afterwards, instructions are given how the consumer can change the behavior either by changing the Smart TV settings or configuring the *Smart TV Protector*. These instructions can be customized for each supported Smart TV model. If no customized version of the instructions is available, standard texts and options are displayed.

The *Smart TV Protector Controller* functionality is grouped in two parts: visualization and control. The visualization part presents the consumer a variety of information. In this part, settings cannot be set. We reduced the shown information to a minimum in order to reduce the time a consumer needs to spend to understand the information. It basically shows the following information:

- **General information.** This section presents general Smart TV information such as activity, IP address, data transfer to the consumers.
- **Events.** Events that are detected by the *Core Protector* or the *HbbTV Privacy Protector*.
- **Communication.** This section outlines the parties to which the Smart TV is communicating.
- **Contents.** The content - as far as we can determine - is presented to the consumer.
- **Security.** We show basic information about the security level of the Smart TV. An overview of malicious connections that were detected is presented.
- **Deduced information.** We inform the consumer what could be determined with the data detected.

The control part offers settings to configure the *Smart TV Protector* and if available information how to disable the functionality directly in the menu of the Smart TV model. It comprises the following sections:

- **General settings.** It enables the consumer to configure whether the Smart TV is allowed to communicate with the Internet.

- **HbbTV settings.** The *Smart TV Protector Controller* provides functionality to configure the HbbTV protection. It is possible to deactivate HbbTV completely as well as selectively. Selectively means that the consumer gets a list of detected HbbTV applications presented and an option whether it should be deactivated. An option that shows an information on the Smart TV is also provided.
- **Advanced settings.** The *Smart TV Protector Controller* provides options to disable update functionality or limit it to a specific time frame.

Note, the user interface is a prototypical implementation that can be extended if necessary. We show some examples of the current version in the next section.

9.3.2 Graphical User Interface

The graphical user interface (GUI) is designed based on the mentioned core functionality.

Figure 9.2 outlines the main parts of the GUI. It is split in three parts: headline, button to switch between views and the content area. The headline contains the title *Smart TV Protector* and a menu that can be clicked for direct view of the desired section. It also indicates which section is currently presented in the content area. The button switches between the visualization view and the control view. The content area shows the functionality. Some functionality cross link from the visualization to the control view and vice versa.

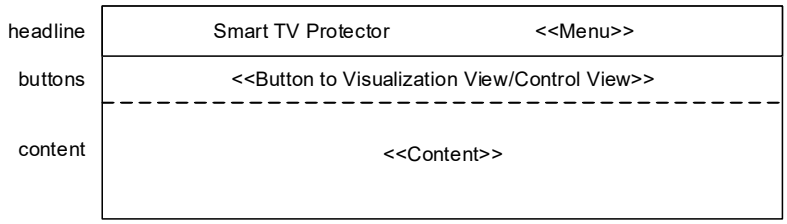


Figure 9.2.: Abstraction of the graphical user interface.

Headline. As depicted in Figure 9.3, *General Settings*, *HbbTV Settings* and *Advanced Settings* are the links to the content sections. The entire headline is fixed on the top of the page. If a section is shown in the content section, the button is highlighted in yellow (here HbbTV Settings).

Figure 9.3.: Example of the headline in the control view.

Button to switch between views. The buttons shown in Figure 9.4 are at the top of each page. When one of the buttons is clicked, the *Smart TV Protector Controller* loads the corresponding view.

Figure 9.4.: Screenshots of both switch buttons.

Content. The content section starts with a headline that is usually shown as a menu item, if the menu item would be too long an abbreviation is provided. Next to the headline follows a description text that explains the functionality. Then, a text that indicates whether additional information on the visualization or the control view is available and a link to this information is provided. If Smart TV related information

is available that supports the consumer to configure the Smart TV, a button *Smart TV specific information ...* is presented. When clicking the button, the how-to manual is loaded.

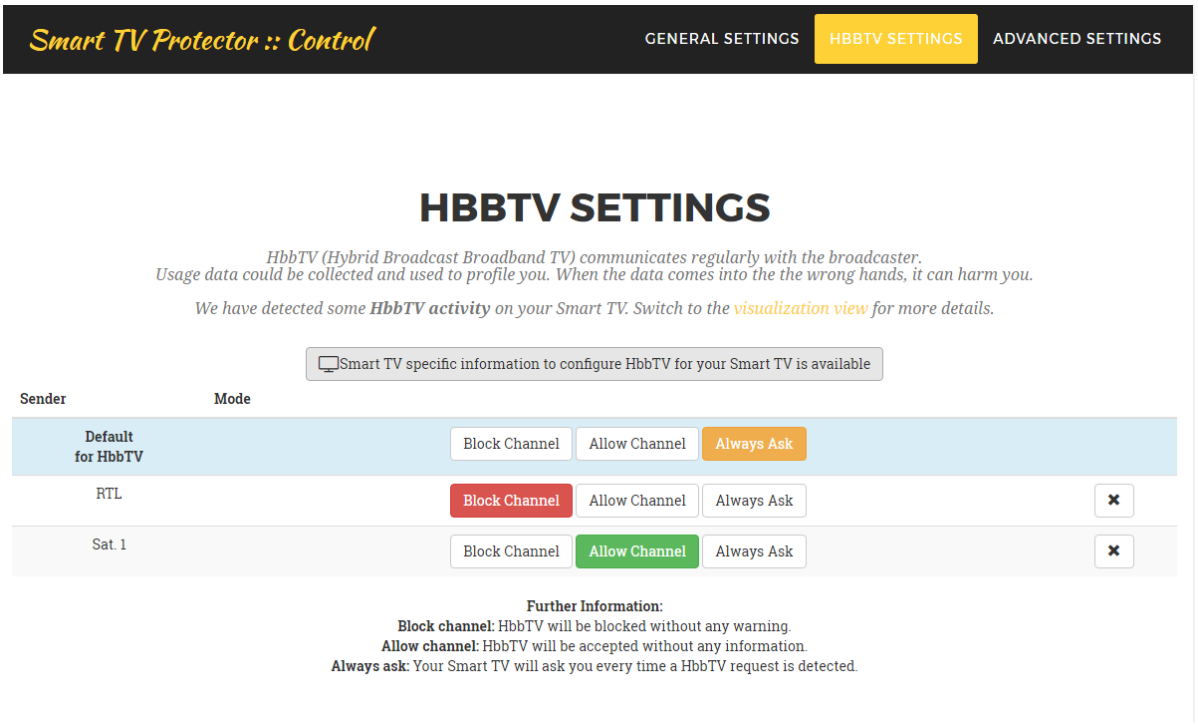


Figure 9.5.: Screenshot of content

The example shown in Figure 9.5 is the control view of the *HbbTV Settings*. Each channel can be set to *Block Channel*, *Allow Channel* and *always ask*. If *Allow Channel* is set for a specific channel, the consumers will not get an information of HbbTV activity and the HbbTV activity is not blocked by the *Smart TV Protector*. If *Block Channel* is set for a specific channel, the consumers will not get a warning. However, the transfer is blocked by the *Smart TV Protector*. If *Always Ask* for a specific channel is set, the consumers get a notification on the Smart TV's screen (see *HbbTV Privacy Protector*). The default settings for HbbTV are used for each channel that is not set by the consumer.

Note, all visualized and control information are stored in a database that we explain in the next section.

9.3.3 Database

The database is structured in five tables. Details of the tables can be found in Figure 9.6. We explain the purposes of each table as follows:

- **HbbTV Channel.** This table stores the channel name and the consumer decision whether the channel is set to *Allow Channel*, *Block Channel* or *Always Ask*.
- **Event.** This table stores the events that are collected by the *Core Protector* and *HbbTV Privacy Protector*. Only selected events are added to the table. Those events are shown to the consumers. The selection is based on the rules of the *Core Protector* (see Section 9.4.3).
- **Consumer information.** This table stores the information that is displayed for different contexts (e.g. HbbTV) to display consumers additional information. For example, how to disable HbbTV at the current detected Smart TV model.

- **Devices.** This table stores information about the detected devices and their names. If the name is not filed, the IP address is used.
- **Configuration parameters.** This table stores configuration parameters such as the local network.

Table: HbbTVChannel	
Name	**Type**
pk	integer
channel	text
decision	integer
url	text
visible	boolean

Table: Device	
Name	**Type**
pk	integer
ip	text
name	text
user_name	text
last_update	datetime

Table: Cinformation	
Name	**Type**
pk	integer
model	text
context	text
text	text

Table: Configuration	
Name	**Type**
pk	integer
key	text
value	text

Table: Event	
Name	**Type**
pk	integer
device_id	foreign_id
value	text
last_update	datetime

Figure 9.6.: Tables of the *Smart TV Protector Controller*.

9.3.4 Implementation

The entire *Smart TV Protector Controller* was implemented in Python[1] and the front-end was designed in HTML, JavaScript and CSS. The web framework Django[2] was used for modelling the logic behind the front-end. The data has been stored in a MySQL database, which is accessed by the *Core Protector* and the *HbbTV Privacy Protector*. The design of the *Smart TV Protector Controller* is built upon Bootstrap[3]. Different visualization and JavaScript libraries are used, e.g. jQuery[4] and Charts[5].

For serving the web application, we used an Apache HTTP Server[6] with mod_wsgi combination, which is for our needs sufficient. No heavy calculations have to be made, so the performance is negligible. We do not explain how the web server is configured since the standard configuration were customized to serve the web application. Moreover, we did not perform security and vulnerability checks against all components of this implementation. If this application should be marketed, it would be necessary to perform thorough security and functionality tests.

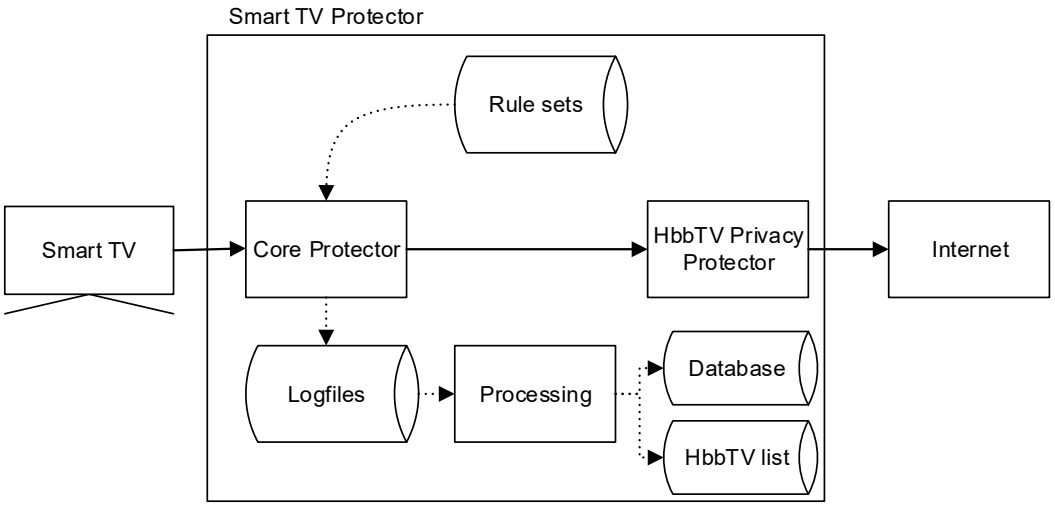
9.4 Core Protector

We present an overview of the *Core Protector* in Section 9.4.1. The *Core Protector* decides whether to take an action based on the deployed rule sets that are discussed in Section 9.4.2. In Section 9.4.3, we explain how the log files that are generated according to the rule sets, are processed. Finally, we give some implementation details in Section 9.4.4.

1 https://www.python.org
2 https://www.djangoproject.com/
3 http://getbootstrap.com/
4 https://jquery.com/
5 http://www.chartjs.org/
6 https://httpd.apache.org/

9.4.1 Overview

The *Core Protector* can record and manipulate all network traffic sent and received by the Smart TV. It takes actions based on the rule sets that are carefully tailored to the Smart TV context. In Figure 9.7 we outline all components of the *Core Protector*. Note, the HbbTV Protector is depicted as a black box and the *Smart TV Protector Controller* is omitted, since it only accesses the *Database*.



dotted line: data that is processed by the *Core Protector*; solid line: network traffic.

Figure 9.7.: Overview of the *Core Protector*.

The *Core Protector* is basically an intrusion detection and prevention system. Intrusion detection and prevention systems (IDS/IPS) are usually in place to detect actions or attacks that attempt to harm an IT-System or network [98]. The *Core Protector* focuses on Smart TVs and protects consumers. The rule sets that are usually used in a company network are to complex and not easy to maintain for our context. We deploy lightweight *rule sets*. Based on these rule sets the *Core Protector* generates log files whenever a rule matches. We extract in the *processing* step information from these log files to fill the database or generate a list of URLs that were requested from an HbbTV channels. If a rule matches that blocks the traffic, the *HbbTV Privacy Protector* does not get any network traffic and therefore no traffic to the Internet is sent.

The open source IPS Suricata[7] fulfills our needs. Thus, all shown source codes are customized for it. Other IDS/IPS software such as Snort[8] could have also been used. Note, our developed rules are not compatible with Snort. For example, Snort does not support SSL fingerprinting which we use to detect malicious HTTPS connections. In the remainder of this section, we explain each component from Figure 9.7 in more detail.

9.4.2 Rule Sets

In this section we explain the rule sets that are deployed in the *Core Protector*. A detailed information how rules for Suricata can be created is explained in the Suricata documentation [99]. We need two different types of rules: (1) alerting or logging rules and (2) blocking rules (see Figure 9.8). The first type does not change the network traffic and logs the event in a log file. The second type blocks the

[7] `https://suricata-ids.org/`
[8] `https://www.snort.org/`

network traffic and logs the event in the log file.

```
alert tcp $SMARTTV_IP any -> $EXTERNAL_NET any (msg:"Found hbbtv"; content:"hbbtv"; nocase; classtype:
    policy-violation; sid:1; rev:1;)
```

```
drop tcp $SMARTTV_IP any -> $EXTERNAL_NET any (msg:"Block hbbtv"; content:"hbbtv"; nocase; classtype:
    policy-violation; sid:1; rev:1;)
```

`$SMARTTV_IP` is replaced with the IP address of the corresponding Smart TV.

Figure 9.8.: Example of an alert and a block rule.

We developed rule sets for the following contexts:

- **SSL/TLS.** Rule set that detects SSL/TLS anomalies, misbehavior and self-signed certificates.
- **HbbTV.** Detects HbbTV channels and can block HbbTV.
- **Regex.** Detects strings that can be modeled by a regex, e.g. credit card numbers or account numbers.

In total, more than 2300 rules are deployed in the *Core Protector*. The number of rules could vary since the amount of user-generated HbbTV rules and some integrated blacklists are subject to change. In the next sections, we explain the rules in more detail and show some examples.

SSL/TLS Rules

We deploy different rules that handle three different types of SSL/TLS issues and misbehaviors:

Detection of malicious SSL/TLS certificates. Malicious SSL/TLS certificates are known to be related to malware or botnet activities. Smart TVs that receives malicious certificates are likely to be under attack and those could cause privacy risks for consumers. We implemented a list of rules for Suricata from abuse.ch [100]. This list includes SHA1 checksums of malicious certificates. The format for these rules are as follows:

```
1 alert tls any any -> any any (msg:"SSL Fingerprint Blacklist: Malicious SSL certificate detected (Gozi
    MITM)"; tls.fingerprint:"00:38:72:2d:4a:a0:ef:28:a0:da:69:1b:e9:fd:ae:68:54:9d:e5:c7"; sid:902329844;
     rev:1;)
```

The list contains more than 2200 fingerprints of malicious certificates. Updates of this list are regularly published.

Detection of SSL/TLS anomalies. Different anomalies in SSL/TLS could occur, e.g., invalid headers, invalid certificates, heartbeat attack. If the Smart TV is vulnerable for some of the anomalies and does not process these issues correctly, attacks on the Smart TV's underlying operation system could be performed. We try to protect the Smart TV against such requests. For the SSL/TLS anomaly detection we use the rule set provided in [101]. A sample rule is:

```
alert tls any any -> any any (msg:"SURICATA TLS certificate invalid length"; flow:established; app-layer-
    event:tls.certificate_invalid_length; flowint:tls.anomaly.count,+,1; classtype:protocol-command-
    decode; sid:2230007; rev:1;)
```

The list includes 20 Suricata rules for the anomaly detection.

Detection of self-signed certificates. For the detection of certificates that are issued by the same entity and should not be accepted by the Smart TV, we deployed the technique explained in [102]. The rule is as follows:

```
alert tls any any -> any any (msg:"SURICATA TLS Self Signed Certificate"; flow:established; luajit:self-
    signed-cert.lua; tls.store; classtype:protocol-command-decode; sid:999666111; rev:1;)
```

For this rule the IPS has to support Lua[9] scripting. Lua is a programming language and the corresponding Lua script is:

```
1 function match(args)
2     version, subject, issuer, fingerprint = TlsGetCertInfo();
3
4     if subject == issuer then
5         return 1
6     else
7         return 0
8     end
9 end
```

This presented Lua script performs the comparison between subject and the issuer.

HbbTV Rules

We discuss three different types of HbbTV specific Suricata rules:

Detection of HbbTV. The HbbTV detection rule finds HbbTV channels and generates a log entry. The detection is performed by identifying an HbbTV application with searching for a specific HTML object containing `application/oipfApplicationManager` in the requested HbbTV web page. All HbbTV applications need to implement this fragment because it enables the HbbTV browser of the Smart TV to display the HbbTV content. The used rule is as follows:

```
alert http any any -> any any (msg : "Found HbbTV" ; content : "application/oipfApplicationManager" ;
    classtype: policy-violation; sid:50; rev:1; )
```

The HbbTV channel is detected in the first response that provides the HbbTV notification.

HbbTV Blocking. An HbbTV application can be blocked by the following rule:

```
drop http any any -> any any (msg : "Blocked HbbTV: {HbbTV}" ; content : "{HbbTV}" ; http_host ;
    classtype: policy-violation ; sid : i ; rev: 1 ; )
```

{HbbTV} describes the extracted URI from the above mentioned detection rule. Basically, it detects and blocks a request to a specific HbbTV resource.

Regular Expression Rules

Rules that detect and block based on regular expressions can find static content. Basically, they detect strings with specific patterns. A selection which we implemented is shown below:

Credit card numbers. Credit card numbers have a specific format that is defined by each company. We implemented the following rules for credit cards:

```
1 # Visa Card
2 alert tcp any any -> any any (msg:"Found Visa credit card number"; pcre:"/4[0-9]{12}(?:[0-9]{3})?/";
      classtype:string-detect; sid:999001;)
3
4 # Master Card
```

[9] https://www.lua.org/

```
5 alert tcp any any -> any any (msg:"Found MasterCard credit card number"; pcre
      :"/(?:5[1-5][0-9]{2}|222[1-9]|22[3-9][0-9]|2[3-6][0-9]{2}|27[01][0-9]|2720)[0-9]{12}/"; classtype:
      string-detect; sid:999002;)

7 # American Express
8 alert tcp any any -> any any (msg:"Found American Express credit card number"; pcre:"/3[47][0-9]{13}/";
      classtype:string-detect; sid:999003;)

10 # Diners Club
11 alert tcp any any -> any any (msg:"Found Diners Club credit card number"; pcre:"/3(?:0[0-5]|[68][0-9])
      [0-9]{11}/"; classtype:string-detect; sid:999004;)

13 # Discover Card
14 alert tcp any any -> any any (msg:"Found Discover credit card number"; pcre:"/6(?:011|5[0-9]{2})
      [0-9]{12}/"; classtype:string-detect; sid:999005;)

16 # JCB Card
17 alert tcp any any -> any any (msg:"Found JCB credit card number"; pcre:"/(?:2131|1800|35\d{3})\d{11}/";
      classtype:string-detect; sid:999006;)
```

All major credit card numbers should be covered by these rules.

Account numbers. We implemented a German IBAN numbers detection. For each country the format differs slightly. The following rule detects them:

```
1 alert tcp any any -> any any (msg:"Found account number"; pcre:"/DE\d{2}[ ]\d{4}[ ]\d{4}[ ]\d{4}[ ]\d{4}[
      ]\d{2}|DE\d{20}/"; classtype:string-detect; sid:999011;)
```

If other countries should be detected, the corresponding regular expression for the IBAN have to be added.

MAC addresses. MAC addresses identify a network adapter of a device uniquely. We deployed the following rules to detect them:

```
1 alert tcp any any -> any any (msg:"Found MAC address with hyphen"; pcre:"/[0-9a-fA-F\p{L}\p{N}\p{Pd
      }]{17}/"; classtype:string-detect; sid:996002;)

3 alert tcp any any -> any any (msg:"Found MAC address with colons"; pcre:"/([0-9a-fA-F]{2}[:]){5}([0-9a-fA
      -F]){2}/"; classtype:string-detect; sid:996003;)

5 alert tcp any any -> any any (msg:"Found MAC address with points"; pcre:"/([0-9a-fA-F]{4}[.]){2}([0-9a-fA
      -F]){4}/"; classtype:string-detect; sid:996004;)
```

These rules detect MAC addresses with three different delimiters.

Other strings or information that can be formulated as a regular expression pattern can be added to the rule set of Suricata.

9.4.3 Processing

In this section, we describe how the log entries that are generated by the rules in Section 9.4.2 are processed. For all our purposes, we need to monitor the log file `eve.json`, which is a collection of all results from matched rules in JSON[10] format. Suricata is configured so that all necessary data is stored in the mentioned JSON log file.

We extract the following information from the log file:

- Local IP addresses in order to determine the device name. The assignments from IP to device name are stored in the *database*.

[10] `http://www.json.org/`

- Extraction of HbbTV URLs for the *HbbTV list* and the *database*.
- Extraction of all SSL/TLS events, e.g. self-signed certificates.
- Extraction of all regular expression events, e.g. credit card number.

