Integrating E-Commerce and Social Engineering Perspectives on Trust in Online Communication

Thomas Pfeiffer
Center of Advanced Security Research Darmstadt
Petersenstr. 30
64287 Darmstadt, Germany
thomas.pfeiffer@cased.de

Michaela Kauer
Technische Universität Darmstadt
Petersenstr. 30
64287 Darmstadt, Germany
kauer@iad.tu-darmstadt.de

Ralph Bruder
Technische Universität Darmstadt
Petersenstr. 30
64287 Darmstadt, Germany
bruder@iad.tu-darmstadt.de

Abstract
Currently, interpersonal trust in computer-mediated communication is a research topic for e-commerce as well as usable security researchers. While the e-commerce researchers focus on gaining warranted trust, usable security researchers focus on preventing misplaced trust, in order to protect users from social engineering attacks. In this paper an approach to integrate findings and theories from both fields is proposed in order to create a complete model for predicting trust in electronic messages or websites, whether they are authentic or not.

Author Keywords
Trust; decision-making; e-commerce; usable security; social engineering; phishing; email

ACM Classification Keywords
H.1.2. [User/Machine Systems]: Software psychology, Human information processing

General Terms
Theory; Human Factors

Social engineering, "[…] the art of gaining access to buildings, systems or data by exploiting human psychology, rather than by breaking in or using technical hacking techniques." [16]

Phishing, "act of sending e-mail that purports to be from a reputable source, such as the recipient's bank or credit card provider, and that seeks to acquire personal or financial information. The name derives from the idea of 'fishing' for information. " [17]

Trust (e-commerce), "a multi-dimensional construct with two inter-related components—*trusting beliefs* (perceptions of the competence, benevolence, and integrity of the vendor), and *trusting intentions*—willingness to depend (that is, a decision to make oneself vulnerable to the vendor)." [7]

Online trust problems (usable security), "those that arise when dichotomies between signals and underlying states can affect the user's decisions and well-being, and when attackers can affect signals, states, and decision processes." [10]

Introduction

Trust plays an important role in digital environments. We have identified three different kinds of trust relevant in digital environments, each with a different pair of trustor and trustee: **Trust networks** [6] attempt to model interpersonal trust, with both trustor and trustee being nodes in a network. There, a trustor assigns a numerical value of trust to a trustee. This trust is then propagated across the network and used autonomously by a computer system e.g. to make recommendations to users. Those users however will only trust these recommendations if they **trust the system** (the second important kind of trust) producing them, believing that its algorithms are correct and not susceptible to manipulation. This paper focuses on a third kind of trust: **Interpersonal or organizational trust in computer-mediated communication**, a person's trust in another person or organization based on electronic messages. This topic is currently being investigated mainly by researchers from two disciplines: E-commerce and usable security.

We will give an introduction to the research on the subject from both fields in the next chapter, before outlining an approach to combine the research from both fields into an integrated understanding of interpersonal trust in computer-mediated communication. The paper closes with an outlook on future research.

Current Research Perspectives

The E-Commerce perspective

Researchers in the field of E-Commerce have been studying trust in e-commerce websites extensively [1,15]. They focus on trust-inducing aspects of websites, aiming to provide guidelines for creating e-commerce websites that gain visitors' trust. In this case, the trustee is the e-commerce vendor; the trustor is the (potential) customer.

Beldad et al. [1] have grouped the antecedents to trust found in the literature in three categories: customer-based (e.g. propensity to trust), website-based (e.g. design or security assurances) and organization-based (e.g. reputation or familiarity) antecedents.

Several models were proposed for the formation of trust in e-commerce vendors (e.g. [2,12]). They usually differentiate between stages in the process (e.g. Deterrence-based, Knowledge-based and Shared identification-based trust [2] or exploratory vs. commitment stage [12]).

The Social Engineering Perspective

Whereas e-commerce researchers study factors influencing trust with the goal of eliciting *legitimate* trust in commercial websites, researchers in the field of usable security try to find out which aspects of a *fraudulent* online message or website (used for the purpose of phishing [17] or social engineering [16] in general) or of its recipient/user either elicit or prevent *misplaced* trust. This knowledge is then used to more effectively educate or warn users about these fraudulent emails or websites.