All mentioned information is extracted in the *Information Extraction and Processing* step.

Information Extraction and Processing

We discuss in this section how the *Core Protector* extracts information from the log entries. We describe for each information which fields are relevant. The following listing shows a log entry that was generated by one of our HbbTV detection rules:

```
{"timestamp":"2017-02-28T22:06:24.103514+0100","flow_id
   ":1778777454558932,"event_type":"alert","src_ip":"95.101.82.10","
   src_port":80,"dest_ip":"192.168.0.12","dest_port":59635,"proto":"TCP
   ","tx_id":0,"alert":{"action":"allowed","gid":1,"signature_id
   ":997001,"rev":1,"signature":"Found HbbTV","category":"Potential
   Corporate Privacy Violation","severity":1},"http":{"hostname":"hbbtv.
   redbutton.de","url":"\/service\/redbutton.php?brand=s1de","
   http_user_agent":"HbbTV\/1.1.1 (;;;;;) Maple_2011","http_content_type
   ":"application\/vnd.hbbtv.xhtml+xml","http_method":"GET","protocol":"
   HTTP\/1.1","status":200,"length":6478}}
```

The shown log entry is from our Samsung UE40D6200 Smart TV and requested HbbTV on the channel *Sat. 1*. Since it was an HTTP request, additional HTTP fields were saved in the log file. The following information is extracted:

Local IP addresses. The IP addresses of local devices can be extracted from the two fields: `src_ip` and `dest_ip`. In order to extract only local IP addresses, it is necessary to read the configuration entry from the *database* that sets the local network. It is checked whether the IP address is already known and saved in the database. If known, no further action is required. If not, the IP address is saved for processing by the device detection (see next section).

HbbTV events. We detect HbbTV events by their `signature_id`. It describes the fired rule and therefore, we can create an entry in the *database*. These *database* entries will be displayed on the graphical user interface of the *Smart TV Protector Controller*.

HbbTV URLs. If the `signature_id` (e.g. 997001) of the rule that detects HbbTV channels is fired, the URL of the HbbTV channel can be extracted from the field `hostname`. The found URL is added to the *HbbTV list*. Duplicates are not added.

SSL/TLS Events. The SSL/TLS events are extracted when corresponding rules fire. They are saved in the *database* in order to present it to the consumers. The detected certificates are saved in a separate folder and so they can be analyzed afterwards, if necessary.

Regular Expression Events. When a rule with a regular expression pattern has fired, an appropriate entry is added to the *database*. Note, the value itself (e.g. credit card number) is not saved, since it could cause privacy risks if the credit card number is saved in plain text in the *database*.

For extracting this information, we developed a script entirely written in Python that monitors the `eve.json` file and regularly processes new log entries. The source code can be found in appendix G.

Device Detection with SSDP

It is essential that the correct Smart TV is automatically named correctly or at least appropriately. There are several reasons: (1) some detection rules are customized to specific Smart TV vendors or models. For example the rules that control the support for settings that can be controlled on the Smart TV, (2) the user interface should show the right name for the consumers.

We show six methods to establish it, sorted from automatic to (semi-)manual:

- The *Simple Service Discovery Protocol* (SSDP) provides a method where devices can announce their services. It is accomplished by sending multicast messages in the network via UDP port 1900 [103]. SSDP is a part of the UPnP Standard. In the data packets that are sent is a header field which states the model name of the Smart TV [104] (see Figure 9.9 for an example for the corresponding lines). If SSDP messages are not detected in a specific time frame, we can also actively discovery the network with a SSDP Discovery. As far as we know all Smart TV vendors implement UPnP for sharing functionality they offer in the network.

```
1 <friendlyName>[TV]UE40D6200</friendlyName>
2 <manufacturer>Samsung Electronics</manufacturer>
```

Figure 9.9.: SSDP message with friendly name and the vendor's name.

  In our tests we could distinguish between three Samsung Smart TV models (UE40D6200, UE40ES6300, UE40JU6580) and three LG Smart TV models[11] (42LN5758, 47LB650V and 32LF6309).

- The *User-Agent* header field in an HTTP request contains information about the user agent performing the request. By convention, the product tokens are listed in order of their significance for identifying the application or service [105]. In our surveys, we found that even different services on Smart TVs send different User-Agent header fields. Figure 9.10 shows a request of the DLNA client where the *User-Agend* field contains the model number of the LG Smart TV.

```
User-Agent: Linux/3.0.13 UPnP/1.0 LGE_DLNA_SDK/1.6.0 [TV][LG]42LN5758-ZE/04.22.07 DLNADOC/1.50
```

Figure 9.10.: Example of a user agent field.

- The *MAC address* is the most commonly used network interface identifier that should be globally unique. The first three octets of the MAC address are assigned to an organization. IEEE publishes updated lists frequently [106]. Therefore, if other methods for device detection fail at least the vendor can be estimated. If a vendor uses a network interface card from a different manufacturer, the detection will most likely result in the manufacturer's name.

- If any other method fail the device will be marked as unknown. *Machine Learning* could be used to characterize the network traffic and tries to label them according to a global set of data. Support Vector Machine algorithms have been a good choice for this scenario so far (see [107]). We did not implement this method. Further research would be necessary.

- If the name detection of a device was entirely wrong. The user can give *user feedback* and enter the name manually in the *Smart TV Protector Controller*.

[11] for these models we extracted the field *DLNADeviceName.lge.com*.

We decided to implement the detection over the SSDP protocol. We implemented an active test, i.e. we send a SSDP discovery request to all devices in the network and collect the responses, extract the names and store the names. We extended the script from [108] as follows[12]:

```
def friendlyNames():
    devices=discover("ssdp:all")
    device_data=[]
    for device in devices:
        try:
            f = urllib2.urlopen(device.location)
            data=f.read()
            odata=data
            if "<friendlyName>" in data:
                fn=data[:data.rfind("</friendlyName>")]
                fn=fn[fn.rfind("<friendlyName>")+len("<friendlyName>"):]

                mn=data[:data.rfind("</modelName>")]
                mn=mn[mn.rfind("<modelName>")+len("<modelName>"):]

                try:
                    fn=unicode(fn)
                except:
                    try:
                        mn=unicode(mn)
                        fn=mn
                    except:
                        fn="Not known"

                hostname=urlparse(device.location).hostname
                host=socket.gethostbyname(hostname)

                device_data.append( (host,fn,mn) )
            f.close()
        except:
            print device.location+" not possible"
    return device_data

def main():
  print "started"

  f=open("ssdp.txt", 'w')
  f.write("%s\n" % (time.time()))
  for item in friendlyNames():
    f.write("%s|%s\n" % (item[0], item[1]))
  f.close()
```

This script is entirely implemented in Python and is executed regularly. The generated file with a pair of IP and name are updated whenever the script runs. Device names that are changed manually by the consumer are not updated, however a tool tip with the detected name can be display. The source code can be found in Appendix G.

Consumer Decision to Rules

We regularly check the *database* for updates of the HbbTV rules. We extract the updates and create new rules in the *database* of the *Core Protector*. The rule format is specified in Section 9.4.2.

9.4.4 Implementation

The *Core Protector* was evaluated on a Ubuntu Linux 16.04 LTS[13] System with Suricata 3.2RC1[14]. We used the following IPTables rules to enable the system to process all requests:

[12] The full source code can be found in Appendix G

[13] https://www.ubuntu.com/

[14] https://suricata-ids.org/

```
sudo iptables -F FORWARD
sudo iptables -I FORWARD -j NFQUEUE
sudo iptables -t nat -A POSTROUTING -o ens33 -j MASQUERADE
```

It enabled Suricata to process all packets that are forwarded through the *Smart TV Protector*. We tested the system on a virtual machine. We could not identify any performance issues.

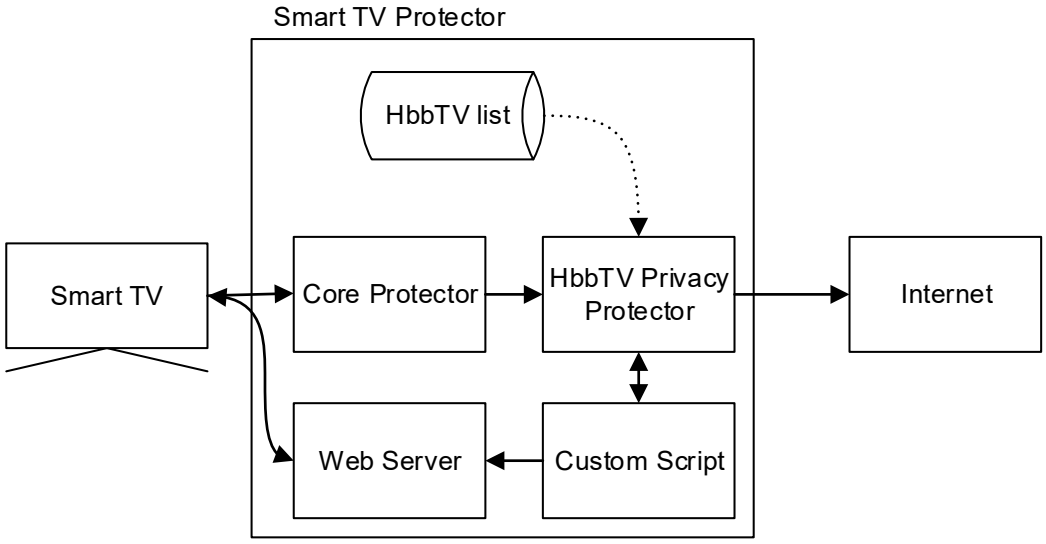
The mentioned Python scripts were tested on the same virtual machine. Since this implementation is a prototype, some errors will not be handled automatically.

9.5 HbbTV Privacy Protector

We present an overview of the *HbbTV Privacy Protector* in Section 9.5.1. Based on a custom script that is explained in Section 9.5.2, the *HbbTV Privacy Protector* decides whether the request is answered by the web server that is discussed in Section 9.5.2 or directly forwarded to the Internet. Finally, we give some details of the implementation in Section 9.5.4.

9.5.1 Overview

The *HbbTV Privacy Protector* extends the *Core Protector* so that consumers are able to decide whether HbbTV should be executed directly on the Smart TV's screen. The *HbbTV Privacy Protector* only modifies traffic that depends to HbbTV. The *HbbTV list* that is generated by the *Core Protector* serves as a white list to detect HbbTV URLs.



dotted line: data that is processed by the *Core Protector*; solid line: network traffic.

Figure 9.11.: Overview of the HbbTV Privacy Protector.

As outlined in Figure 9.11 the *Core Protector* forwards, if not blocked, the traffic from the Smart TV to the *HbbTV Privacy Protector*. If the traffic is HTTP, the *HbbTV Privacy Protector* processes the traffic with a *custom script*. The *custom script* checks whether the requested URL is on the *HbbTV list* and how the status is (*Allow Channel* or *Always Ask*). Note, the blocked HbbTV channels are blocked by the *Core Protector*. If the HbbTV channel status is always ask, the *Web Server* delivers a notification to the Smart TV. This notification states that HbbTV was detected and the consumer can activate it by pressing the *Green Button* on his/her remote.

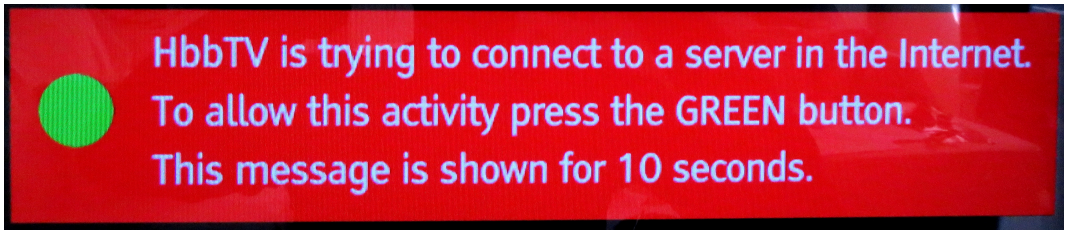


Figure 9.12.: *HbbTV Privacy Protector* notification for consumers on the Smart TV.

Figure 9.12 shows the message displayed to consumers when *Always Ask* is selected. The default setting is that this message is automatically closed after ten seconds.

Technically, we decided for the software mitmproxy[15] that acts as the core of the *HbbTV Privacy Protector*. In the remainder of this section, we explain the components of the *HbbTV Privacy Protector* in more detail.

9.5.2 Custom Script

The *Custom Script* extends the basic functionality of mitmproxy. In more detail, the *custom script* performs the following steps (see Figure 9.13):

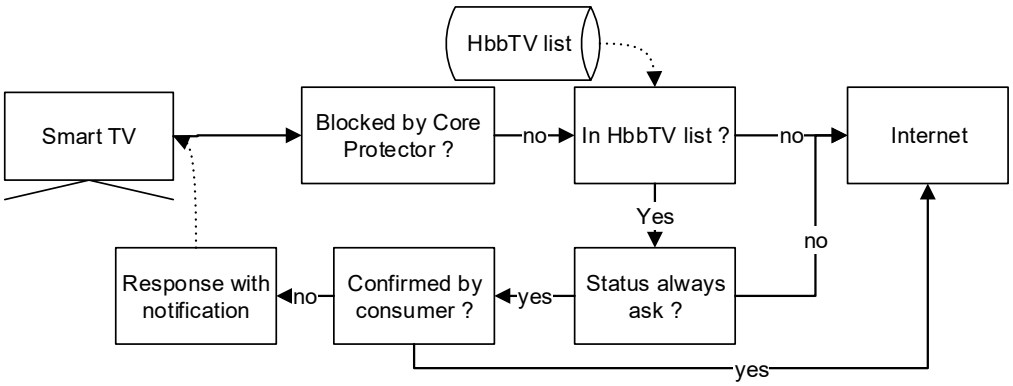


Figure 9.13.: Overview of the interception process of the *HbbTV Privacy Protector*.

1. It loads the *HbbTV list* generated by the *Core Protector* and the current status (*Allow Channel* or *Always Ask*) for each HbbTV channel.
2. If the status of an HbbTV channel is *Always Ask* and is detected, the network traffic is intercepted and an interception rule is set. The interception rule states that the traffic is forwarded to the *Web Server*. If the status is *Allow Channel*, no action is taken and the HbbTV application is load from the Internet.
3. The original HbbTV request by the Smart TV is answered with a redirect that redirects the Smart TV to the *web server*. As long as the interception rule is set, the Smart TV communicates with the *Web Server*.
4. If the consumer presses the *Green Button* on the remote (detected by a request of `http://1.2.3.4/do-not-inte` the Smart TV will be redirected to the original HbbTV application in the Internet.

The full source code can be found in the Appendix G.

[15] `http://www.mimproxy.org`

9.5.3 Web Server

The *Web Server* delivers an alternative HbbTV application to the Smart TV. This application serves as a dummy to protect the consumer. It presents information how the consumer can activate the broadcaster's HbbTV application. We implemented the text that is shown in Figure 9.12. We decided for the *Green Button* on his/her remote in order to not confuse the consumers with the *Red Button*.

If the message is displayed and the consumer presses the *Green Button*, a JavaScript event is triggered. The corresponding source code that is delivered to the Smart TV is:

```
1 function handleButton (e) {
2   if (e.keyCode == GREEN_BUTTON)
3   { show(false); document.location.href = 'http://1.2.3.4/do-not-intercept'; }
4 }
```

The JavaScript sends a redirect to the Smart TV that tries to request the web site with the URL `http://1.2.3.4/do-not-intercept`. This request is intercepted by the *Custom Script* and the original broadcaster's HbbTV application is requested.

In order to enable the *Web Server*, here Apache Web Server, to provide an HbbTV application the mime type of HbbTV had to be added to the configuration. The HbbTV mime type is

```
1 application/vnd.hbbtv.xhtml+xml        hbbtv
```

The full source code of the HTML files can be found in Appendix G.

9.5.4 Implementation

We implemented the *HbbTV Privacy Protector* for two different purposes. We implemented it on top of the *Raspberry Pi* architecture to run as a stand-alone appliance and for the *Smart TV Protector* on top of *Ubuntu Linux*.

The *HbbTV Privacy Protector* for the *Raspberry Pi* platform, a small ARM based computer that is quite popular for building TV media centers, was on top of the Raspbian[16] Linux operating system. To operate properly the Smart TV Internet traffic needs to be routed through the *Raspberry Pi* for example using the Internet connector and can then be passed on to the local Wi-Fi using a USB Wi-Fi adaptor. The small device size makes it possible to mount it on the Smart TV's backside, out of sight. Even the USB port of the Smart TV can be used to power the *Raspberry Pi*. As an advantage it starts automatically when switching on the Smart TV. The software and the pre-packed Raspbian are available on our website[17].

The Raspbian image is pre-configured to work with the USB Wi-Fi adaptor EDIMAX EW-7811UN. The system boots and starts directly the mitmproxy with our script. The on-board LAN port has to be connected to the device and the USB adaptor connects to the home network. At the moment only WPA and WPA2 networks are supported. As language we have a German and an English version. For using the graphical configuration interface the LAN port has to be connected to a computer. The user interface can then be requested by entering http://192.168.10.1 in a web browser. On the LAN port the DHCP server is assigning IP addresses, so a direct connection to a home network is not recommended. Additionally, we had to implement the HbbTV detection manually in the custom script to run the *HbbTV Privacy Protector* stand-alone.

[16] `https://www.raspbian.org/`
[17] `http://www.smarthome.sit.tu-darmstadt.de`

For the combination with the *Core Protector* and therefore for the usage in the *Smart TV Protector*, we double checked the software to be compatible with Ubuntu Linux.

In both versions, we used mitmproxy[18], a lightweight HTTP and HTTPS interception proxy written entirely in Python. Technically, the mitmproxy waits for connections on port 8080 for HTTP and HTTPS connections. The underlying Linux can transparently forward traffic from port 80 (HTTP) and 443 (HTTPS) to 8080. The Smart TV cannot detect this redirection. *Iptables* is used for this task (see Figure 9.14). Due to performance reasons, we ignore all network traffic that belongs to an image or video.

```
1 iptables -t nat -A PREROUTING -i eth0 -p tcp --dport 80 -j REDIRECT --to-port 8080
2 iptables -t nat -A PREROUTING -i eth0 -p tcp --dport 443 -j REDIRECT --to-port 8080
```

Figure 9.14.: Example of iptables commands.

9.6 Evaluation

We technically evaluated the components of the *Smart TV Protector*. In particular, the *Core Protector* is based on the open source software Suricata that is tested by the development community thoroughly. Therefore, we only tested our deployed rules and scripts. We also did not test the mitmproxy that we use for the *HbbTV Privacy Protector* due to the same reason.

The following tests were performed in order to evaluate the deployed rules:

- We evaluated the detection of self-signed certificates with created web sites that were requested on the Smart TVs, which were all detected. Other SSL/TLS anomalies were only tested with modified rules, since we did not have a malicious CA or certificate that we could test with these rules. It is likely that all rules fire as expected.

- We tested the HbbTV URL extraction with our test Smart TVs on live data. It has proven to be reliable. However, to detect an HbbTV application with our deployed method, the first request has to be performed. The broadcaster could detect the first contact.

  Furthermore, our blocking rules block the HbbTV application before they are able to contact the broadcaster's server. Note, HbbTV is only blocked if the consumer decides so.

- We were able to detect credit cards numbers as well as account numbers. In order to test it, we created web sites with valid credit card numbers as well as account numbers. The *Core Protector* detected this sensitive information. However, if the data is written in a different format, e.g. more spaces or other delimiters it might be missed.

- We were able to detect MACs of the connected Smart TVs in network packets. We tested the rules on a live capture of one of our Samsung Smart TVs.

The detection of the Smart TV model was performed with an active process. It were possible to detect all our test Smart TVs. However, on LG, we had to check the DLNA values in UPnP.

The *HbbTV Privacy Protector* were evaluated in real households as a stand-alone device and in combination with the *Smart TV Protector*. While developing the *HbbTV Privacy Protector*, we found that Samsung devices sent a HEAD request as the first packet to the HbbTV provider. Other vendors do not perform an HEAD request. Therefore, a differentiation without the inspection of packets is not possible. Therefore,

[18] `http://www.mimproxy.org`

we use the *Core Protector* for detecting HbbTV. It is possible that we miss HbbTV applications that changed the URL shortly. However, as long as the detection works, it is only a short period of time.

We discuss limitations of the Smart TV Protector:

- The *Smart TV Protector* is not able to break HTTPS. We did not found an option to import own certificates in the Smart TVs. Requests with HTTPS could not be inspected by our approach. But, some extensions of HTTPS such as server name indication (SNI) could be used to identify the destination of the data packets. Therefore, the content is not analyzable but the destination. Often that is sufficient to decide if a connection is legitimate.
- If Smart TVs implement protocols that are not standardized, it is difficult to analyze them. Blocking is always possible but could lead to false positives and broken functionality.
- The presented consumer support that assists the consumers to configure their Smart TVs is only available for Smart TVs, which are explicitly added to the *database*. A community approach would help to add appropriate information for more Smart TV models.

9.7 Related Work

To the best of our knowledge, there is no protection system that is specialized for Smart TVs. However, some technologies are related to our prototype:

Software for protecting privacy. Privoxy [109] is a proxy that handles web traffic. It has advanced filtering capabilities for protecting user's privacy. It can manipulate data on transit. We are not aware that it can protect consumer's privacy on Smart TVs, for example for HbbTV. If necessary, privoxy can be chained with our solution to enhance the privacy protection further.

Intrusion detection/prevention systems. An overview of intrusion detection systems is presented in [110, 111]. A variety of DLP products are on the market [112]. All of them are not customized for Smart TVs and therefore can only handle general issues.

Firewall. Enterprise networks are usually protected by hardware or software based firewall systems. Almost every home router for households implements a limited amount of firewall functionality. Firewalls can protect against active attacks. Chen *et al.* outlined that misconfigurations of firewall policies may result in unexpected behavior, such as allowing unauthorized traffic or disallowing legal traffic [113]. A firewall-like system with a smart phone app is in development [114]. The reason why consumers are mostly not able to configure it, is that policies can become too complex to understand and manage them.

Guidelines for securing Smart TVs. Guidelines how to secure the smart home can be found in [115, 116] and especially for Smart TVs [117]. However, all of them require that the consumers knows how to configure the system.

9.8 Discussion and Summary

In this chapter, we presented the *Smart TV Protector* that protects consumers' privacy. We explained the three components: the *Smart TV Protector Controller*, the *Core Protector* and the *HbbTV Privacy Protector*.

The *Core Protector* monitors network traffic sent and received by the Smart TV. It is able to block specific traffic based on rules that we described in detail. The *HbbTV Privacy Protector* is an HbbTV specialized

component. It is able to allow or block HbbTV applications depending on consumers' decisions. Consumers can decide whether they want to load the HbbTV application. This decision can be performed directly on the Smart TV's screen with a customized notification that is presented to the consumer. The *Smart TV Protector Controller* serves as a control unit that enables consumers to configure the *Core Protector* and the *HbbTV Privacy Protector* on a graphical user interface. It offers a web user interface that can be requested on any device with a current web browser.

We have shown that our *Smart TV Protector* can reduce privacy risks that are caused by Smart TV related Internet functionality. Especially, the *HbbTV Privacy Protector* gives consumers the option to control HbbTV applications on a specific channel. We evaluated the *HbbTV Privacy Protector* as a stand-alone system.

We intentionally used a blacklisting for HbbTV since it is the most convenient concept for consumers. They would not recognize a malfunction of any device if no rule matches. However, from a security point, it is a more insecure concept because malicious or privacy leaks occur without knowledge of the consumers.

Thus, it is important to generate appropriate rule sets for households. An approach could be to connect the *Smart TV Protector* to a global rule set. It could protect consumers' privacy better and the rule sets are based on more households. For example if a consumer bought a new marketed Smart TV, the *Smart TV Protector* has no rules for it. It could request rules from a global rule set, download and use them in the local system. A challenge is to define the process how to establish a global rule set without manipulation and privacy risks. Privacy risks could occur if a locally deployed *Smart TV Protector* shares its data with the global rule set without any anonymization techniques. On the one hand people benefit from a global rule set but on the other hand the household that shares the data may leak some sensitive information.

As future work it is worthy to extend the *Smart TV Protector* to detect outdated components of a Smart TV. It could warn consumers to update their Smart TVs, which would further help to reduce privacy risks and security vulnerabilities.

10 Developing an Alternative respecting Broadcasters' and Vendors' Interests

In Section 9, we discussed the *Smart TV Protector* where the Smart TV consumer could decide whether data transfers are permitted or not. However, based on our surveys (see Sections 5-8) some participants justified their responses that usage data is important to improve the product or the TV program, so we discuss our proposal that develops a solution which is a trade-off between privacy and the interest of third parties: the *Privacy Protecting Collector*.

In Section 10.1, we discuss technical requirements. We present an overview of our proposal in Section 10.2 and discuss both parts, the *Collector* (Section 10.3) and *Central Share* (Section 10.4). We describe our evaluation in Section 10.5. In Section 10.6, we report on related work. We summarize and discuss our approach in Section 10.7. We published parts of this chapter in [26, 27]. In these publications we presented a broader concept called PriMSED and PriSEMD. Both were considered for Smart Entertainment Devices. Here, we present that concept focused on Smart TVs.

10.1 Requirements

The functional requirements for the *Privacy Protecting Collector* are based on the revised OECD privacy principles from 2013 [118]. The OECD website[1] states:

> *The OECD Privacy Principles provide the most commonly used privacy framework, they are reflected in existing and emerging privacy and data protection laws, and serve as the basis for the creation of leading practice privacy programs and additional principles.*

We quote the principle from the OECD guidelines and explain our corresponding requirement:

> ***Collection Limitation Principle.*** *There should be limits to the collection of personal data and any such data should be obtained by lawful and fair means and, where appropriate, with the knowledge or consent of the data subject.*

The Smart TV usage data should only be collected by the *Privacy Protecting Collector* and transmitted to a third party with the knowledge or consent of the consumer. A mechanism must be in place that takes care of this requirement.

> ***Data Quality Principle.*** *Personal data should be relevant to the purposes for which they are to be used, and, to the extent necessary for those purposes, should be accurate, complete and kept up-to-date*

The usage data that is produced by the Smart TV and collected by the *Privacy Protecting Collector* should be relevant to the purposes for which they should be used. It should be accurate and kept up-to-date in a specific time period. No other data than needed should be collected.

> ***Purpose Specification Principle.*** *The purposes for which personal data are collected should be specified not later than at the time of data collection and the subsequent use limited to the fulfilment of those purposes or such others as are not incompatible with those purposes and as are specified on each occasion of change of purpose.*

[1] `http://oecdprivacy.org/`

The purpose for which the *Privacy Protecting Collector* collects Smart TV usage data should be specified before it stores and analyzes the data. Other data should not be collected and data that is collected due to technical circumstances should be removed immediately.

> ***Use Limitation Principle.*** *Personal data should not be disclosed, made available or otherwise used for purposes other than those specified in accordance with Paragraph 9 except:*
>
> *a) with the consent of the data subject; or*
>
> *b) by the authority of law.*

Smart TV usage data should not be disclosed, made available or otherwise used for purposes other than those specified in accordance with the last mentioned requirement "Purpose Specification Principle". It is hard to enforce it technically but it should be communicated to all third parties that have access to the data collected by the *Privacy Protecting Collector*.

> ***Security Safeguards Principle.*** *Personal data should be protected by reasonable security safeguards against such risks as loss or unauthorised access, destruction, use, modification or disclosure of data.*

Smart TV usage data should be protected by reasonable methods against privacy risks and unauthorized access, use, modification or disclosure of data. We try to fulfill this requirement with some privacy preserving methods.

> ***Openness Principle.*** *There should be a general policy of openness about developments, practices and policies with respect to personal data. Means should be readily available of establishing the existence and nature of personal data, and the main purposes of their use, as well as the identity and usual residence of the data controller.*

All methods that are used to process and analyze Smart TV usage data should be publicly available. Furthermore, it should be communicated which party has access to which data. The consumer should be informed about the usage data that is produced by the Smart TV.

These requirements are incorporated in the *Privacy Protecting Collector*. Note, we do not discuss whether any Smart TV fulfills these requirements.

10.2 Overview of the Privacy Protecting Collector

The *Privacy Protecting Collector* is a concept that shows how audience measurement of Smart TVs could be realized with respect to consumers' privacy. The idea is to collect data in the household's local network and deliver it pre-processed to third parties in a privacy protecting format. Consumers are able to control which data is shared.

The *Privacy Protecting Collector* is split into two components: a device that collects the data locally in the household (*Collector*) and a centralized service that shares the data with third parties (*Central Share*).

The *Central Share* prepares the received data from *Collectors* and stores it for sharing with third parties. It provides a data store and the service for preparing the data to be shared in a privacy protecting format. One *Central Share* can process data from n different *Collectors* in the same or different households (see Figure 10.1). The location of the *Central Share* is at a trustworthy third party that has no interest on the data collected, e.g. a university.

10.3 Collector

We give an overview of the *Collector* in Section 10.3.1 and describe the process how the data is processed in Sections 10.3.2, 10.3.3, 10.3.4 and 10.3.5. Finally, we explain our implementation in Section 10.3.6.

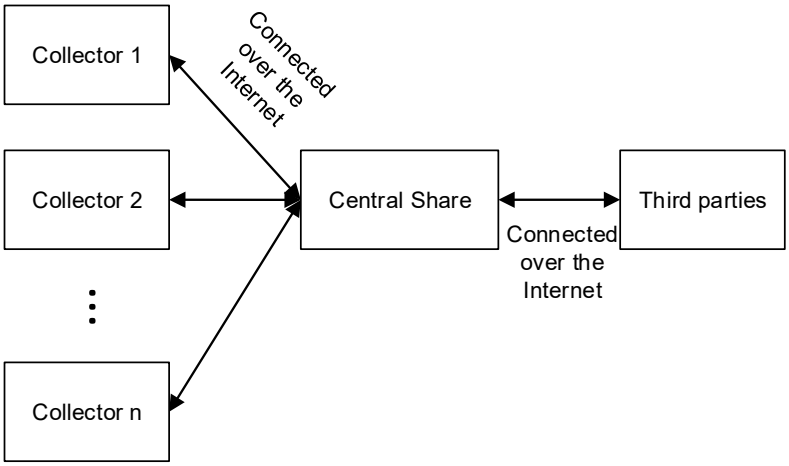


Figure 10.1.: Overview of the *Privacy Protecting Collector*.

10.3.1 Overview

A *Collector* is supposed to be installed in the household between one or more Smart TVs and the connection to the Internet.

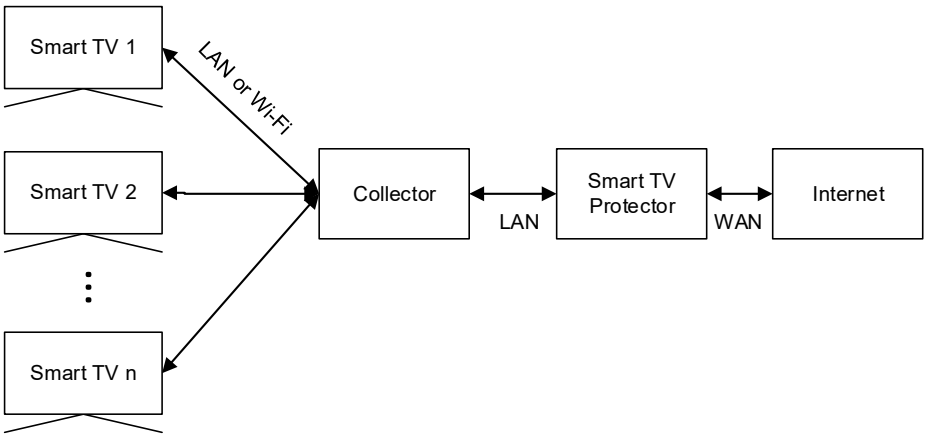


Figure 10.2.: Overview of a *Collector*.

As depicted in Figure 10.2, the *Collector* is connected with a limited number of Smart TVs, the *Smart TV Protector* and a home router that is connected to the Internet. The *Smart TV Protector* protects consumers against privacy risks as explained in Chapter 9. Each *Collector* processes data in four steps (see Figure 10.3):

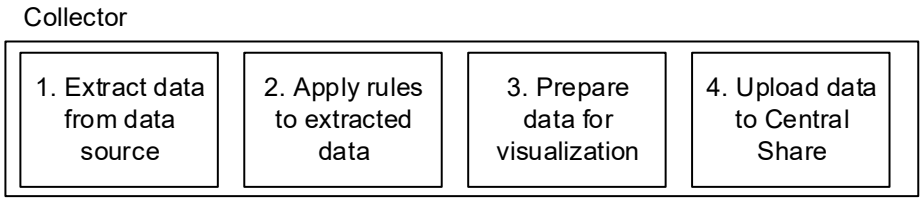


Figure 10.3.: Data processing of a Collector.

First, extract data from the data sources. It extracts data produced by many services: UPnP, infrared data, browser activities, HbbTV, DNS services, DHCP and many more. Each of them reveals different information depending on the service and the Smart TV model.

Next, rules that defines which information is needed are applied to the data. The resulting data is then prepared for visualization and afterwards uploaded to the *Central Share*.

A *Collector* does not manipulate any data, i.e. data is monitored and information is saved. We explain the process in more detail in the following sections.

10.3.2 Extract Data from Data Sources

In the first step, the *Collector* extracts all data that contains information and prepares it for further processing. We explain important data sources, which information can be extracted and how the extraction process is designed:

Network agent. The network agent is the main data source of the *Collector*. It collects different kind of data from services and protocols: DHCP, UPnP, HTTP, HTTPS and HbbTV. The most important services for our proposal are explained below:

- **HbbTV.** Hybrid Broadcast Broadband TV as explained in Section 2 is a protocol to deliver content on top of the running TV program. The content is delivered by the broadcaster, so it is possible to identify the communication partner of the TV and determine which TV program is watched on an HbbTV supporting Smart TV. HbbTV is transferred via HTTP or HTTPS and different channels are using different requests, so it depends on the channel how fast the running program can be detected and how accurate the information is. Generally, it is possible to detect the channel at turn-on time. On some channels a detection is even possible when a program is already running due to periodic requests to the broadcasters.

- **DHCP.** The Dynamic Host Configuration Protocol (DHCP) [119] is used to assign dynamic IP addresses to hosts in a network. Here, we can detect if a Smart TV requests an IP address, this means that the Smart TV was not a member of the network. In most cases, the Smart TV was turned on or an IP renewal has been requested. We check the MAC[2] address of the new IP if the Smart TV already occurred in the network, so we can distinguish between both cases. If the DHCP address is released we infer that the Smart TV has been turned off. However, not all Smart TVs release DHCP addresses properly. Hence, the turn off time may be missed. To overcome this issue, we use information coming from other protocols like UPnP or ICMP[3] requests.

- **UPnP/SSDP.** The Universal Plug and Play (UPnP) protocol [104] is a vendor independent protocol to control devices over an IP network. Many Smart TVs are using parts of UPnP. The Simple Service Discovery Protocol (SSDP) for example is used to announce a device in the network. It broadcasts packets on port 1900/udp in the network. Information like device names can often be extracted. In many cases some control services are announced. SSDP-Alive resp. SSDP-ByeBye packets can help to determine if a Smart TV is turned on or off. Depending on the Smart TV model the implementation level of UPnP differs. For example, some Smart TVs are only announcing their media player functionally with DLNA[4] support. However, device names are often included in plain text and can be extracted. No security techniques like encryption in this protocol could be detected. Thus, it is generally recommended that only local devices should respond to UPnP requests.

  Additionally, we have identified some Smart TV services that reveal the current channel, the current volume or brightness of the display. The list of information that Smart TVs can provide over UPnP is much longer than the previous mentioned ones. In any case, this information can be used to clearly determine if a consumer is watching a channel.

[2] media access control address
[3] Internet Control Message Protocol
[4] Digital Living Network Alliance

- **HTTP.** HTTP is the standard method to request web pages in the Internet [44]. The content on Smart TVs is often delivered by third parties and in many cases the HTTP protocol is used. For example, HbbTV is a service provided over HTTP. From a HTTP data stream a lot of information can be extracted, e.g., which data is requested on a Smart TV, which video on demand services are used and so on.
- **HTTPS.** HTTPS is the encrypted and integrity safe version of HTTP [45] (see Chapter 4 for further information). The payload cannot be decrypted without the corresponding private key. But, meta data can be extracted in plain text. The communication partners can be inferred from the packets' source and destination. HTTPS has an extension called Server Name Indication (SNI) that can be used to identify the destination host of the request. This information can also give information about the request reason.

Infrared agent. Many Smart TVs can be controlled by infrared remote controls. The infrared signal is usually not secured, so it can be eavesdropped easily. However, the signal must be decoded appropriately, i.e., the signal contains some code that must be mapped to a function of the Smart TV in order to process it the right way. Examples for information that can be extracted are channel switching, muting, change the volume and so on. This data source is a supporting agent, i.e., the information can also be extracted from other sources.

Other vendor dependent services. On some Smart TVs we detected non-standardized services that transfer data to the Internet or in the local network. For example, on a set-top box we found an image request each time a channel was switched. It downloaded the channel logos from a vendor operated server. On some Smart TVs we detected requests to the vendor when the device was turned on.

Other useful services that are not listed here have not been found. But due to the modular system it can be extended by other data sources. After finishing this step, the data is prepared for applying rules in the next step. Note, in this step no data is permanently stored without consumer's consent.

10.3.3 Apply Rules to Extracted Data

After introducing the data sources for the *Collector*, we discuss the information extraction process in more detail. The *Collector* is part of a local network and can analyze traffic that is going from the home network to the Internet and vice versa. In order to extract the same information on each *Collector* the data is analyzed based on a rule set. The rule set is distributed by the *Central Share*. Therefore, we define a set of n rules that can be extended, but the *Central Share* distribution process must ensure that all *Collector* have the same version of rules.

A rule set R contains n rules. In Table 10.1 five example rules are defined. A rule r is formulated as a question with a boolean answer, e.g., whether a consumer is watching a specific TV channel. Generally, a rule's answer is true if the extracted information indicates that the fact is true. If not, false.

id	Rule	Answer
1	Is a Smart TV used ? ?	time schedule
2	Is channel A watched ?	time schedule
3	Is a Smart TV used in parallel to a Blu-ray player ?	time schedule

Table 10.1.: Example rules for the *Privacy Protecting Collector*.

For simplicity, we define an answer type *time schedule*, which groups many boolean answers. We split the day in slices of 15 minutes resulting in 96 boolean values. An example for an answer vector is shown in Table 10.2.

0:00 - 0:15	0:15-0:30	0:30 - 0:45	...	23:30 - 23:45	23:45 - 0:00
0	1	1	...	0	0

Table 10.2.: Example of day slices.

For each consumer in the household, any rule in Table 10.1 can be answered in the vector format shown in Table 10.2. In order to compare our system with today's audience measurement systems, a connection between age resp. gender is necessary. We define an illustrative set of age groups A (see Table 10.3).

id	gender	age	id	gender	age
1	f	0 - 15	5	m	0 - 15
2	f	16 - 30	6	m	16 - 30
3	f	31 - 50	7	m	31 - 50
4	f	51 -	8	m	51 -

Table 10.3.: Example of an age distribution.

In a household several people can belong to an age group a, so the vectors of those people are added. Hence, for each rule r in R and each age group a in A exists $x_{ra} = \{0, 0, ..., 2, 1\} \in \mathbb{Z}^{96}$, whereas $\max(x_{ra})$ is smaller than the number of people in the age group a. Therefore, each household submits a dataset $X = [x_{11}, ...x_{18}, ..., x_{n8}]$ of length $len(R) \cdot len(A)$ to the central share.

The *Collector* does not save any data that is not covered by a rule installed on the system.

10.3.4 Prepare Data for Visualization

The *Collector* provides a web application that presents the information which can be shared with a third party. Moreover, the consumer can decide which rule shall be answered with real data. If the consumer does not agree to answer a rule, all entries of the vector are 0. With this method the *Collector* cannot distinguish between real data and a declined rule.

In the web application consumers with correct login credentials can see real time data as soon as the time slice has been passed. Any data gathered by the *Collector* is stored for a limited time due to privacy and storage restrictions. The time can be defined by the consumer.

The age group assignment can be directly done on a Smart TV or, if no device with display is used, over a web browser enabled device afterwards.

10.3.5 Upload Data to the *Central Share*

The data is uploaded via HTTPS to the *Central Share*. It is checked if the *Central Share* can prove it's identity with the correct digital certificate. The data is transmitted once a day to avoid privacy issues when uploading information too early. We use an anonymity network such as TOR [120] that ensures privacy of each household. It is unlikely that the TOR network is attacked because of measuring viewing behavior, so we assume it is secure.

10.3.6 Implementation

The implementation of the *Collector* is Linux-based and completely written in Python. We use standard software: Apache 2, MySQL database server, WSGI and the Django framework for the web application.

All connections are handled over TLS/SSL.

The *Collector* has been tested on a Cubietruck 3 (C3) and a Raspberry Pi (RPi). The RPi has no infrared sensor, so the infrared source has been disabled. Both devices were configured to operate in a gateway mode. Any traffic coming from a Smart TV went through them and was relayed to the Internet gateway. No traffic manipulation has been made.

For the proof-of-concept we hard-coded the rules. An update of rules can be made with a software update.

Scapy[5] is a Python software for packet capturing and manipulation. It is used to capture the network traffic and extract the information for the mentioned protocols. For example if a DHCP packet is detected, a turn on/off event is created.

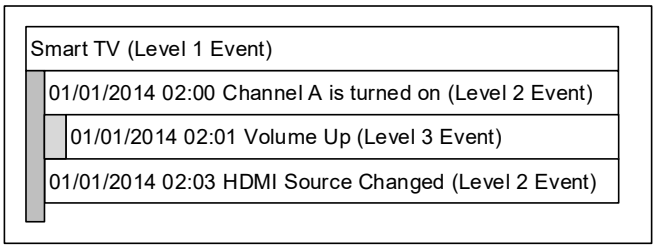


Figure 10.4.: Examples of some *Collector* events.

For the presentation layer, we built up a structure with different event levels (see Figure 10.4). An event is an action that is detected by an agent. The events are as follows:

- *Level 1 Events* are created if a SED is detected.
- *Level 2 Events* are connected to a level 1 event. Captured actions that belong to a specific SED are listed under a device. An example could be the power on time of a SED.
- *Level 3 Events* are connected to a level 2 event. They depend on the SED and a specific action already occurred, e.g., a channel is turned on (level 2 event) and the volume is muted (level 3 event).

The presented structure can be browsed easily by consumers. As already mentioned, the data shown in this structure is limited to the rules implemented in the system. The rules can be activated and deactivated on a separate screen. An example is shown in Figure 10.5.

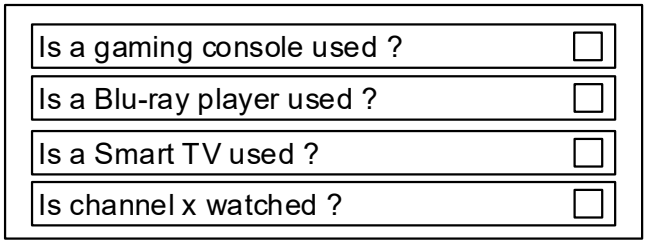


Figure 10.5.: Examples of *Collector* rules.

[5] http://www.secdev.org/projects/scapy/

10.4 Central Share

We give an overview of the *Central Share* in Section 10.4.1. In Section 10.4.2, we explain how the data is processed after uploading by a *Collector*. Finally, we describe some implementation details in Section 10.4.3.

10.4.1 Overview

The *Central Share* receives data once a day from all connected *Collectors* and summarizes all received data packets. After summarizing the data can be requested by interested third parties, e.g., broadcasters, vendors or other third parties. We describe some techniques that reduce privacy risks for consumers. We call X_i the data delivered by a *Collector*, whereas i is the household identifier, e.g., *Collector* in household 1 delivers X_1.

10.4.2 Data Processing

In this section we show techniques and methods used by the *Central Share* to reduce privacy risks for consumers:
Summarizing data. Summarizing data means in this context that if two data sets X_1 and X_2 are received, the *Central Share* will immediately add them to the total X_t, i.e., $X_t := X_1 + X_2 + X_t$. That technique avoids that a third party is able to identify data coming from a single household. Information that could identify a single household is not included in the sum X_t. It is essential to only summarize these rules from X that are gathered with the same rules r. If other values are summarized, the results might be wrong.

Intermediate results. The *Central Share* is not allowed to submit any intermediate results of X_t or any X_i to a third party. At a specific time the total X_t is submitted to third parties and X_t is then set to empty. Results that are not summarized could reveal information about households, so for example once a day data can be requested.

Delayed data delivery. A third party could detect in real-time if a household is empty by analyzing the difference in the data stream if the data stream of households would have been provided in real-time. If no real-time data is delivered and a data transfer is conducted periodically, it is hard for a third party to gain information about consumers at a household. Per default, no real-time data is shared from *Collector* or *Central Share*.

Deletion of data. The *Central Share* does not save any data and removes all data calculated after successful submission to any connected third party.

Connection security. All connections to other parties are secured with HTTPS. Each *Collector* delivers data with the public key of the *Central Share*. Therefore, data is encrypted by *Collector* and can only be decrypted by the *Central Share*. In order to reduce the attack surface of the *Central Share*, it sends X_t subscribed data periodically to connected third parties. The *Central Share* does not immediately respond to requests from third parties.

As long as the *Central Share* is physically secure and honest, data will not leak to a third party. Vulnerabilities caused by implementation errors are not in scope of this work.

10.4.3 Implementation

The implementation of the *Central Share* is Linux-based and completely written in Python. The implementation uses standard software: Apache 2, MySQL database server, WSGI and the Django framework for the web application. All connections are handled over TLS/SSL.

The *Central Share* is installed on a university server and provides a service that receives the information extracted by the *Collectors* from households. The data format is *json* and a packet consists of any resulting vector of the current deployed rule set. However, it is not necessary that any *Collector* sends a packet every time. If a *Collector* does not send a data packet, the resulting amount of devices participating is lower. An example for x_{ra} sent from a *Collector* is shown next (truncated due to space):

```
1 {'ruleid','agegroupid','answer'}
2 {'1','1','1|1|1|1|1|1|1|11|23|1|1|1|1...'}
```

10.5 Evaluation

We have tested our implementation on the RPis in four households. In those households the following Smart TVs were detected: Samsung UE40D6200, Samsung UE40ES6300, LG 42LN5758. Other devices were detected, but not measured: Sonos Sound System, home routers, NAS systems and a Samsung Blu-ray player (BD-D5500).

Based on our measurements we identified different implementation levels of the UPnP protocol. For example the Samsung Smart TV UE40ES6300 offers the most amount of UPnP services. These services allowed controlling the entire device. Even the watched program could be requested. However, the older model (UE40D6200) did not provide additional information to the running program. At least every device provided a friendly name that could be used to help consumers in a local network to identify the network device. For consumers IP addresses are hard to remember and often dynamically that means they change from time to time, so for the presentation layer it can be replaced by the friendly name. Interestingly, the LG TV did not broadcast SSDP Alive packets that led to an extension of the collector network agent. The friendly name is in the current version extracted from a DLNA service announcement.

In this prototype version, we had no third parties connected to the *Central Share*, so we did not deliver any consumer data. The general result is that it is possible to detect how many devices are used at a time and when they are activated. In one of our test households we detected that the Smart TV was turned on and directly after that the Blu-Ray player was started. This resulted in the conclusion that the consumer watched a video.

Limitations The discussed *Privacy Protecting Collector* has some limitations:

- It is not considered that malicious clients push a lot of wrong or faked data to the *Central Share*. It could lead to imprecise and useless data that is shared with third parties.
- The software has not been hardened yet. It is likely that is has vulnerabilities.
- The *Central Share* must be honest, controlled and operated by a trusted party.

10.6 Related Work

To the best of our knowledge we are the first who presents the topic in this section including an implementation tested in households. We report on related work according to audience measurement.

Audience Measurement. Nielsen Company is the leading company for audience measurement. It measures the TV viewing behavior with special devices connected to the TV. The technique does not need Smart TVs. Moreover, Nielsen Company claims that they can measure more devices at a time. No public information of the used technique could be found [121]. In Germany the GFK measures the audience with a device called GFK Meter. It has to be installed on each TV device that should be measured [122]. The amount of people watching TV is measured by pressing special buttons on a remote control provided by the GFK, i.e., the person watching TV has to log in and log out to the specific GFK Meter. It is provided to a group of people, which are characteristic for a group of people in a country, so one person in the test group reflects the characteristics for thousands of people of the population. The test group must be chosen carefully to receive meaningful data. The handling of GFK Meter is complex and not easy to use [123]. Some patents for monitoring program ownership can be found, e.g., [124, 125]. They have been published long before the first Smart TV came to a private household.

Privacy in Audience Measurement. The first academic work that tries to reduce privacy risks in existing audience measurement methods for Smart TVs is PrivTam [126]. Privacy enhancing technologies like homomorphic encryption are used. The consumer has no possibility to control the data sent to third parties and the implementation is based on a specific operating system on TVs which cannot be assumed in real households.

10.7 Discussion and Summary

In this chapter, we discussed the *Privacy Protecting Collector*, a concept and a prototype how usage data can be shared so that the interests of both, the consumers and third parties, can be satisfied. We evaluated it as a stand-alone device, but it greatly extends the *Smart TV Protector*.

Although privacy is considered in this concept, the *Privacy Protecting Collector* offers third parties more information about the usage of Smart TV as currently used audience measurement systems. However, the approach needs the consent of each consumer. The data is anonymized so that it is not possible to assign it to households. From a technical perspective, this work revealed how much data can be gathered if a device is part of a home network.

The *Privacy Protecting Collector* is secure as long as all parties are honest. In future versions of this software some improvements should be considered. On the one hand, general privacy questions, for example how already shared data can be controlled or how sharing conditions may benefit, should be analyzed. On the other hand, technical improvements like using cryptographic methods to further secure the data and lower the assumptions to the involve parties, may improve the technical implementation significantly.

The *Central Share* could be operated by any third party if one can guarantee that no data leaks. The concept of homomorphic encryption could be used to give the *Central Share* the possibility to sum the values without knowing the content (zero knowledge). The Paillier cryptosystem could be one possibility to implement that requirement (see [127] for more information about the cryptosystem). Therefore, each *Collector* could encrypt X and send that to the *Central Share*. The *Central Share* receives many $E(X)$ data sets and can sum them with homomorphic encryption. In order to deploy it effectively, it is necessary to assure that the decryption process cannot be executed without summarizing the intermediate results. Threshold cryptosystems can be used for sharing the private key with more trusted parties, e.g., the threshold version of the Paillier cryptosystem could be a candidate. Other possible protocols for other solutions must be researched.

Furthermore, a proper compensation model for consumers should be researched. It is fair to pay consumers for information, which can be used for product optimization. It is worthy to consider further research in this topic. For many third parties it is essential to get real feedback to optimize the product.

Thus, an interest for usage data will always exist. The challenge is to find the right balance between privacy and information sharing.

11 Conclusion

In this work, we identified several Smart TV related privacy risks, researched consumers' awareness and attitudes towards Smart TV related privacy risks and developed a combination of awareness and technical protection measures.

We showed that the Hybrid Broadcast Broadband TV (HbbTV) standard that is supported by almost every Smart TV can be misused to profile consumers by broadcasters without consumer's explicit consent. Consumers are not able to protect themselves due to different reasons: (1) consumers do not know that they are being tracked or data is transferred to the broadcasters and (2) they are most likely not informed that this privacy risks could harm them. Furthermore, we identified techniques such as Evercookie that are developed to identify people very accurately over a long lifetime on Smart TVs. Thus, even if a consumer tries to delete all identifying cookies, the likelihood to be successful is very low.

Moreover, we revealed severe vulnerabilities in the HTTPS certificate validation in Samsung and LG Smart TVs. Not only were the web browsers affected, also other functionality such as HbbTV and the update mechanisms. In addition we found a severe downgrading vulnerability in LG Smart TVs that enables attackers to install an outdated firmware version.

Both, the vulnerability in the HTTPS certificate validation and the HbbTV related privacy risks, could cause severe privacy risks for consumers. The importance of our work were confirmed by several TV interviews and articles in newspaper and magazines that reported on our findings (see Chapter List of Publications and Press). Additionally, we published the following articles: [15–21, 23].

We researched consumers' attitudes towards Smart TV related privacy risks in order to establish adequate awareness and technical measures for consumers. We conducted four surveys with in total 699 participants. The results are:

- We confirmed a lack of awareness of Smart TV related privacy risks and countermeasures.
- Consumers using the Internet on the Smart TV do not know how to disable HbbTV. It is likely that consumers use the default settings of a Smart TV.
- We identified factors that influence consumers' attitudes towards Smart TV related privacy and security risks: Who gathers data, which type of data is collected and what can happen.
- Just making people aware of Smart TV related privacy risks is not very promising as long as no adequate privacy protecting alternatives are provided; i.e. adequate with respect to the provided functionality.
- If properly communicated, consumers are willing to spend some time and money to better protect their privacy.

The currently available technical protection measures are limited. The most effective solution for consumers is to disconnect their Smart TVs. However, all Internet functionality would not be usable any more. The studies have shown that consumers would rather sacrifice their privacy instead of disconnecting their Smart TVs. Another option would be to deactivate Internet functionality in the configuration menus of the Smart TV. Most of them are enabled by default and it is likely that consumers do not know how to disable them or do not know that they are activated (see survey results about HbbTV related questions in Chapter 5).

Thus, these results encourage the development of usable privacy enhancing technologies providing both an adequate level of privacy and functionality; instead of only making people aware of the privacy

risks of current Smart TVs. We published these results in [25]. It is likely that those findings can be transferred to other Internet of Things technologies coming to households.

We developed the *Smart TV Protector* that protects consumers against different Smart TV related privacy risks. We successfully tested a part of the *Smart TV Protector*: the *HbbTV Privacy Protector*. It gives consumers the option to control whether a specific HbbTV channel is allowed to load data from the Internet. The *Smart TV Protector* can additionally support consumers to configure their Smart TVs according to their privacy attitudes. If the Smart TV does not provide options to enable or disable a specific functionality, the *Smart TV Protector* can block functionality and some vulnerabilities of Smart TVs like SSL/TLS issues and connection attempts to the Smart TV. The *Smart TV Protector* is extensible so that new risks can also be taken into account. The *HbbTV Privacy Protector* is published in [16, 17] and was mentioned in some newspaper and magazine articles.

The interest of vendors and content providers gathering data about consumer behavior will not end in the near future. On the one hand companies need detailed information how a product is used in order to improve it effectively and cost-optimized. On the other hand, consumers have no incentives to share profile data with companies. Even more, often data is shared without explicit consent of consumers. Therefore, solutions that guarantee a balance between data sharing and consumers' interests should be established.

The *Privacy Protecting Collector* is our theoretical approach to extend the *Smart TV Protector* with a possibility to share data privacy protecting only to those third parties that are accepted by the consumers. We use the *Smart TV Protector* to restrict the data transfer to third parties, the *Privacy Protecting Collector* processes data and publishes it on a trusted *Central Share* that shares the data with authorized third parties. We published it in [26, 27].

As far as we know no protection measures for households has been introduced onto the market yet. This research project is the first work trying to establish a protection measure with both technical and awareness components. A lot more discussions with consumers, vendors and broadcasters are needed to balance security, privacy and usability. In detail, we see more (research) work in the following fields:

- How much effort/money are consumers willing to spend to protect against Smart TV related risks? There are less publications showing that consumers are willing to spend money for privacy protection. But, as far as we know no work that explicitly covered effort and money for Smart TV related risks. In the broader field of Internet of Things (IoT) is this also unclear. However, for vendors it could lead to an advertisement opportunity and an increase of revenue when security and privacy are taken into account.

- Why do most consumers not know countermeasures or risks? Are the risks not important? Are the consequences not clear or even not severe enough? We found evidence that consumers are not aware of risks and countermeasures. It is likely that the information given to consumers when buying new Smart TVs is simply not enough. But, we did not researched that issue in detail. Further investigations would reduce occurring issues through information in an early stage.

In the future a tremendous amount of data comes from different devices inside a household. These devices were in the past not connected to the Internet, e.g., coffee makers, refrigerators, electrical tooth brushes, Smart TVs. It becomes more important to educate consumers and help them to be able to protect their data. Those devices are closer to the private life than other connected devices. A challenge will be the usability of security and privacy features and not the technical feasibility.

References

[1] M. Antonoff, "Stay Tuned for Smart TV," *Popular Science*, vol. 37, no. 5, pp. 62–65, 1990.

[2] Ty Pendlebury (CNET), *Smart TV: what you need to know*, Last accessed on 06 November 2016, http://www.cnet.com/news/smart-tv-what-you-need-to-know/, Jul. 2011.

[3] QUORA, *When did the first Smart TV come out?* Last accessed on 06 November 2016, https://www.quora.com/When-did-the-first-Smart-TV-come-out.

[4] Samsung, *History of samsung smart tv*, Last accessed on 06 November 2016, http://www.samsung.com/sa_en/offer/TV_History/.

[5] Andrew Burger (telecompetitor), *Report: Smart TVs Account for More than 25% of Global TV Shipments*, Last accessed on 06 November 2016, http://www.telecompetitor.com/report-smart-tvs-account-for-more-than-25-of-global-tv-shipments/.

[6] Michael Balderston (TVTechnology), *Smart TV Shipments Exceed 100 Million in 2015*, Last accessed on 06 November 2016, http://www.tvtechnology.com/news/0002/smart-tv-shipments-exceed-100-million-in-2015/278675.

[7] British Broadcasting Corporation, Independent Broadcasting Authority, British Radio Equipment Manufacturer's Association, *Broadcast Teletext Specification*, Last accessed on 08 January 2017, http://www.bighole.nl/pub/mirror/homepage.ntlworld.com/kryten_droid/teletext/spec/teletext_spec_1974.htm.

[8] Seven One Media, *Addressable TV - The Future is now.* Available from author on request, Feb. 2016.

[9] Working Group Smart TV of the German TV-Platform, *Marktanalyse Smart-TV - Eine Bestandsaufnahme der Deutschen TV-Plattform*, Last accessed on 06 November 2016, http://tv-plattform.de/images/stories/pdf/marktanalyse_smart-tv_2013.pdf.

[10] gfu Consumer & Home Electronics, *Was sich Konsumenten wünschen und wo sie skeptisch sind*, Last accessed on 06 November 2016, http://www.gfu.de/fileadmin/media/downloads/Insights-Trends-2015-Kamp.pdf.

[11] "Watch and be Watched: Compromising All Smart TV Generations," in *2014 IEEE 11th Consumer Communications and Networking Conference (CCNC)*, Jan. 2014.

[12] Rob Waugh (Metro), *Smart TV hackers are filming people having sex on their sofas – and putting it on porn sites*, Last accessed on 06 November 2016, http://metro.co.uk/2016/05/23/smart-tv-hackers-are-filming-people-having-sex-on-their-sofas-and-putting-it-on-porn-sites-5899248/.

[13] Lisa de Moraes, *Where's the Love? CNBC Scrambles to Woo Viewers for 'McEnroe'*, Last accessed on 06 November 2016, https://web.archive.org/web/20121104002650/http://www.washingtonpost.com/wp-dyn/articles/A61516-2004Aug12.html.

[14] C. Mulliner and B. Michéle, "Read it twice! a mass-storage-based tocttou attack.," in *WOOT*, 2012, pp. 105–112.

[15] M. Ghiglieri, F. Oswald, and E. Tews, "HbbTV – I Know What You Are Watching," in *Informationssicherheit stärken – Vertrauen in die Zukunft schaffen*, Bundesamt für Sicherheit in der Informationstechnik, May 2013, pp. 225–238.

[16] M. Ghiglieri and E. Tews, "A Privacy Protection System for HbbTV in Smart TVs," in *Consumer Communications and Networking Conference (CCNC), 2014 IEEE 11th*, IEEE, 2014, pp. 357–362.

[17] M. Ghiglieri, "I Know What You Watched Last Sunday – A New Survey Of Privacy In HbbTV," *Workshop Web 2.0 Security & Privacy 2014 in conjunction with the IEEE Symposium on Security and Privacy*, 2014.

[18] M. Ghiglieri and M. Waidner, "HbbTV Security and Privacy: Issues and Challenges," *IEEE Security Privacy*, vol. 14, no. 3, pp. 61–67, May 2016, ISSN: 1540-7993. DOI: 10.1109/MSP.2016.54.

[19] M. Ghiglieri, "HbbTV – aktueller Stand 2014," Deutsch, in *FKT - Die Fachzeitschrift für Fernsehen, Film und elektronische Medien*, Schiele & Schön, Ed., vol. 11/2014, Nov. 2014.

[20] M. Ghiglieri, F. Oswald, and E. Tews, "HbbTV: Neue Funktionen mit möglichen Nebenwirkungen," Deutsch, in *FKT - Die Fachzeitschrift für Fernsehen, Film und elektronische Medien*, Schiele & Schön, Ed., vol. 10/2013, Oct. 2013, pp. 563–566.

[21] M. Ghiglieri, M. Hansen, M. Nebel, J. V. Pörschke, and H. S. Fhom, "Smart-TV und Privatheit - Bedrohungspotenziale und Handlungsmöglichkeiten," Forum Privatheit, Tech. Rep., Feb. 2016.

[22] HbbTV Association, *HbbTV Specification 2.0 (approved by ETSI as TS 102 796 V1.3.1 in October 2015)*, Last accessed on 06 November 2016, http://www.etsi.org/deliver/etsi_ts/102700_102799/102796/01.03.01_60/ts_102796v010301p.pdf.

[23] M. Ghiglieri, "Incorrect HTTPS Certificate Validation in Samsung Smart TVs," Technical Report, 2014.

[24] T. Neidig, "Sicherheits- und Privatsphärenanalyse von Smart-TVs mit HDMI-ARC Unterstützung," Bachelor's Thesis, Technische Universität Darmstadt, 2016.

[25] M. Ghiglieri, M. Volkamer, and K. Renaud, "Exploring Consumers' Attitudes of Smart TV Related Privacy Risks," *Human Computer Interaction Conference 2017*, 2017, to be published (accepted).

[26] M. Ghiglieri and J. Müller, "Datenschutzfreundliche Erfassung von Nutzungsdaten bei Smart Entertainment Geräten," in *14. Deutscher IT-Sicherheitskongress*, Bundesamt für Sicherheit in der Informationstechnik, May 2015.

[27] M. Ghiglieri, "PriMSED-Privacy-friendly measurement of Smart Entertainment Devices," in *Consumer Communications and Networking Conference (CCNC), 2015 12th Annual IEEE*, IEEE, 2015, pp. 65–70.

[28] HbbTV Association, *HbbTV Overview*, Last accessed on 06 November 2016, http://hbbtv.org/overview/#hbbtv-overview.

[29] HbbTV Association, *HbbTV Specification 1.5 (approved by ETSI as ETSI TS 102 796 v1.2.1 in November 2012)*, Last accessed on 06 November 2016, http://www.etsi.org/deliver/etsi_ts/102700_102799/102796/01.02.01_60/ts_102796v010201p.pdf.

[30] DVB Project, *History of DVB*, Last accessed on 06 November 2016, https://www.dvb.org/about/history.

[31] HbbTV Association, *HbbTV Specification 2.0.1*, Last accessed on 06 November 2016, http://www.hbbtv.org/wp-content/uploads/2015/07/HbbTV-SPEC20-00023-002-HbbTV_2.0.1_specification_for_publication_clean.pdf.

[32] Kamkar, Samy, *evercookie*, Last accessed on 06 November 2016, http://samy.pl/evercookie/, Sep. 2010.

[33] IEEE, *Standard for Information technology–Telecommunications and information exchange between systems Local and metropolitan area networks–Specific requirements Part 11: Wireless LAN Medium Access Control (MAC) and Physical Layer (PHY) SpecificationsÏEEE Std 802.11-2012 (Revision of IEEE Std 802.11-2007)*, pp.1-2793, March 29 2012 doi: 10.1109/IEEESTD.2012.6178212.

[34] A. Jaritz and L. Lo Iacono, "Untersuchung des datenverkehrs aktueller smart-tvs," *Datenschutz und Datensicherheit - DuD*, vol. 40, no. 8, pp. 511–518, 2016, ISSN: 1862-2607. DOI: 10.1007/s11623-016-0648-0. [Online]. Available: http://dx.doi.org/10.1007/s11623-016-0648-0.

[35] A. Sachs and M. Meder, "Technische prüfung der datenflüsse bei smart-tvs," *Datenschutz und Datensicherheit - DuD*, vol. 39, no. 7, pp. 449–454, 2015, ISSN: 1862-2607. DOI: 10.1007/s11623-015-0448-y. [Online]. Available: http://dx.doi.org/10.1007/s11623-015-0448-y.

[36] Y. Oren and A. D. Keromytis, "From the aether to the ethernet—attacking the internet using broadcast digital television," in *23rd USENIX Security Symposium (USENIX Security 14)*, 2014, pp. 353–368.

[37] DoctorBeet's Blog, *LG Disables Smart TV features in the EU to force users to accept new oppressive Privacy policy*, Last accessed on 06 November 2016, http://doctorbeet.blogspot.de/.

[38] E. Zolfagharifard (Daily Mail), *Is YOUR TV spying on you? Report reveals how Vizio smart televisions track your data so that it can be sold to advertisers*, Last accessed on 06 November 2016, http://www.dailymail.co.uk/sciencetech/article-3312597/Is-TV-spying-Report-reveals-Vizio-smart-televisions-track-data-sold-advertisers.html, 2015.

[39] Samsung, *Samsung Privacy Policy–SmartTV Supplement*, Last accessed on 06 November 2016, http://www.samsung.com/sg/info/privacy/smarttv/.

[40] LG, *Legal Documents(Smart TV) - Viewing Information*, Last accessed on 06 November 2016, http://gb.lgappstv.com/appspc/footer/footer/moveDeviceTerms.lge?type=S_ADG&level=3&link=301.

[41] Chris Matyszczyk (CNET), *Samsung's warning: Our Smart TVs record your living room chatter*, Last accessed on 06 November 2016, http://www.cnet.com/uk/news/samsungs-warning-our-smart-tvs-record-your-living-room-chatter/, 2015.

[42] Shane Harris (The Daily beast), *WATCH YOUR MOUTH - Your Samsung SmartTV Is Spying on You, Basically*, Last accessed on 17 November 2016, http://www.thedailybeast.com/articles/2015/02/05/your-samsung-smarttv-is-spying-on-you-basically.html, 2015.

[43] David Lodge (Pen Test Partners), *Is Your Samsung TV Listening To You?* Last accessed on 06 November 2016, https://www.pentestpartners.com/blog/is-your-samsung-tv-listening-to-you/.

[44] Network Working Group, *RFC2616 - HTTP/1.1*, Last accessed on 06 November 2016, https://tools.ietf.org/html/rfc2616, Jun. 1999.

[45] Network Working Group, *RFC2818 - HTTP Over TLS*, Last accessed on 06 November 2016, https://tools.ietf.org/html/rfc2818, May 2000.

[46] Network Working Group, *RFC5280 - Internet X.509 Public Key Infrastructure Certificate and Certificate Revocation List (CRL) Profile*, Last accessed on 06 November 2016, https://tools.ietf.org/html/rfc5280, May 2008.

[47] Network Working Group, *RFC6818 - Updates to the Internet X.509 Public Key Infrastructure Certificate and Certificate Revocation List (CRL) Profile*, Last accessed on 06 November 2016, https://tools.ietf.org/html/rfc6818, Jan. 2013.

[48] OpenBSD, *zic — time zone compiler*, Last accessed on 25 November 2016, http://man.openbsd.org/zic.8, 2015.

[49] HDMI Licensing LL.C., *HDMI Specification Version 1.4a*, 2010.

[50] M. Niemietz, J. Somorovsky, C. Mainka, and J. Schwenk, *Not so Smart: On Smart TV Apps*, http://www.ei.ruhr-uni-bochum.de/media/nds/veroeffentlichungen/2015/08/31/SmartTvAttacks.pdf, undated.

[51] G. Keizer, *Hackers steal SSL certificates for CIA, MI6, Mossad*, Last accessed on 06 November 2016, http://www.computerworld.com/s/article/9219727/Hackers_steal_SSL_certificates_for_CIA_MI6_Mossad, Sep. 2011.

[52] M. Metzger, *Symantec purges employees after unauthorised use of Google SSL certificates*, Last accessed on 28 February 2017, https://www.scmagazineuk.com/symantec-purges-employees-after-unauthorised-use-of-google-ssl-certificates/article/535297/, Sep. 2015.

[53] BSI für Bürger, *Phishing*, Last accessed on 06 November 2016, https://www.bsi-fuer-buerger.de/BSIFB/DE/Risiken/SpamPhishingCo/Phishing/phishing_node.html.

[54] L. Auriemma, *Endless restarts*, Last accessed on 06 November 2016, http://aluigi.altervista.org/adv/samsux_1-adv.txt, Apr. 2012.

[55] L. SeungJin, *Dirty note on Samsung Smart TV Security*, Last accessed on 06 November 2016, http://beistlab.files.wordpress.com/2012/12/samsung_smart_tv_attack_surfaces2.pdf, Dec. 2012.

[56] Kaspersky Lab, *Smart-TV: Cyberangriffs- und Spionageszenarien*, Last accessed on 06 November 2016, http://www.kaspersky.com/de/about/news/virus/2016/Smart-TV_Cyberangriffs-und_Spionageszenarien, Jan. 2016.

[57] C. Cimpanu, *Android Ransomware Infects LG Smart TV*, Last accessed on 28 February 2017, https://www.bleepingcomputer.com/news/security/android-ransomware-infects-lg-smart-tv//, Dec. 2016.

[58] H. Krasnova and N. F. Veltri, "Privacy calculus on social networking sites: explorative evidence from germany and usa," in *HICSS'10*, IEEE, 2010, pp. 1–10.

[59] L. J. Camp, "Mental models of privacy and security," *Technology and Society Magazine, IEEE*, vol. 28, no. 3, pp. 37–46, 2006.

[60] P. Dourish, J. Delgado De La Flor, and M. Joseph, "Security as a practical problem: some preliminary observations of everyday mental models," in *Proceedings of CHI 2003 Workshop on HCI and Security Systems*, Fort Lauderdale, Florida, May 2003.

[61] R. Wash, "Folk models of home computer security," in *Proceedings of the Sixth Symposium on Usable Privacy and Security*, ACM, Redmond, WA, 2010, p. 11.

[62] J. Ophoff and M. Robinson, "Exploring end-user smartphone security awareness within a South African context," in *Information Security for South Africa (ISSA), 2014*, IEEE, 2014, pp. 1–7.

[63] M. Volkamer, K. Renaud, O. Kulyk, and S. Emeröz, "A socio-technical investigation into smartphone security," in *Security and Trust Management*, Springer, 2015, pp. 265–273.

[64] M. Harbach, E. von Zezschwitz, A. Fichtner, A. De Luca, and M. Smith, "It's a hard lock life: a field study of smartphone (un) locking behavior and risk perception," in *Symposium on Usable Privacy and Security (SOUPS)*, 2014.

[65] Elie Bursztein, *Survey: most people don't lock their Android phones - but should*, Last accessed on 06 November 2016, https://www.elie.net/blog/survey-most-people-dont-lock-their-android-phones-but-should, 2014.

[66] D. J. Solove, "I've Got Nothing to Hide and Other Misunderstandings of Privacy," *San Diego law review*, vol. 44, p. 745, 2007.

[67] F. Raja, K. Hawkey, S. Hsu, K.-L. Wang, and K. Beznosov, "Promoting a physical security mental model for personal firewall warnings," in *CHI '11 Extended Abstracts on Human Factors in Computing Systems*, ser. CHI EA '11, Vancouver, BC, Canada, 2011, pp. 1585–1590, ISBN: 978-1-4503-0268-5.

[68] B. Friedman, D. Hurley, D. C. Howe, E. Felten, and H. Nissenbaum, "Users' conceptions of web security: a comparative study," in *CHI'02 extended abstracts on Human factors in computing systems*, ACM, 2002, pp. 746–747.

[69] D. Weirich and M. A. Sasse, "Pretty good persuasion: a first step towards effective password security in the real world," in *Proc. of 2001 Workshop on New Security Paradigms*, ser. NSPW '01, Cloudcroft, NM, 2001, pp. 137–143.

[70] S. Gupta and R. P. Bostrom, "Theoretical model for investigating the impact of knowledge portals on different levels of knowledge processing," *International Journal of knowledge and Learning*, vol. 1, no. 4, pp. 287–304, 2005.

[71] E. Wästlund, J. Angulo, and S. Fischer-Hübner, "Evoking comprehensive mental models of anonymous credentials.," in *iNetSeC*, J. Camenisch and D. Kesdogan, Eds., ser. Lecture Notes in Computer Science, vol. 7039, Springer, 2011, pp. 1–14, ISBN: 978-3-642-27584-5. [Online]. Available: `http://dblp.uni-trier.de/db/conf/ifip11-4/inetsec2011.html#WastlundAF11`.

[72] M. Harbach, S. Fahl, M. Rieger, and M. Smith, "On the acceptance of privacy-preserving authentication technology: the curious case of national identity cards," in *Privacy Enhancing Technologies*, Springer, 2013, pp. 245–264.

[73] B. Debatin, J. P. Lovejoy, A.-K. Horn, and B. N. Hughes, "Facebook and online privacy: Attitudes, Behaviors, and Unintended Consequences," *Journal of Computer-Mediated Communication*, vol. 15, no. 1, pp. 83–108, 2009.

[74] S. Gaw, E. W. Felten, and P. Fernandez-Kelly, "Secrecy, flagging, and paranoia: adoption criteria in encrypted email," in *SIGCHI Conference on Human Factors in Computing Systems*, ser. CHI '06, 2006, pp. 591–600.

[75] K. Renaud, M. Volkamer, and A. Renkema-Padmos, "Why doesn't Jane protect her privacy?" In *14th International Symposium on Privacy Enhancing Technologies. Springer LNCS*, 2014, pp. 244–262.

[76] S. Clark, T. Goodspeed, P. Metzger, Z. Wasserman, K. Xu, and M. Blaze, "Why (Special Agent) Johnny (Still) Can't Encrypt: A Security Analysis of the APCO Project 25 Two-Way Radio System.," in *USENIX Security Symposium*, 2011.

[77] M. Asplund and S. Nadjm-Tehrani, "Attitudes and perceptions of iot security in critical societal services," *IEEE Access*, vol. 4, pp. 2130–2138, 2016.

[78] S. Trepte and L. Reinecke, *Privacy online: perspectives on privacy and self-disclosure in the social web*, 2011.

[79] T. Dienlin and S. Trepte, "Is the privacy paradox a relic of the past? an in-depth analysis of privacy attitudes and privacy behaviors," *European Journal of Social Psychology*, vol. 45, no. 3, pp. 285–297, 2015.

[80] S. Trepte, T. Dienlin, and L. Reinecke, "Risky behaviors: how online experiences influence privacy behaviors," *Von der Gutenberg-Galaxis zur Google-Galaxis [From the Gutenberg galaxy to the Google galaxy]*, pp. 225–244, 2014.

[81] S. Trepte, D. Teutsch, P. K. Masur, C. Eicher, M. Fischer, A. Hennhöfer, and F. Lind, "Do people know about privacy and data protection strategies? towards the "online privacy literacy scale"(oplis)," in *Reforming European data protection law*, Springer Netherlands, 2015, pp. 333–365.

[82] C. Jensen and C. Potts, "Privacy policies as decision-making tools: an evaluation of online privacy notices," in *SIGCHI'04*, ACM, 2004, pp. 471–478.

[83] A. Acquisti and R. Gross, "Imagined communities: awareness, information sharing, and privacy on the facebook," in *PET*, Springer, 2006, pp. 36–58.

[84] P. G. Kelley, S. Consolvo, L. F. Cranor, J. Jung, N. Sadeh, and D. Wetherall, "A conundrum of permissions: installing applications on an android smartphone," in *FC'12*, Springer, 2012, pp. 68–79.

[85] A. P. Felt, E. Ha, S. Egelman, A. Haney, E. Chin, and D. Wagner, "Android permissions: user attention, comprehension, and behavior," in *Proceedings of the Eighth Symposium on Usable Privacy and Security*, ACM, Washington, DC, 2012, p. 3.

[86] M. Harbach, M. Hettig, S. Weber, and M. Smith, "Using personal examples to improve risk communication for security & privacy decisions," in *SIGCHI'14*, ACM, 2014, pp. 2647–2656.

[87] T. C. Leonard, "Richard H. Thaler, Cass R. Sunstein, Nudge: Improving decisions about health, wealth, and happiness," *Constitutional Political Economy*, vol. 19, no. 4, pp. 356–360, 2008.

[88] T. Dinev and P. Hart, "An extended privacy calculus model for e-commerce transactions," *Info. Sys. Research*, vol. 17, no. 1, pp. 61–80, Mar. 2006, ISSN: 1526-5536. DOI: 10.1287/isre.1060.0080. [Online]. Available: http://dx.doi.org/10.1287/isre.1060.0080.

[89] G. Kim and H. Koo, "The causal relationship between risk and trust in the online marketplace," *Comput. Hum. Behav.*, vol. 55, no. PB, pp. 1020–1029, Feb. 2016, ISSN: 0747-5632. DOI: 10.1016/j.chb.2015.11.005. [Online]. Available: http://dx.doi.org/10.1016/j.chb.2015.11.005.

[90] N. K. Lankton and D. H. McKnight, "What does it mean to trust facebook?: examining technology and interpersonal trust beliefs," *SIGMIS Database*, vol. 42, no. 2, pp. 32–54, May 2011, ISSN: 0095-0033. DOI: 10.1145/1989098.1989101. [Online]. Available: http://doi.acm.org/10.1145/1989098.1989101.

[91] B. C. Choi and L. Land, "The effects of general privacy concerns and transactional privacy concerns on facebook apps usage," *Inf. Manage.*, vol. 53, no. 7, pp. 868–877, Nov. 2016, ISSN: 0378-7206. DOI: 10.1016/j.im.2016.02.003. [Online]. Available: https://doi.org/10.1016/j.im.2016.02.003.

[92] O. Kulyk, P. Gerber, M. El Hanafi, B. Reinheimer, K. Renaud, and M. Volkamer, "Encouraging Privacy-Aware Smartphone App Installation: Finding out what the Technically-Adept Do," in *USEC'16*, Inter, 2016.

[93] K. Fawaz and K. G. Shin, "Location privacy protection for smartphone users," in *Proceedings of the 2014 ACM SIGSAC Conference on Computer and Communications Security*, ser. CCS '14, Scottsdale, Arizona, USA: ACM, 2014, pp. 239–250, ISBN: 978-1-4503-2957-6. DOI: 10.1145/2660267.2660270. [Online]. Available: http://doi.acm.org/10.1145/2660267.2660270.

[94] E. Rose, "Data users versus data subjects: are consumers willing to pay for property rights to personal information?" In *HICSS'05*, IEEE, 2005, pp. 180c–180c.

[95] J. Grossklags and A. Acquisti, "When 25 cents is too much: an experiment on willingness-to-sell and willingness-to-protect personal information.," in *WEIS*, 2007.

[96] A. Acquisti, L. John, and G. Loewenstein, "What is privacy worth," in *Workshop on Information Systems and Economics (WISE)*, 2009.

[97] J. Y. Tsai, S. Egelman, L. Cranor, and A. Acquisti, "The effect of online privacy information on purchasing behavior: an experimental study," *Information Systems Research*, vol. 22, no. 2, pp. 254–268, 2011. DOI: 10.1287/isre.1090.0260. eprint: http://pubsonline.informs.org/doi/pdf/10.1287/isre.1090.0260. [Online]. Available: http://pubsonline.informs.org/doi/abs/10.1287/isre.1090.0260.

[98] SANS, *What is Intrusion Detection ?* Last accessed on 06 November 2016, https://www.sans.org/security-resources/idfaq/what-is-intrusion-detection/1/1.

[99] Suricata, *Suricata Rules*, Last accessed on 06 November 2016, http://suricata.readthedocs.io/en/latest/rules/intro.html.

[100] abuse.ch, *abuse.ch SSL Fingerprint Blacklist for Suricata*, Last accessed on 15 November 2016,https://sslbl.abuse.ch/blacklist/sslblacklist.rules.

[101] Suricata, *TLS event rules*, Last accesses on 15 November 2016, https://github.com/inliniac/suricata/blob/master/rules/tls-events.rules.

[102] P. Manev, Last accessed on 27 February 2017, https://www.stamus-networks.com/2015/07/24/finding-self-signed-tls-certificates-suricata-and-luajit-scripting/, Jul. 2015.

[103] Yaron Y. Goland, Ting Cai, Paul Leach, Ye Gu, *Simple Service Discovery Protocol/1.0 Operating without an Arbiter*, Last accessed on 06 November 2016, https://tools.ietf.org/html/draft-cai-ssdp-v1-03.

[104] Open Connectivity Foundation, *UPnP Device Architecture version 2.0*, Last accessed on 06 November 2016, https://openconnectivity.org/resources/specifications/upnp/specifications.

[105] Fielding, R. and Reschke, J., *Hypertext transfer protocol (http/1.1): semantics and content*, Last accessed on 06 November 2016, https://tools.ietf.org/html/rfc7231, 2014.

[106] Eastlake, Donald and Abley, J., *IANA Considerations and IETF Protocol and Documentation Usage for IEEE 802 Parameters*, Last accessed on 06 November 2016, https://tools.ietf.org/html/rfc7042, 2013.

[107] H.-A. Engels, *Device Learner – Analysis of machine learning algorithms to learn smart home network traffic patterns*, Tech Report. Available from author on request, 2015.

[108] D. Krause, *davea/ssdp.py*, Last accessed on 28 February 2017, https://gist.github.com/davea/215ef0b2541c479dbc27, 2014.

[109] Privoxy Developers, *Privoxy*, Last accessed on 06 November 2016, https://www.privoxy.org/.

[110] Ernst and Young, "Insights on governance, risk and compliance – Data loss prevention: Keeping your sensitive data out of the public domain," Tech. Rep., 2011, Last accessed on 06 November 2016, http://www.ey.com/Publication/vwLUAssets/EY_Data_Loss_Prevention/\protect\T1\textdollarFILE/EY_Data_Loss_Prevention.pdf.

[111] R. A. Kemmerer and G. Vigna, "Intrusion detection: a brief history and overview," *Computer*, vol. 35, no. 4, pp. 27–30, Apr. 2002, ISSN: 0018-9162. DOI: 10.1109/MC.2002.1012428.

[112] Eric Ouellet, "Magic Quadrant for Content-Aware Data Loss Prevention," *Gartner, Inc.*, 2013.

[113] H. Chen, O. Chowdhury, J. Chen, N. Li, and R. Proctor, "Towards quantification of firewall policy complexity," in *Proceedings of the 2015 Symposium and Bootcamp on the Science of Security*, ACM, 2015, p. 18.

[114] Dojo Labs, *Dojo*, Last accessed on 06 November 2016, https://www.dojo-labs.com/product/dojo.

[115] FAHMIDA Y. RASHID, *How to Secure Your (Easily Hackable) Smart Home*, Last accessed on 06 November 2016, http://www.tomsguide.com/us/secure-smart-home-how-to,news-19380.html, 2014.

[116] Gira, *Service Builders and end customers*, Last accessed on 06 November 2016, http://www.gira.com/en/service/bauherren/datenschutz.html.

[117] BSI, *Smart TV*, Last accessed on 06 November 2016, https://www.bsi-fuer-buerger.de/BSIFB/DE/DigitaleGesellschaft/SmartTV/SmartTV_node.html.

[118] Organisation for Economic Co-operation and Development, Last accessed on 06 November 2016, http://www.oecd.org/internet/ieconomy/privacy-guidelines.htm, 2013.

[119] R.Droms, *RFC 2131 - Dynamic Host Configuration Protocol*, Last accessed on 06 November 2016,http://tools.ietf.org/html/rfc2131, 1997.

[120] R. Dingledine, N. Mathewson, and P. Syverson, "Tor: the second-generation onion router," in *Proceedings of the 13th Conference on USENIX Security Symposium - Volume 13*, ser. SSYM'04, San Diego, CA: USENIX Association, 2004, pp. 21–21. [Online]. Available: http://dl.acm.org/citation.cfm?id=1251375.1251396.

[121] Nielsen Company, *Audience Measurement*, Last accessed on 06 November 2016,http://www.nielsen.com/us/en/solutions/audience-measurement.html, Aug. 2014.

[122] GfK Fernsehforschung GmbH, *Die Entwicklung und Zusammensetzung des AGF-Fernsehpanels*, Last accessed on 06 November 2016, https://www.agf.de/forschung/methode/fernsehpanel/.

[123] jetzt-Redaktion, *Ich war die Quote*, Last accessed on 06 November 2016, http://jetzt.sueddeutsche.de/texte/anzeigen/508994/Ich-war-die-Quote, Aug. 2010.

[124] E. Sesto, T. Travaille, C. Michel, and J. Paquette, *Configurable monitoring of program viewership and usage of interactive applications*, US Patent 6,530,082, Mar. 2003. [Online]. Available: http://www.google.com/patents/US6530082.

[125] J. Houston, *Cooperative system for measuring electronic media*, US Patent 6,353,929, Mar. 2002. [Online]. Available: http://www.google.com/patents/US6353929.

[126] G. Drosatos, A. Tasidou, and P. Efraimidis, "Privacy-Preserving Television Audience Measurement Using Smart TVs," English, in *Information Security and Privacy Research*, ser. IFIP Advances in Information and Communication Technology, D. Gritzalis, S. Furnell, and M. Theoharidou, Eds., vol. 376, Springer Berlin Heidelberg, 2012, pp. 223–234, ISBN: 978-3-642-30435-4. DOI: 10.1007/978-3-642-30436-1_19. [Online]. Available: http://dx.doi.org/10.1007/978-3-642-30436-1_19.

[127] P.-A. Fouque, G. Poupard, and J. Stern, "Sharing Decryption in the Context of Voting or Lotteries," English, in *Financial Cryptography*, ser. Lecture Notes in Computer Science, Y. Frankel, Ed., vol. 1962, Springer Berlin Heidelberg, 2001, pp. 90–104, ISBN: 978-3-540-42700-1. DOI: 10.1007/3-540-45472-1_7. [Online]. Available: http://dx.doi.org/10.1007/3-540-45472-1_7.

[128] Duden.de, *das Smart-TV*, Last accessed on 06 November 2016, http://www.duden.de/rechtschreibung/Smart_TV.

[129] JOHN R. QUAIN: Tom's Guide, *Smart TVs: Everything You Need to Know*, Last accessed on 06 November 2016, http://www.tomsguide.com/us/smart-tv-faq,review-2111.html.

[130] S. T. Margulis, "Three theories of privacy: an overview," in *Privacy Online*, Springer, 2011, pp. 9–17.

[131] A. F. Westin, *Privacy and Freedom*. New York: Atheneum, 1967.

[132] J. H. Ziegeldorf, O. G. Morchon, and K. Wehrle, "Privacy in the internet of things: threats and challenges," *Security and Communication Networks*, vol. 7, no. 12, pp. 2728–2742, 2014.

[133] J. Daintith and E. Wright, *A dictionary of computing*. [Online]. Available: //www.oxfordreference.com/10.1093/acref/9780199234004.001.0001/acref-9780199234004.

A Explanation of Terms

This appendix chapter serves as an explanation of some terms that are used in this dissertation. We list them and give some information.

Smart TV
The definition of the term 'Smart TV' differs in publications, see [128, 129]. For this work we declare that Smart TVs (sometimes called connected TVs, addressable TVs) are television devices that can be connected to the Internet and the traditional broadcast channel, e.g. satellite, terrestrial or cable. Thus, they enable broadcaster, vendors and other content providers to deliver content over the Internet directly to these devices. Some set-top boxes provide similar functionality as Smart TVs. We consider them as Smart TVs as long as not mentioned separately.

Privacy
Privacy is not clearly defined since it depends on different personal factors. Thus, many different explanation can be found in the literature [130]. For Westin [131], people have the right to decide what and when information about them is communicated to others and under what circumstances. Ziegeldorf *et al.* [132] adapted Westin's definition and concretized it for the Internet of Things domain. Since Smart TVs are a part of the Internet of Things domain, we refine that definition for Smart TVs. Therefore, for this work, Smart TV consumer's privacy can be outlined with the following aspects:

- **Awareness of Privacy Risks and Consequences:** Consumers should be aware of potential privacy risks and their consequences caused by Smart TVs or related services.
- **Informed Decisions:** Consumers should be able to do informed decision whether they want to use Smart TV functionality that may cause privacy risks.
- **Awareness/Control of Data Processing:** Consumers should be aware and be able to control their data which is sent outside of the personal control sphere.

These three aspects cover the concept of informed self-determination: (1) consumers are aware of privacy risks and consequences, (2) they are able to protect their privacy and (3) know how third parties process their data and they can control it, if necessary. The personal control sphere is here the household where the Smart TV is used.

Note, the boundaries of what is considered a privacy risk differ among people. People define where is the boundary and often adjust it to be sufficient for serving the current needs [130, 131]. In this work, we do not focus on legislative aspects of privacy.

Security
Security in computer systems is the protection of data against hackers and other non-legitimate people to gain access to systems in order to invade the privacy. The Oxford Dictionary [133] states:

> *Prevention of or protection against (a) access to information by unauthorized recipients or (b) intentional but unauthorized destruction or alteration.*

In technical literature security is often described with three basic security goals: confidentiality, integrity and availability of data. If one of these basic security goals can be violated easily, a vulnerability that can be exploited exists. Exploited vulnerabilities, especially attacks on confidentiality, often causes privacy issues.

Broadcaster
Broadcasters are the institution which operates one or more TV or radio channels. They are responsible for the content that is delivered over different media such as satellite (DVB-S), cable (DVB-C) and terrestrial (DVB-T) as well as over the Internet, which is known as the functionality HbbTV.

Hybrid Broadband Broadcast TV (HbbTV)
HbbTV is a standardized technique that is implemented by most Smart TV vendors. It covers video on demand and information services for Smart TVs. Web technologies are the main technology that is used for HbbTV applications. Technically, a web site with transparent background over the current channel is delivered to the devices.

Digital Video Broadcast (DVB)
The DVB project is an Alliance of many companies worldwide. It defines specifications for digital media delivery [30]. In this context, a DVB stream is a data stream that transports radio or TV signals via satellite (DVB-S), cable (DVB-C) or terrestrial (DVB-T) to the end devices.

B Additional Details of Findings in Privacy Risks of Hybrid Broadcast Broadband TV

This appendix chapter shows the source code that is used to identify channels in an encrypted Wi-Fi network. For detailed information see the Chapter 3.

```
# coding=utf8

import re
import sys
import signal


class Stats:
    """ Stats about packet lengths """
    def __init__(self):
        self.s = {}


    """ Add a new packet of length plen arrived at ptime """
    def add(self, plen, ptime):
        if not self.s:
            self.starttime = ptime
            self.c = False
        self.s[plen] = self.s.get(plen, 0) + 1

        if (self.starttime + 10.0 < ptime) and (not self.c):
            print "continious traffic for 10 seconds"
            self.c = True
            self.show()

    """ Show the current statistics, if at least one packet has been added """
    def show(self):
        if not self.s:
            # There is no packet to show
            return

        # print the arrival time
        s = "+++ packet at " + str(self.starttime) + " +++\n"

        # print all packets sorted by packet length
        for k in sorted(self.s.keys()):
            s += "%(n)04d" % {'n': k } + ": "
            for i in range(self.s[k]):
                s += "#"
            s += "\n"
        print s
        if ((187 in self.s) and (281 in self.s)) or (308 in self.s):
            print "ARD Group"
        if (313 in self.s):
            print "Might be Phoenix"
        if (371 in self.s):
            print "Might be BR"
        if (357 in self.s) and (188 in self.s):
            print "ZDF Group"
        if (344 in self.s) and (76 in self.s) and (68 in self.s):
            print "Pro7"
        if (291 in self.s):
            print "Kabel 1"
        if (395 in self.s) and (132 in self.s) and (124 in self.s):
            print "Sat1"
        if (209 in self.s):
            print "Anixe"
        if (179 in self.s):
            print "QVC"
        if (507 in self.s):
            print "ARTE"
    if (112 in self.s):
```

```
64        print "RTL2"

66      """ Reset to empty state """
67      def reset(self):
68          self.s = {}

70  class TsharkParser:
71      """ Parser for Tshark CSV output """
72      def __init__(self, s):
73          self.s = s
74          self.lasttime = 0
75          # Use the ALRM signal to check if 5 seconds have passed since the
76          # last packet
77          signal.signal(signal.SIGALRM, self.handler)

79      """ parse a single line of input """
80      def parse(self, line):
81          [l, t] = re.split(",", line)
82          # check if input is broken, if so, skip this line
83          if (len(l) == 0) or (len(t) == 0):
84              return

86          # convert time to float and packet length to int
87          t = float(t)
88          l = int(l)

90          # if 5 seconds have passed in the capture, print the statistics
91          if (self.lasttime + 3.0 < t):
92              self.flush()

94          # reset timer
95          self.lasttime = t

97          # add the packet
98          self.s.add(l, t)

100         # start a new signal timer
101         signal.alarm(3)
102         #print "prepared alarm"

104     """ signal handler for SIGALRM """
105     def handler(self, signum, frame):
106         #print "Alarm triggered"
107         self.flush()

109     """ print the statistics and reset the statistics """
110     def flush(self):
111         self.s.show()
112         self.s.reset()

114 class InputReader:
115     """ Read output of tshark from stdin and process it with a TsharkParser """
116     def __init__(self, parser):
117         self.parser = parser

119     """ Run until end of input """
120     def run(self):
121   print "ich warte mal"
122   line = sys.stdin.readline()
123         print "jo"
124   while (line):
125             print line
126       self.parser.parse(line.rstrip())
127             line = sys.stdin.readline()
128         self.parser.flush()

130 if __name__ == '__main__':
131     stats = Stats()
132     parser = TsharkParser(stats)
133     reader = InputReader(parser)
134     reader.run()
135 }
```

C Original Questionnaire of Consumer Awareness and Attitudes

This appendix chapter shows the original questionnaire that is explained in Chapter 5. The survey was conducted in Germany. Thus, the next part is in German. Each framed box represents a page of the questionnaire. Due to readability some texts and links were modified but the changes do not change the meaning.

Seite 1 - Einleitung:

Fragebogen zu Smart TVs

Unterhaltungselektronik findet man heute in jedem Haushalt. Tauscht man alte Geräte gegen neuere Geräte aus, wird man feststellen, dass viele Geräte mit Internetfunktionen wie z.B. Skype oder Internet-Browser ausgestattet sind. Häufig können diese auch mit dem Smartphone oder einem Tablet bedient werden. Typische Beispiele sind Smart TVs, Spielekonsolen (wie z.B. Xbox oder PlayStation), Stereoanlagen mit Internetfunktionen und DVD/Blu-Ray Player. In dieser Studie werden wir Ihnen einige Fragen speziell für Fernseher mit Internetfunktionen (Smart TVs oder Fernseher mit internetfähigem Sat-/Kabel-Receiver) stellen.

Bevor Sie starten, wollen wir Ihnen noch folgende Hinweise geben:

- Ihre Informationen werden **anonym und ausschließlich zu wissenschaftlichen Zwecken ausgewertet**.
- Die Umfrage nimmt **ca. 20 Minuten** in Anspruch.
- Sie helfen uns am meisten, wenn Sie versuchen alle Fragen **wahrheitsgemäß** zu beantworten. Es gibt keine richtigen und falschen Antworten.

Sollten Sie Fragen haben, können Sie mich (Marco Ghiglieri, Technische Universität Darmstadt) jederzeit per E-Mail unter marco.ghiglieri@sit.tu-darmstadt.de kontaktieren.

Seite 2 - Smart-TV Demografie

Bevor wir starten, wollen wir Sie kurz darauf aufmerksam machen, dass Sie auf jeder Seite eine Information angezeigt bekommen, die kurz erklärt, was in dem Fragebogen unter Smart TV verstanden wird:

Smart TV
In diesem Fragebogen nennen wir alle Fernseher, die eine Möglichkeit haben Internetfunktionen zu nutzen, Smart TVs. Eingeschlossen sind hier auch Fernseher, die über einen internetfähigen Sat- oder Kabelreceiver angeschlossen sind.

1. Haben Sie einen Fernseher?*
   - Ja.
   - Nein.

Auswahlfeld

2. *Bei 1. Nein.* Wieso haben Sie keinen Fernseher ?*
   Sie können beliebig viele Gründe anwählen.
   - zu teuer.
   - keine Zeit um einen Fernseher zu nutzen.
   - Programme sind uninteressant.
   - Datenschutzbedenken.
   - Sicherheitsbedenken.
   - Ich möchte mir demnächst einen kaufen.
   - Sonstige Gründe: *Textfeld*
   - Ich möchte keinen Grund angeben.

   Auswahlfeld

3. *Bei 1. Ja.* Können Sie auf diesem Fernseher Internetfunktionen nutzen?*
   In diesem Fragebogen nennen wir alle Fernseher, die eine Möglichkeit haben Internetfunktionen zu nutzen, Smart TV.
   - Ja, es ist ein Smart TV.
   - Ja, es ist ein Fernseher mit Kabel- oder Sat-Receiver mit Internet.
   - Ja, aber ich weiß nicht, wie die Technik heißt.
   - Ich weiß es nicht.
   - Nein.

   Auswahlfeld

* Pflichtfeld/Pflichtangabe

Seite 3a - Smart-TV-Demografie (nur wenn Smart TV)

Smart TV
In diesem Fragebogen nennen wir alle Fernseher, die eine Möglichkeit haben Internetfunktionen zu nutzen, Smart TVs. Eingeschlossen sind hier auch Fernseher, die über einen internetfähigen Sat- oder Kabelreceiver angeschlossen sind.

1. Nutzen Sie Internet auf Ihrem Fernseher?*
   - Ja.
   - Vielleicht. Ich weiß nicht, welche Funktionen etwas mit Internet zu tun haben.
   - Nein.

   Auswahlfeld

* Pflichtfeld/Pflichtangabe

Seite 3b - Smart-TV-Demografie (nur wenn Fernseher und kein Smart TV)

Smart TV
In diesem Fragebogen nennen wir alle Fernseher, die eine Möglichkeit haben Internetfunktionen zu nutzen, Smart TVs. Eingeschlossen sind hier auch Fernseher, die über einen internetfähigen Sat- oder Kabelreceiver angeschlossen sind.

1. Würden Sie gerne Internet nutzen, wenn Ihr Fernseher es könnte ?
   - Ja.
   - Vielleicht, ich weiß es noch nicht.
   - Nein, weil *Textfeld*

   Auswahlfeld

* Pflichtfeld/Pflichtangabe
Wenn Nein, dann direkt zur Schlußseite.

Seite 4 - Gefahren

Smart TV
In diesem Fragebogen nennen wir alle Fernseher, die eine Möglichkeit haben Internetfunktionen zu nutzen, Smart TVs. Eingeschlossen sind hier auch Fernseher, die über einen internetfähigen Sat- oder Kabelreceiver angeschlossen sind.

1. Vermutlich ist Ihnen bekannt, dass im Internet verschiedene Gefahren lauern. In dieser Umfrage geht es hauptsächlich um Gefahren bei Smart TVs (TVs mit denen Sie Internetzugriff haben). Kennen Sie Gefahren oder Probleme bei Smart TVs?*
   - Ja.
   - Nein.

   Auswahlfeld

2. *Wenn Ja.* Welche Gefahren kennen Sie speziell bei Smart TVs? Wenn möglich erklären Sie das Problem auch. Stufen Sie für jede Gefahr ein, ob es für Sie eher eine kritische Gefahr ist oder nicht.*
   - Gefahr/Problem: *Textfeld*
     Erklärung: *Textfeld*
   - Gefahr/Problem: *Textfeld*
     Erklärung: *Textfeld*
   - Gefahr/Problem: *Textfeld*
     Erklärung: *Textfeld*
   - Gefahr/Problem: *Textfeld*
     Erklärung: *Textfeld*
   - Gefahr/Problem: *Textfeld*
     Erklärung: *Textfeld*

3. Tragen Sie Schutzmaßnahmen, die Sie für Smart TVs kennen in die Textfelder ein.
   - *Textfeld*
   - *Textfeld*
   - *Textfeld*
   - *Textfeld*
   - *Textfeld*

* Pflichtfeld/Pflichtangabe

Seite 5: Seite 5-8 in zufälliger Reihenfolge

Smart TV
In diesem Fragebogen nennen wir alle Fernseher, die eine Möglichkeit haben Internetfunktionen zu nutzen, Smart TVs. Eingeschlossen sind hier auch Fernseher, die über einen internetfähigen Sat- oder Kabelreceiver angeschlossen sind.

1. Stellen Sie sich nun folgendes Szenario vor und bewerten Sie, wie kritisch dieses für Sie im Bezug auf Sicherheit und/oder Datenschutz sind*.

   "Ihr Smart TV besitzt ein Mikrofon. Aufzeichnungen des Mikrofons können von Fremden aus dem Internet angehört werden. Sie merken davon nichts."
   Format Auswahl von unkritisch bis kritisch in 5 Stufen, sowie Ich weiß nicht, was gemeint ist.

2. Bitte begründen Sie Ihre oben gewählte Einstufung.* *Textfeld*

Seite 6: Seite 5-8 in zufälliger Reihenfolge

Smart TV
In diesem Fragebogen nennen wir alle Fernseher, die eine Möglichkeit haben Internetfunktionen zu nutzen, Smart TVs. Eingeschlossen sind hier auch Fernseher, die über einen internetfähigen Sat- oder Kabelreceiver angeschlossen sind.

1. Stellen Sie sich nun folgendes Szenario vor und bewerten Sie, wie kritisch dieses für Sie im Bezug auf Sicherheit und/oder Datenschutz sind*.

   "Der Sender, den Sie gerade schauen, bekommt Informationen darüber, wann und wie lange Sie ihn schauen. Bei Sendeanstalten mit mehreren Sendern (zum Beispiel Sat.1 und Pro Sieben), besteht die Möglichkeit, dass die Informationen beider Sender zusammengeführt werden."
   Format Auswahl von unkritisch bis kritisch in 5 Stufen, sowie Ich weiß nicht, was gemeint ist.

2. Bitte begründen Sie Ihre oben gewählte Einstufung.* *Textfeld*

Seite 7: Seite 5-8 in zufälliger Reihenfolge

Smart TV
In diesem Fragebogen nennen wir alle Fernseher, die eine Möglichkeit haben Internetfunktionen zu nutzen, Smart TVs. Eingeschlossen sind hier auch Fernseher, die über einen internetfähigen Sat- oder Kabelreceiver angeschlossen sind.

1. Stellen Sie sich nun folgendes Szenario vor und bewerten Sie, wie kritisch dieses für Sie im Bezug auf Sicherheit und/oder Datenschutz sind*.

   "Der Hersteller Ihres Smart TVs bekommt Informationen darüber, wie Sie den TV nutzen. Zum Beispiel bekommt der Hersteller detaillierte Informationen, welche Programme (z.B. Skype) Sie nutzen. Weiterhin bekommt er auch Informationen darüber wie lange und häufig Sie Ihren Smart TV nutzen"
   Format Auswahl von unkritisch bis kritisch in 5 Stufen, sowie Ich weiß nicht, was gemeint ist.

2. Bitte begründen Sie Ihre oben gewählte Einstufung.* *Textfeld*

Seite 8: Seite 5-8 in zufälliger Reihenfolge

Smart TV
In diesem Fragebogen nennen wir alle Fernseher, die eine Möglichkeit haben Internetfunktionen zu nutzen, Smart TVs. Eingeschlossen sind hier auch Fernseher, die über einen internetfähigen Sat- oder Kabelreceiver angeschlossen sind.

1. Stellen Sie sich nun folgendes Szenario vor und bewerten Sie, wie kritisch dieses für Sie im Bezug auf Sicherheit und/oder Datenschutz sind*.

   "Sie haben ein Smart TV mit Mikrofon und können ihn mit Sagen der Worte „TV ein" oder „TV aus" ein- bzw. ausschalten. Der Hersteller wertet die Sprachnachrichten auf seinen Servern aus. Es ist nicht ausgeschlossen, dass auch andere Stimmen zu den Servern geschickt werden."
   Format Auswahl von unkritisch bis kritisch in 5 Stufen, sowie Ich weiß nicht, was gemeint ist.

2. Bitte begründen Sie Ihre oben gewählte Einstufung.* *Textfeld*

Seite 9 - HbbTV

Smart TV
In diesem Fragebogen nennen wir alle Fernseher, die eine Möglichkeit haben Internetfunktionen zu nutzen, Smart TVs. Eingeschlossen sind hier auch Fernseher, die über einen internetfähigen Sat- oder Kabelreceiver angeschlossen sind.

In diesem Abschnitt wird es um die Funktion HbbTV gehen. Es ist die Abkürzung für Hybrid Broadcasting TV und fast alle Smart TVs ab 2012 haben diese Funktion integriert. Falls Sie den Namen nicht kennen, haben wir hier ein paar Bilder für Sie:

1. Haben Sie schon einmal diese (oder ähnliche) HbbTV-Meldungen aus den Bildern gesehen?*
   - Ja.
   - Vielleicht. Ich kann mich aber nicht erinnern.
   - Nein.

   Auswahlfeld

2. Wissen Sie, wo diese Meldung auf den Bildern herkommen?* Daten können über das Fernsehsignal und/oder über das Internet übertragen werden.
   - Ja, aus dem Internet.
   - Ja, vom Fernsehsignal.
   - Ja, aus dem Internet und dem Fernsehsignal.
   - Nein, weiß ich nicht.

   Auswahlfeld

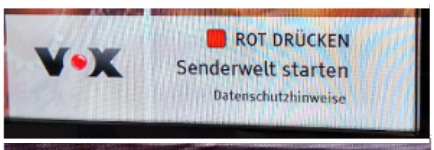
3. Gibt es aus Ihrer Sicht Sicherheits- und/oder Datenschutzgefahren bei HbbTV?*
   - Ja, Datenschutz, denn
   - Ja, Sicherheit, denn
   - Vielleicht, ich weiß es nicht.
   - Nein, da
   - Nein.

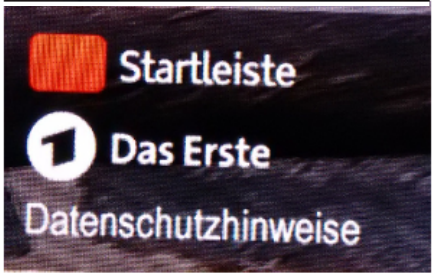
   Auswahlfeld

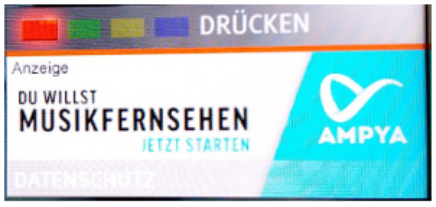
4. Wissen Sie, wie Sie HbbTV ausschalten können?*
   - Ja, im Menü unter
   - Ja,
   - Nein.

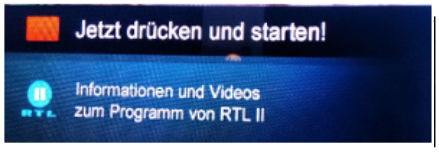
   Auswahlfeld

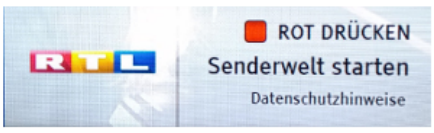
Seite 10 - Demografie











Allgemeine Fragen
Sie haben es bald geschafft. Zum Schluss noch ein paar allgemeine Fragen zu Ihrer Person.

1. Wie alt sind Sie?*
   Ich bin [x] Jahre alt.
   Format von x: Zahlen größer 18
2. Welches Geschlecht haben Sie ?*
   - weiblich
   - männlich
   - keine Angabe

   Auswahlfeld

* Pflichtfeld/Pflichtangabe

Seite 11 - Schlußseite

Vielen Dank für Ihre Teilnahme!

Wir möchten uns ganz herzlich für Ihre Mithilfe bedanken. Dieser Fragebogen hilft uns dabei Smart TVs sicherer und verständlicher zu machen. Er gibt ein Bild darüber, welche Unklarheiten im Bezug auf Sicherheit und Datenschutz bei Smart TVs bestehen.

Ihr Teilnahmecode lautet *Payment-Code*

Sollten Sie noch weitere Fragen zu diesem Fragebogen haben, können Sie sich gerne an Marco Ghiglieri unter der E-Mail marco.ghiglieri@sit.tu-darmstadt.de wenden.

Ihre Antworten wurden gespeichert, Sie können das Browser-Fenster nun schließen.

D Original Questionnaire of Evaluating Messages

This appendix chapter shows the original questionnaire that is explained in Chapter 6. The survey was conducted in Germany. Thus, the next part is in German. Each framed box represents a page of the questionnaire. Due to readability some texts and links were modified but the changes do not change the meaning.

Seite 1 - Einleitung:

Umfrage Smart TV

Smart TVs sind Fernseher, die mit dem Internet verbunden werden können. Entsprechend bieten sie innovative Internet-Funktionen und können regelmäßig aktualisiert (d.h. upgedatet) werden. Es gibt derzeit verschiedene Möglichkeiten, einen Smart TV zu nutzen.

Bevor Sie nun starten, möchten wir Ihnen noch folgende Hinweise geben:

- Ihre Informationen werden anonym und ausschließlich zu wissenschaftlichen Zwecken ausgewertet.
- Die Umfrage dauert etwa 10 Minuten.
- Sie helfen uns am meisten, wenn Sie versuchen, alle Fragen wahrheitsgemäß zu beantworten. Es gibt keine richtigen und falschen Antworten.
- Dieser Fragebogen ist nicht für Smartphones geeignet. Bitte nutzen Sie ein Tablet oder einen PC/Laptop.
- Bitte nutzen Sie nicht den Zurück-Button Ihres Browsers. Dies kann zu Fehlern und Abbrüchen führen.

Sollten Sie Fragen haben, können Sie mich (Marco Ghiglieri, Technische Universität Darmstadt) jederzeit per E-Mail unter marco.ghiglieri@sit.tu-darmstadt.de kontaktieren.

Seite 2 - Smart TV Demographie:

Bitte lesen Sie die Informationen aufmerksam durch, um die nachfolgenden Fragen zu beantworten!

Allgemeine Informationen zu Smart TVs
Smart TVs (auch Connected TVs oder Adressable TVs genannt) bieten zu den herkömmlichen Funktionen eines Fernsehers wie das Fernsehschauen, weitere Funktionen an, wenn sie mit dem Internet verbunden sind. Viele der Geräte verfügen über ein Mikrofon, welches eine Sprachsteuerung ermöglicht.
Es werden nur noch sehr wenige TVs verkauft, die keine Smart TVs sind.

1. Haben Sie einen Smart TV?*

- Ja.
- Nein.

Auswahlfeld

* Pflichtfeld/Pflichtangabe

Seite 3 - Reihenfolge von Seite 3 - 8 zufällig: Gefahren bei Smart TVs

Gefahren bei Smart TVs

Die Nutzung von Smart TVs, die mit dem Internet verbunden sind, birgt verschiedene Gefahren. Sechs dieser Gefahren zeigen wir Ihnen auf den folgenden Seiten an. Wir bitten Sie diese hinsichtlich empfundener Gefährlichkeit (wie kritisch finden Sie es) zu bewerten.

Bitte beachten Sie, dass sich viele Szenarien ähnlich anhören, sich aber im Detail unterscheiden. Lesen Sie daher die Texte sehr aufmerksam durch! Die Reihenfolge der Gefahren ist zufällig gewählt und haben daher keine zusammenhängende Bedeutung.

Gefahr 1 von 6

1. Wie kritisch stufen Sie die folgende Gefahr ein?*

   Das Mikrofon ist die ganze Zeit eingeschaltet, damit Sie Ihr Smart TV mit Ihrer Stimme bedienen können. Der Hersteller hat damit Zugriff auf alle Gespräche im Raum. Es kann nicht ausgeschlossen werden, dass diese Informationen in falsche Hände geraten und genutzt werden, um Ihnen zu schaden.

   Format Auswahl von unkritisch bis kritisch in 5 Stufen, sowie Ich weiß nicht, was gemeint ist.

2. Bitte begründen Sie Ihre Bewertung bezüglich Ihrer Einschätzung wie kritisch es ist.

   Format Textfeld

* Pflichtfeld/Pflichtangabe

Seite 4 - Reihenfolge von Seite 3 - 8 zufällig: Gefahren bei Smart TVs

Gefahren bei Smart TVs

Die Nutzung von Smart TVs, die mit dem Internet verbunden sind, birgt verschiedene Gefahren. Sechs dieser Gefahren zeigen wir Ihnen auf den folgenden Seiten an. Wir bitten Sie diese hinsichtlich empfundener Gefährlichkeit (wie kritisch finden Sie es) zu bewerten.

Bitte beachten Sie, dass sich viele Szenarien ähnlich anhören, sich aber im Detail unterscheiden. Lesen Sie daher die Texte sehr aufmerksam durch! Die Reihenfolge der Gefahren ist zufällig

gewählt und haben daher keine zusammenhängende Bedeutung.

Gefahr 2 von 6

1. Wie kritisch stufen Sie die folgende Gefahr ein?*

   Smart TVs sind ohne weitere Sicherheitsmaßnahmen viel anfälliger für Angriffe als PCs/Laptops und Smartphones. Es besteht die Gefahr, dass Hacker Zugriff auf Ihren Smart TV erhalten und das Mikrofon unbemerkt einschalten. Dadurch kann der Hacker z.B. feststellen, wann der beste Zeitpunkt zum Einbruch in Ihre Wohnung (bzw. in Ihr Haus) ist.

   Format Auswahl von unkritisch bis kritisch in 5 Stufen, sowie Ich weiß nicht, was gemeint ist.

2. Bitte begründen Sie Ihre Bewertung bezüglich Ihrer Einschätzung wie kritisch es ist.

   Format Textfeld

* Pflichtfeld/Pflichtangabe

Seite 5 - Reihenfolge von Seite 3 - 8 zufällig: Gefahren bei Smart TVs

Gefahren bei Smart TVs

Die Nutzung von Smart TVs, die mit dem Internet verbunden sind, birgt verschiedene Gefahren. Sechs dieser Gefahren zeigen wir Ihnen auf den folgenden Seiten an. Wir bitten Sie diese hinsichtlich empfundener Gefährlichkeit (wie kritisch finden Sie es) zu bewerten.

Bitte beachten Sie, dass sich viele Szenarien ähnlich anhören, sich aber im Detail unterscheiden. Lesen Sie daher die Texte sehr aufmerksam durch! Die Reihenfolge der Gefahren ist zufällig gewählt und haben daher keine zusammenhängende Bedeutung.

Gefahr 3 von 6

1. Wie kritisch stufen Sie die folgende Gefahr ein?*

   Smart TVs sind ohne weitere Sicherheitsmaßnahmen viel anfälliger für Angriffe als PCs/Laptops und Smartphones. Wenn Sie Ihr Smart TV ohne weitere Schutzmaßnahme an das Internet anschließen, besteht die Gefahr, dass Hacker Zugriff auf Ihr Smart TV erhalten und das Mikrofon unbemerkt einschalten. Dadurch kann der Hacker z.B. Informationen über Sie sammeln, um Ihnen zu schaden.

   Format Auswahl von unkritisch bis kritisch in 5 Stufen, sowie Ich weiß nicht, was gemeint ist.

2. Bitte begründen Sie Ihre Bewertung bezüglich Ihrer Einschätzung wie kritisch es ist.

   Format Textfeld

* Pflichtfeld/Pflichtangabe

Seite 6 - Reihenfolge von Seite 3 - 8 zufällig: Gefahren bei Smart TVs

Gefahren bei Smart TVs

Die Nutzung von Smart TVs, die mit dem Internet verbunden sind, birgt verschiedene Gefahren. Sechs dieser Gefahren zeigen wir Ihnen auf den folgenden Seiten an. Wir bitten Sie diese hinsichtlich empfundener Gefährlichkeit (wie kritisch finden Sie es) zu bewerten.

Bitte beachten Sie, dass sich viele Szenarien ähnlich anhören, sich aber im Detail unterscheiden. Lesen Sie daher die Texte sehr aufmerksam durch! Die Reihenfolge der Gefahren ist zufällig gewählt und haben daher keine zusammenhängende Bedeutung.

Gefahr 4 von 6

1. Wie kritisch stufen Sie die folgende Gefahr ein?*

   Ihre Nutzungsgewohnheiten (d.h. z.B. wozu Sie Ihren Smart TV wann und wie oft nutzen) werden beim Hersteller und bei den TV Sendern gespeichert. Die über Sie gesammelten Informationen werden analysiert, um Ihnen personalisierte (d.h. auf Sie zugeschnittene) Werbung anzuzeigen.

   Format Auswahl von unkritisch bis kritisch in 5 Stufen, sowie Ich weiß nicht, was gemeint ist.

2. Bitte begründen Sie Ihre Bewertung bezüglich Ihrer Einschätzung wie kritisch es ist.

   Format Textfeld

* Pflichtfeld/Pflichtangabe

Seite 7 - Reihenfolge von Seite 3 - 8 zufällig: Gefahren bei Smart TVs

Gefahren bei Smart TVs

Die Nutzung von Smart TVs, die mit dem Internet verbunden sind, birgt verschiedene Gefahren. Sechs dieser Gefahren zeigen wir Ihnen auf den folgenden Seiten an. Wir bitten Sie diese hinsichtlich empfundener Gefährlichkeit (wie kritisch finden Sie es) zu bewerten.

Bitte beachten Sie, dass sich viele Szenarien ähnlich anhören, sich aber im Detail unterscheiden. Lesen Sie daher die Texte sehr aufmerksam durch! Die Reihenfolge der Gefahren ist zufällig gewählt und haben daher keine zusammenhängende Bedeutung.

Gefahr 5 von 6

1. Wie kritisch stufen Sie die folgende Gefahr ein?*

   Ihre Nutzungsgewohnheiten (d.h. z.B. wozu Sie Ihren Smart TV wann und wie oft nutzen) werden beim Hersteller und bei den TV Sendern gespeichert. Es kann nicht ausgeschlossen werden, dass die über Sie gesammelten Informationen in falsche Hände geraten und genutzt werden, um Ihnen zu schaden.

   Format Auswahl von unkritisch bis kritisch in 5 Stufen, sowie Ich weiß nicht, was gemeint ist.

2. Bitte begründen Sie Ihre Bewertung bezüglich Ihrer Einschätzung wie kritisch es ist.

   Format Textfeld

* Pflichtfeld/Pflichtangabe

Seite 8 - Reihenfolge von Seite 3 - 8 zufällig: Gefahren bei Smart TVs

Gefahren bei Smart TVs

Die Nutzung von Smart TVs, die mit dem Internet verbunden sind, birgt verschiedene Gefahren. Sechs dieser Gefahren zeigen wir Ihnen auf den folgenden Seiten an. Wir bitten Sie diese hinsichtlich empfundener Gefährlichkeit (wie kritisch finden Sie es) zu bewerten.

Bitte beachten Sie, dass sich viele Szenarien ähnlich anhören, sich aber im Detail unterscheiden. Lesen Sie daher die Texte sehr aufmerksam durch! Die Reihenfolge der Gefahren ist zufällig gewählt und haben daher keine zusammenhängende Bedeutung.

Gefahr 6 von 6

1. Wie kritisch stufen Sie die folgende Gefahr ein?*

   Ihre Nutzungsgewohnheiten (d.h. z.B. wozu Sie Ihren Smart TV wann und wie oft nutzen) werden beim Hersteller und bei den TV Sendern gespeichert und analysiert.

   Format Auswahl von unkritisch bis kritisch in 5 Stufen, sowie Ich weiß nicht, was gemeint ist.

2. Bitte begründen Sie Ihre Bewertung bezüglich Ihrer Einschätzung wie kritisch es ist.

   Format Textfeld

* Pflichtfeld/Pflichtangabe

Seite 9 - Demographie:

...und zum Schluss

Wir bitten Sie noch einige Daten für statistische Zwecke auszufüllen.

1. Wie alt sind Sie?*
   Ich bin [x] Jahre alt.
   Format von x: Zahlen größer 18

2. Welches Geschlecht haben Sie ?*
   weiblich, männlich, keine Angabe
   Auswahlfeld

* Pflichtfeld/Pflichtangabe

Seite 10 - Vielen Dank:

Vielen Dank für Ihre Teilnahme!

Wir möchten uns ganz herzlich für Ihre Mithilfe bedanken. Dieser Fragebogen hilft uns dabei Smart TVs sicherer und verständlicher zu machen.

Ihr Bestätigungscode lautet *Payment-Code*.

Sollten Sie noch weitere Fragen zu diesem Fragebogen haben, können Sie sich gerne an Marco Ghiglieri unter der E-Mail marco.ghiglieri@sit.tu-darmstadt.de wenden.

Ihre Antworten wurden gespeichert, Sie können das Browser-Fenster nun schließen.

E Original Questionnaire of Raising Awareness

This appendix chapter shows the original questionnaire that is explained in Chapter 7. The survey was conducted in Germany. Thus, the next part is in German. Each framed box represents a page of the questionnaire. Due to readability some texts and links were modified but the changes do not change the meaning.

Seite 1 - Einleitung:

Umfrage zur Smart TV Nutzung

Smart TVs sind Fernseher, die mit dem Internet verbunden werden können. Entsprechend bieten sie innovative Internet-Funktionen und können regelmäßig aktualisiert (d.h. upgedatet) werden. Es gibt derzeit verschiedene Möglichkeiten, einen Smart TV zu nutzen.

Bevor Sie nun starten, möchten wir Ihnen noch folgende Hinweise geben:

- Ihre Informationen werden anonym und ausschließlich zu wissenschaftlichen Zwecken ausgewertet.
- Die Umfrage dauert etwa 5-10 Minuten.
- Sie helfen uns am meisten, wenn Sie versuchen, alle Fragen wahrheitsgemäß zu beantworten. Es gibt keine richtigen und falschen Antworten.
- Dieser Fragebogen ist nicht für Smartphones geeignet. Bitte nutzen Sie ein Tablet oder einen PC/Laptop.
- Bitte nutzen Sie nicht den Zurück-Button Ihres Browsers. Dies kann zu Fehlern und Abbrüchen führen.

Sollten Sie Fragen haben, können Sie mich (Marco Ghiglieri, Technische Universität Darmstadt) jederzeit per E-Mail unter marco.ghiglieri@sit.tu-darmstadt.de kontaktieren.

Seite 2 - Smart-TV Demographie:

Bitte lesen Sie die Informationen aufmerksam durch, um die nachfolgenden Fragen zu beantworten!

Allgemeine Informationen zu Smart TVs
Smart TVs (auch Connected TVs oder Adressable TVs genannt) bieten zu den herkömmlichen Funktionen eines Fernsehers wie das Fernsehschauen, weitere Funktionen an, wenn sie mit dem Internet verbunden sind. Viele der Geräte verfügen über ein Mikrofon, welches eine Sprachsteuerung ermöglicht.
Es werden nur noch sehr wenige TVs verkauft, die keine Smart TVs sind.

1. Haben Sie einen Smart TV?*

- Ja.
- Nein.

Auswahlfeld

* Pflichtfeld/Pflichtangabe

Seite 3 - Smart-TV Demographie:

Internet-Funktionen
Internet-Funktionen erfordern, dass der Smart TV mit dem Internet verbunden ist. Dies geschieht entweder per Kabel oder WLAN. Beispiele für Internet-Funktionen sind

- Mediatheken der Sender für verpasste Sendungen, sowie verschiedener anderer Anbieter wie z.B. Maxdome, Watchever, Amazon,
- Live-Informationen zum laufenden TV-Programm,
- Direkte Homeshopping-Möglichkeit auf Teleshopping-Kanälen,
- Spiele direkt auf dem Fernsehbildschirm,
- und viele mehr...

Einige Programme (auch Apps genannt), die von Smartphones/PCs bekannt sind, gibt es auch für den Smart TV z.B. Facebook.

1. Ich nutze oder würde gerne Internet-Funktionen auf meinem Smart TV regelmäßig nutzen.* Trifft nicht zu (1) bis Trifft zu (5).
   Auswahl mit 5-Punkten

* Pflichtfeld/Pflichtangabe

Seite 4 - Auswahl Möglichkeit:

Informationstext zu Funktionen
Hier finden Sie die unveränderten Texte der Einführungsseiten. Klicken Sie auf “Erklärung zu .. von der Einführungsseite anzeigen” werden diese Informationen sichtbar.

- Erklärung zu Internet-Funktionen von der Einführungsseite anzeigen *Original war ein Link*
- Verschiedene Möglichkeiten zur Nutzung eines Smart TVs *Original war ein Link*

Verschiedene Möglichkeiten zur Nutzung eines Smart TVs
Wir betrachten **zwei** verschiedene Möglichkeiten einen Smart TV zu nutzen. In der unten dargestellten Tabelle ist pro Spalte eine Möglichkeit dargestellt. Die Reihenfolge der Möglichkeiten ist zufällig und hat keine weitere Bedeutung. Im Folgenden werden wir Ihnen diese Möglichkeiten mit ihren Vor- und Nachteilen bzgl. Funktionalität, Sicherheit und Privatsphäre vorstellen.
Bitte lesen Sie sich die Angaben in Ruhe durch und wählen Sie Ihre bevorzugte Möglichkeit nach

folgender Fragestellung aus:

Wie würden Sie gerne Ihren Smart TV nutzen (den Sie bereits besitzen bzw. angenommen Sie würden sich einen kaufen)?*

Bitte wählen Sie die von Ihnen präferierte Möglichkeit in der letzten Zeile der Tabelle aus.

Die Tabelle befindet sich für den Fragebogen in Table E.1. In der ursprünglichen Version des Fragebogens wurde sie an dieser Stelle eingeblendet.

Der Platzhalter Gefahr in der Tabelle wurde abwechselnd ersetzt durch

- *"Ihre Nutzungsgewohnheiten (d.h. z.B. wozu Sie Ihren Smart TV wann und wie oft nutzen) werden beim Hersteller und bei den TV Sendern gespeichert und analysiert".*
- *"Ihre Nutzungsgewohnheiten (d.h. z.B. wozu Sie Ihren Smart TV wann und wie oft nutzen) werden beim Hersteller und bei den TV Sendern gespeichert. Es kann nicht ausgeschlossen werden, dass die über Sie gesammelten Informationen in falsche Hände geraten und genutzt werden, um Ihnen zu schaden."*

Der Platzhalter Keine Gefahr war im Fragebogen "Keine Gefahr Ihrer Privatsphäre und der Sicherheit des Smart TVs"

1. Bitte begründen Sie Ihre oben getroffene Auswahl.*
   Freitext

* Pflichtfeld/Pflichtangabe

	Der Smart TV wird ohne weitere Vorkehrungen **mit dem Internet** verbunden	Der Smart TV wird **gar nicht mit dem Internet verbunden**
Internet-Funktionen	Keine Einschränkung	Nicht verfügbar / keine Updates
Gefahr	*Gefahr*	*Keine Gefahr*
Zusätzlicher Aufwand	Keiner	Keiner
Zusätzliche Kosten	Keine	Keine
Ihre Auswahl	☐	☐

Table E.1.: Appendix: Tabelle mit Nachrichten

Seite 5 - Demographie:

...und zum Schluss

Wir bitten Sie noch einige Daten für statistische Zwecke auszufüllen.

1. Wie alt sind Sie?*
   Ich bin [x] Jahre alt.
   Format von x: Zahlen größer 18

2. Welches Geschlecht haben Sie ?*
   weiblich, männlich, keine Angabe
   Auswahlfeld

* Pflichtfeld/Pflichtangabe

Seite 6 - Vielen Dank:

Vielen Dank für Ihre Teilnahme!

Wir möchten uns ganz herzlich für Ihre Mithilfe bedanken. Dieser Fragebogen hilft uns dabei Smart TVs sicherer und verständlicher zu machen.

Ihr Bestätigungscode lautet *Payment-Code*.

Sollten Sie noch weitere Fragen zu diesem Fragebogen haben, können Sie sich gerne an Marco Ghiglieri unter der E-Mail marco.ghiglieri@sit.tu-darmstadt.de wenden.

Ihre Antworten wurden gespeichert, Sie können das Browser-Fenster nun schließen.

F Original Questionnaire of Raising Awareness and Offering Alternatives for Connecting the Smart TV

This appendix chapter shows the original questionnaire that is explained in Chapter 8. The survey was conducted in Germany. Thus, the next part is in German. Each framed box represents a page of the questionnaire. Due to readability some texts and links were modified but the changes do not change the meaning.

Seite 1 - Einleitung:

Umfrage zur Smart TV Nutzung

Smart TVs sind Fernseher, die mit dem Internet verbunden werden können. Entsprechend bieten sie innovative Internet-Funktionen und können regelmäßig aktualisiert (d.h. upgedatet) werden. Es gibt derzeit verschiedene Möglichkeiten, einen Smart TV zu nutzen.

Bevor Sie nun starten, möchten wir Ihnen noch folgende Hinweise geben:

- Ihre Informationen werden anonym und ausschließlich zu wissenschaftlichen Zwecken ausgewertet.
- Die Umfrage dauert etwa 5-10 Minuten.
- Sie helfen uns am meisten, wenn Sie versuchen, alle Fragen wahrheitsgemäß zu beantworten. Es gibt keine richtigen und falschen Antworten.
- Dieser Fragebogen ist nicht für Smartphones geeignet. Bitte nutzen Sie ein Tablet oder einen PC/Laptop.
- Bitte nutzen Sie nicht den Zurück-Button Ihres Browsers. Dies kann zu Fehlern und Abbrüchen führen.

Sollten Sie Fragen haben, können Sie mich (Marco Ghiglieri, Technische Universität Darmstadt) jederzeit per E-Mail unter marco.ghiglieri@sit.tu-darmstadt.de kontaktieren.

Seite 2 - Smart-TV Demographie:

Bitte lesen Sie die Informationen aufmerksam durch, um die nachfolgenden Fragen zu beantworten!

Allgemeine Informationen zu Smart TVs
Smart TVs (auch Connected TVs oder Adressable TVs genannt) bieten zu den herkömmlichen Funktionen eines Fernsehers wie das Fernsehschauen, weitere Funktionen an, wenn sie mit dem Internet verbunden sind. Viele der Geräte verfügen über ein Mikrofon, welches eine Sprachsteuerung ermöglicht.
Es werden nur noch sehr wenige TVs verkauft, die keine Smart TVs sind.

1. Haben Sie einen Smart TV?*

- Ja.
- Nein.

Auswahlfeld

* Pflichtfeld/Pflichtangabe

Seite 3 - Smart-TV Demographie:

Internet-Funktionen
Internet-Funktionen erfordern, dass der Smart TV mit dem Internet verbunden ist. Dies geschieht entweder per Kabel oder WLAN. Beispiele für Internet-Funktionen sind

- Mediatheken der Sender für verpasste Sendungen, sowie verschiedener anderer Anbieter wie z.B. Maxdome, Watchever, Amazon,
- Live-Informationen zum laufenden TV-Programm,
- Direkte Homeshopping-Möglichkeit auf Teleshopping-Kanälen,
- Spiele direkt auf dem Fernsehbildschirm,
- und viele mehr...

Einige Programme (auch Apps genannt), die von Smartphones/PCs bekannt sind, gibt es auch für den Smart TV z.B. Facebook.

1. Ich nutze oder würde gerne Internet-Funktionen auf meinem Smart TV regelmäßig nutzen.* Trifft nicht zu (1) bis Trifft zu (5).
   Auswahl mit 5-Punkten

* Pflichtfeld/Pflichtangabe

Seite 4 - Auswahl Möglichkeit:

Informationstext zu Funktionen
Hier finden Sie die unveränderten Texte der Einführungsseiten. Klicken Sie auf “Erklärung zu .. von der Einführungsseite anzeigen” werden diese Informationen sichtbar.

- Erklärung zu Internet-Funktionen von der Einführungsseite anzeigen *Original war ein Link*
- Verschiedene Möglichkeiten zur Nutzung eines Smart TVs *Original war ein Link*

Wir betrachten fünf verschiedene Möglichkeiten einen Smart TV ans Internet anzuschließen. In der unten dargestellten Tabelle ist pro Spalte eine Möglichkeit dargestellt. Die Reihenfolge der Möglichkeiten ist zufällig und hat keine weitere Bedeutung. Im Folgenden werden wir Ihnen diese Möglichkeiten mit ihren Vor- und Nachteilen bzgl. Funktionalität, Sicherheit und Privatsphäre, Aufwand und Kosten vorstellen.
Bitte lesen Sie sich die Angaben in Ruhe durch und wählen Sie Ihre bevorzugte Möglichkeit nach

folgender Fragestellung aus:

Wie würden Sie gerne Ihren Smart TV nutzen (den Sie bereits besitzen bzw. angenommen Sie würden sich einen kaufen)?*

Bitte wählen Sie die von Ihnen präferierte Möglichkeit in der letzten Zeile der Tabelle aus.

Die Tabelle befindet sich für den Fragebogen in Table E.1. In der ursprünglichen Version des Fragebogens wurde sie an dieser Stelle eingeblendet.

Der Platzhalter Gefahr in der Tabelle wurde abwechselnd ersetzt durch

- *"Ihre Nutzungsgewohnheiten (d.h. z.B. wozu Sie Ihren Smart TV wann und wie oft nutzen) werden beim Hersteller und bei den TV Sendern gespeichert und analysiert".*
- *"Ihre Nutzungsgewohnheiten (d.h. z.B. wozu Sie Ihren Smart TV wann und wie oft nutzen) werden beim Hersteller und bei den TV Sendern gespeichert. Es kann nicht ausgeschlossen werden, dass die über Sie gesammelten Informationen in falsche Hände geraten und genutzt werden, um Ihnen zu schaden."*

Der Platzhalter Keine Gefahr war im Fragebogen "Keine Gefahr Ihrer Privatsphäre und der Sicherheit des Smart TVs"

1. Bitte begründen Sie Ihre oben getroffene Auswahl.*
   Freitext

* Pflichtfeld/Pflichtangabe

Seite 5 - Demographie:

...und zum Schluss

An dieser Stelle wollen wir Sie noch darauf aufmerksam machen, dass die beiden Möglichkeiten eines Smart TV Schutzes noch nicht auf dem Markt sind. Sie haben mit Ausfüllen dieser Umfrage aktiv geholfen diese Schutzmöglichkeiten zu erforschen.

Wir bitten Sie noch einige Daten für statistische Zwecke auszufüllen.

1. Wie alt sind Sie?*
   Ich bin [x] Jahre alt.
   Format von x: Zahlen größer 18
2. Welches Geschlecht haben Sie ?*
   weiblich, männlich, keine Angabe
   Auswahlfeld

* Pflichtfeld/Pflichtangabe

Seite 6 - Vielen Dank:

	Der Smart TV wird ohne weitere Vorkehrungen **mit dem Internet** verbunden	Der Smart TV wird **gar nicht mit dem Internet verbunden**	Der Smart TV wird nicht mit dem Internet verbunden und wird zusätzlich **als externer Monitor** für einen PC/Laptop genutzt	Der Smart TV wird erst **von Ihnen über eine Schutzsoftware** abgesichert, bevor Sie ihn an das Internet anschließen	Der Smart TV wird über eine **vorkonfigurierte Schutzsoftware** abgesichert, bevor Sie ihn an das Internet anschließen
Internet-Funktionen	Keine Einschränkung	Nicht verfügbar / keine Updates	Nur Standard-Funktionen des Laptops/PCs inkl. Mediathek / keine Updates	Keine Einschränkung	Keine Einschränkung
Gefahr	*Gefahr*	*Keine Gefahr*	*Keine Gefahr*	*Keine Gefahr*	*Keine Gefahr*
Zusätzlicher Aufwand	Keiner	Keiner	Laptop/PC muss konfiguriert und angeschlossen werden	Keiner, da vorkonfiguriert	einmalig 15 min. zur Konfiguration der Schutzsoftware
Zusätzliche Kosten	Keine	Keine	Keine	einmalig 20€	einmalig 40€
Ihre Auswahl	☐	☐	☐	☐	☐

Table F.1.: Appendix: Tabelle mit Alternativen

Vielen Dank für Ihre Teilnahme!

Wir möchten uns ganz herzlich für Ihre Mithilfe bedanken. Dieser Fragebogen hilft uns dabei Smart TVs sicherer und verständlicher zu machen.

Ihr Bestätigungscode lautet *Payment-Code*.

Sollten Sie noch weitere Fragen zu diesem Fragebogen haben, können Sie sich gerne an Marco Ghiglieri unter der E-Mail marco.ghiglieri@sit.tu-darmstadt.de wenden.

Ihre Antworten wurden gespeichert, Sie können das Browser-Fenster nun schließen.

G Additional Details for the Chapter Developing an Alternative to Connect the Smart TV

The explanations for the source codes can be found in Chapter 9.

Source Code of Information Extraction and Processing

```
import json
import time

def main():

  f=open("logs/eve.json")
  while 1:
    where=f.tell()
    line=f.readline()
    if not line:
      time.sleep(1)
      f.seek(where)
    else:
      try:
        j=json.loads(line)

        if 'alert' in j:
          # Extraction of HbbTV
          if 'signature_id' in j['alert']:
            if j['alert']['signature_id']==997001:
              h=open("hbbtv.txt","r")
              urlsin=[]
              for l in h:
                urlsin.append(l)
              h.close()
              url=("http://%s%s\n") % (j['http']['hostname'],j['http']['url'])
              if not url in urlsin:
                h=open("hbbtv.txt","a")
                h.write(("%s\n") % url)
                h.close()

            else: #other alerts
              h=open("alerts.txt","a")
              h.write(("%s|%s\n") % (time.time(),j['alert']['signature']))
              h.close()
      except:
        pass

if __name__ == "__main__":
    main()
```

Source Code of Device Detection with SSDP

```
#   Copyright 2014 Dan Krause
# Extended by Marco Ghiglieri 2017
#
#   Licensed under the Apache License, Version 2.0 (the "License");
#   you may not use this file except in compliance with the License.
#   You may obtain a copy of the License at
#
#       http://www.apache.org/licenses/LICENSE-2.0
#
#   Unless required by applicable law or agreed to in writing, software
#   distributed under the License is distributed on an "AS IS" BASIS,
#   WITHOUT WARRANTIES OR CONDITIONS OF ANY KIND, either express or implied.
#   See the License for the specific language governing permissions and
#   limitations under the License.
```

```
16 import socket
17 import httplib
18 import StringIO
19 import urllib2
20 import time
21 from urlparse import urlparse
22 import os

24 class SSDPResponse(object):
25     class _FakeSocket(StringIO.StringIO):
26         def makefile(self, *args, **kw):
27             return self
28     def __init__(self, response):
29         r = httplib.HTTPResponse(self._FakeSocket(response))
30         r.begin()
31         self.location = r.getheader("location")
32         self.usn = r.getheader("usn")
33         self.st = r.getheader("st")
34         self.cache = r.getheader("cache-control").split("=")[1]
35     def __repr__(self):
36         return "<SSDPResponse({location}, {st}, {usn})>".format(**self.__dict__)

38 def discover(service, timeout=2, retries=1):
39     group = ("239.255.255.250", 1900)
40     message = "\r\n".join([
41         'M-SEARCH * HTTP/1.1',
42         'HOST: {0}:{1}',
43         'MAN: "ssdp:discover"',
44         'ST: {st}','MX: 3','',''])
45     socket.setdefaulttimeout(timeout)
46     responses = {}
47     for _ in range(retries):
48         sock = socket.socket(socket.AF_INET, socket.SOCK_DGRAM, socket.IPPROTO_UDP)
49         sock.setsockopt(socket.SOL_SOCKET, socket.SO_REUSEADDR, 1)
50         sock.setsockopt(socket.IPPROTO_IP, socket.IP_MULTICAST_TTL, 2)
51         sock.bind(("192.168.0.111",1900))
52         print sock.getsockname()
53         sock.sendto(message.format(*group, st=service), group)
54         while True:
55             try:
56                 response = SSDPResponse(sock.recv(1024))
57                 responses[response.location] = response
58             except socket.timeout:
59                 break
60     return responses.values()
61 # Added Marco Ghiglieri
62 def friendlyNames():
63     devices=discover("ssdp:all")
64     device_data=[]
65     for device in devices:
66         try:
67             f = urllib2.urlopen(device.location)
68             data=f.read()
69             odata=data
70             if "<friendlyName>" in data:
71                 fn=data[:data.rfind("</friendlyName>")]
72                 fn=fn[fn.rfind("<friendlyName>")+len("<friendlyName>"):]

74                 mn=data[:data.rfind("</modelName>")]
75                 mn=mn[mn.rfind("<modelName>")+len("<modelName>"):]

77                 try:
78                     fn=unicode(fn)
79                 except:
80                     try:
81                         mn=unicode(mn)
82                         fn=mn
83                     except:
84                         fn="Not known"

86                 hostname=urlparse(device.location).hostname
```

```
87                  host=socket.gethostbyname(hostname)

89                  device_data.append( (host,fn,mn) )
90              f.close()
91          except:
92              print device.location+" not possible"
93      return device_data

95  def main():
96    print "started"

98    f=open("ssdp.txt", 'w')
99    f.write("%s\n" % (time.time()))
100   for item in friendlyNames():
101     f.write("%s|%s\n" % (item[0], item[1]))
102   f.close()



106 if __name__ == "__main__":
107     main()
```

Source Code of Consumer Decision

```
1   #! /usr/bin/env python

3   import os
4   import sys
5   from urlparse import urlparse

7   path=os.path.abspath(os.path.dirname(__file__))
8   path=path[:path.rfind('/')]
9   sys.path.append(path)
10  os.environ['DJANGO_SETTINGS_MODULE'] = 'settings'

12  from django.conf import settings
13  from django.db import models
14  from core.models import *

16  hbbtvlist="/home/marco/ownCloud/Marco_Suricata/hbbtvprotector/hbbtvlist.txt"

18  #Check new HbbTV urls in HbbTVlist

20  f=open(hbbtvlist, "r")
21  for line in f:
22      if len(line)>1:
23          status,url=line.strip().replace("\n","").split("|")
24          channels=HbbTVChannel.objects.filter(url=url)
25          host=urlparse(url)
26          if len(channels)==0:
27              HbbTVChannel(channel=host.netloc, url=url).save()

29  f.close()
30  #Transfer status to HbbTVlist

32  f=open(hbbtvlist, "w")
33  channels=HbbTVChannel.objects.filter(visible=True)

35  for item in channels:
36      if item.decision=="B":
37          status=0
38      elif item.decision=="AA":
39          status=2
40      else:
41          status=1
42      f.write("%s|%s\n" % (status, item.url))
43  f.close()
```

Source Code of *HbbTV Privacy Protector*

```
# HbbTV Privacy Protector

from libmproxy.models import HTTPResponse
from netlib.http import Headers
import os


abs_path="/home/marco/ownCloud/Marco_Suricata/hbbtvprotector"
srv_url="http://192.168.0.111/"
hbbtvlist=abs_path+'/hbbtvlist.txt'
lang="en"
coreprotector=False

red_url = srv_url+lang+"_overview.hbbtv"
urls = set()
remember=""
intercept =True
urlstatus=dict()


def load_urls():
  f = open(hbbtvlist, 'r')
  for line in f:
    line=line.replace("\n","").replace("\r","")
    status,url=line.split('|')
    urlstatus[url]=status
    urls.add(url)
  f.close()
load_urls()

def save_urls():
  f=open(hbbtvlist, 'w')
  for url in urls:
    url=url.replace("\n","").replace("\r","")
    if len(url)>2:
      f.write("%s|%s\n" % (urlstatus[url], url))
  f.close()

def remember_HbbTV(flow,urls):
  remember=""
  for item in urls:
    if item==str(get_url(flow)):
      remember=str(get_url(flow))
  return remember

def redirect_response(flow,answer,location):
  content =  "<html><head><title>Redirect</title></head><body>Redirect</body></html>"
  resp = HTTPResponse("HTTP/1.1", 307, "Temporary Redirect", Headers(Content_Type="text/html", Location=
      location),content)
  flow.reply(resp)

def block_response(flow,answer):
  content =  "<html><head><title>Blocked</title></head><body>Blocked</body></html>"
  resp = HTTPResponse("HTTP/1.1", 200, "OK",Headers(Content_Type="text/html"), content)
  flow.reply(resp)

def get_url(flow):
  return "%s://%s%s" % (flow.request.scheme, flow.request.pretty_host, flow.request.path)

def response(context, flow):
  global urls, red_url, intercept,  remember
  # Some File types should not be checked
  if flow.response.headers['content-type'] not in ['image/jpeg','image/png','image/gif','video/mp4','
      video/x-flv','application/x-javascript']:

    # If an object with this type is found HbbTV signal is found
    if "application/oipfApplicationManager" in flow.response.content:

      # If this HbbTV URL has not been found, add it
      if coreprotector==False and not get_url(flow) == red_url:
        if len(str(get_url(flow)))>3:
          url=str(get_url(flow))
```

```
            urls.add(url)
            #add standard behavior
            if not url in urlstatus:
              urlstatus[url]="2"
            urls=set(urls)
            save_urls()


        if intercept:
          remember=remember_HbbTV(flow,urls)

        # Channel changed
        intercept=True
        load_urls()

def request(context, flow):
  global intercept,urls, remember, red_url

  if not str(get_url(flow))[-3:] in ["png","gif","mp4","jpg"]:
    flow.request.anticache()
  # If an HbbTV URL in interception mode is found, stop

  if (get_url(flow) in urls and urlstatus[get_url(flow)]=="2") and intercept:
    # Save URL of HbbTV
    remember=remember_HbbTV(flow,urls)
    # Redirect to local web server
    redirect_response(flow, flow.request,red_url)

  if (get_url(flow) in urls and urlstatus[get_url(flow)]=="0") and intercept:
    # Block to local web server
    block_response(flow, flow.request)


  # If this url is found, stop interception
  if get_url(flow) == "http://1.2.3.4/do-not-intercept":
    # Set interception False
    intercept = False
    # Redirect to HbbTV
    redirect_response(flow,flow.request,remember)
```

Source Code of HbbTV application provided by the *HbbTV Privacy Protector*

Both files are delivered to the Smart TV, when interception mode of the *HbbTV Privacy Protector* is enabled.

HTML file: en_overview.hbbtv

```
<?xml version="1.0" encoding="utf-8" ?>
<!DOCTYPE html PUBLIC "-//W3C//DTD XHTML 1.0 Transitional//EN" "http://www.w3.org/TR/xhtml1/DTD/xhtml1-
    loose.dtd">
<html xmlns="http://www.w3.org/1999/xhtml">
<head>
<meta http-equiv="Content-Type" content="text/html; charset=ISO-8859-1" />
<title>HbbTV Protector</title>
<script type="text/javascript" src="hbbtvprotector.js"></script>

<style type="text/css">
body {
    background-color: transparent;
    color: white;
    font-size: 24px;
    height: 720px;
    margin: 0;
    padding: 0;
    width: 1280px;
}
</style>
```

```
21  </head>
22  <body>

24  <div style="visibility: hidden; height: 0; width: 0; position: absolute;">
25    <object type="application/oipfApplicationManager" id="oipfAppMan"></object>
26  </div>
27    <div style="background-color:#FF0000; float:right;margin:10px;padding:10px;background-image:url('green.
          png');background-repeat:no-repeat;padding-left:75px;background-position: 15px 35px">
28      HbbTV is trying to connect to a server in the Internet. <br /> To allow this activity press the GREEN
            button.<br />
29      This message is shown for 10 seconds.
30    </div>

32    <script type="text/javascript">init();</script>
33  </body>
34  </html>
```

HTML file: de_overview.hbbtv

```
1   <?xml version="1.0" encoding="utf-8" ?>
2   <!DOCTYPE html PUBLIC "-//W3C//DTD XHTML 1.0 Transitional//EN" "http://www.w3.org/TR/xhtml1/DTD/xhtml1-
        loose.dtd">
3   <html xmlns="http://www.w3.org/1999/xhtml">
4   <head>
5   <meta http-equiv="Content-Type" content="text/html; charset=ISO-8859-1" />
6   <title>HbbTV Protector</title>
7   <script type="text/javascript" src="hbbtvprotector.js"></script>

9   <style type="text/css">
10  body {
11      background-color: transparent;
12      color: white;
13      font-size: 24px;
14      height: 720px;
15      margin: 0;
16      padding: 0;
17      width: 1280px;
18  }
19  </style>

21  </head>
22  <body>

24  <div style="visibility: hidden; height: 0; width: 0; position: absolute;">
25    <object type="application/oipfApplicationManager" id="oipfAppMan"></object>
26  </div>
27    <div style="background-color:#FF0000; float:right;margin:10px;padding:10px;background-image:url('green.
          png');background-repeat:no-repeat;padding-left:75px;background-position: 15px 35px">
28      HbbTV versucht gerade Daten aus dem Internet zu laden. <br /> Um diese Aktivit&aauml;t zu erlauben,
            dr&uuml;cken Sie auf den gr&uuml;nen Button.<br />
29      Diese Nachricht wird Ihnen f&uuml;r 10 Sekunden angezeigt.
30    </div>

32    <script type="text/javascript">init();</script>
33  </body>
34  </html>
```

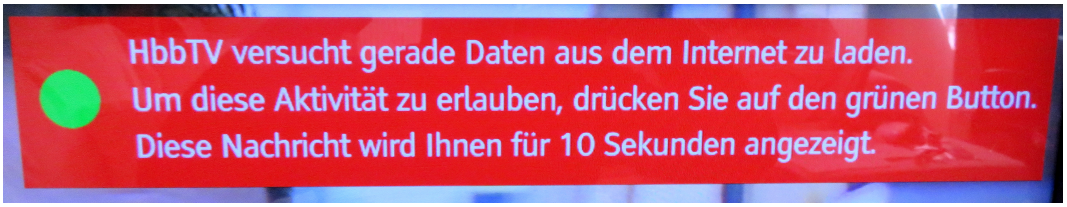


Figure G.1.: *HbbTV Privacy Protector* notification for consumers on the Smart TV (in German).

JavaScript file: hbbtvprotector.js

```
var protector = null;
var keyset = null;
var GREEN_BUTTON=KeyEvent.VK_GREEN  || 404;

function init() {
// May be only working with HbbTV 1.1.1
  try {
    protector = document.getElementById("oipfAppMan").getOwnerApplication(document);
    keyset = protector.privateData.keyset;
    document.addEventListener("keypress", function(event) { handleButton(event); }, false);
    show(true);
  } catch (e) { protector = null; keyset=null; }
}

function handleButton (e) {
  if (e.keyCode == GREEN_BUTTON)
  { show(false); document.location.href = 'http://1.2.3.4/do-not-intercept'; }
}

function show(f) {
try {
    if (f)
      { protector.show(); window.setTimeout("show(false)", 10000);}
    else
      protector.hide();
    keyset.setValue(keyset.GREEN + keyset.RED);
    return true;
  } catch (e) { return false; }
}
```

H Wissenschaftlicher Werdegang

Juni 2011 — März 2017
Promotion im Fachgebiet Sicherheit in der Informationstechnik im Fachbereich Informatik der Technischen Universität Darmstadt unter Leitung von Prof. Dr. Michael Waidner

Juli 2007 — April 2009
Masterstudium der Informatik an der Technischen Universität Darmstadt

Oktober 2004 — Juli 2007
Bachelorstudium der Informatik an der Technischen Unversität Darmstadt