Experiments and interviews have shown the effect of aspects like content [3,9,11,14], design [3,9,11,14], third-party seals [11,14], URLs [3,9,14] sender's email address [8,9], brand / reputation [10,11] or presence of security / privacy assurances [11] in emails and websites on either user's likelihood to click links in emails / enter information on websites or their

subjective evaluation of their authenticity. Other studies focusing on attributes of the recipient show that knowledge and experience with internet technology and phishing [4,8], personal traits [4,13] as well as demographic factors [8,13] influence individual susceptibility to phishing attacks.

Generally, social engineering literature usually focuses on users' ability to distinguish fraudulent emails / websites from authentic ones. It is assumed that users click a link in a message or enter sensitive information in a website perceived as authentic whereas they dismiss emails / websites perceived as fraudulent.

However, according to results of previous studies [3,5], users without specific knowledge about social engineering mostly base this distinction on properties which experts dismiss as easily fakeable (such as address, design or brand). This suggests that these "novice" users do not explicitly evaluate potential indicators of forged emails or websites as experts do, but instead apply the same indicators of trust as they do for legitimate emails and websites.

Even though both perspectives are concerned with computer-mediated interpersonal trust, currently not much cooperation between the two fields is evident and we know of no integrated approach which covers both warranted and unwarranted trust.

Integrating the Perspectives

We suggest an approach which integrates results from both the e-commerce and social engineering fields in order to understand the factors that influence trust in online communication, regardless of whether a message or website is legitimate or not.

Following this approach, we use those characteristics of the message or website (e.g. language, content, design), the sender (e.g. familiarity, reputation) and the receiver (e.g. knowledge, personality, demographics) which were found to be relevant by either of the fields to predict users' trust in an online message or website. Specifically, we are creating a model to predict a user's decision to follow or dismiss a request (such as clicking a link, providing data or opening an attachment) presented in an electronic message. A preliminary version of that model will be presented at this workshop.

The results from research following this approach will in return expand both the body of empirical evidence and the theoretical background for both fields, as each field can make use of the other field's results and theoretical considerations.

Integrating the results from both fields is possible since they actually study the same thing: Factors influencing user's trust in communication received online. Factors influencing trust which were found in experiments or interviews in social engineering studies can therefore be integrated into the trust models created and validated by e-commerce researchers in order to create a comprehensive model which predicts trust in both legitimate and fraudulent messages / websites.

Outlook

In the next step, our model will be validated empirically to test the assumption that results from both fields can be integrated in one overall model and the model will be refined according to the evaluation's results.

References

[1] Beldad, A., de Jong, M., and Steehouder, M. How shall I trust the faceless and the intangible? A literature review on the antecedents of online trust. *Computers in Human Behavior 26*, 5 (2010), 857–869.

[2] Corritore, C.L., Kracher, B., and Wiedenbeck, S. On-line trust: concepts, evolving themes, a model. *International Journal of Human-Computer Studies 58*, 6 (2003), 737–758.

[3] Dhamija, R., Tygar, J.D., and Hearst, M. Why phishing works. *Proceedings of the SIGCHI conference on Human Factors in computing systems*, ACM (2006), 581–590.

[4] Downs, J.S., Holbrook, M., and Cranor, L.F. Behavioral response to phishing risk. *Proceedings of the anti-phishing working groups 2nd annual eCrime researchers summit*, ACM (2007), 37–44.

[5] Downs, J.S., Holbrook, M.B., and Cranor, L.F. Decision strategies and susceptibility to phishing. *Proceedings of the second symposium on Usable privacy and security*, ACM (2006), 79–90.

[6] Guha, R., Kumar, R., Raghavan, P., and Tomkins, A. Propagation of trust and distrust. *Proceedings of the 13th international conference on World Wide Web*, ACM (2004), 403–412.

[7] Harrison McKnight, D., Choudhury, V., and Kacmar, C. The impact of initial consumer trust on intentions to transact with a web site: a trust building model. *The Journal of Strategic Information Systems 11*, 3–4 (2002), 297–323.

[8] Jagatic, T.N., Johnson, N.A., Jakobsson, M., and Menczer, F. Social phishing. *Commun. ACM 50*, 10 (2007), 94–100.

[9] Karakasiliotis, A., Furnell, S., and Papadaki, M. Assessing end-user awareness of social engineering and phishing. *Information Warfare and Security Conference*, (2006), 60–72.

[10] Kumaraguru, P., Acquisti, A., and Cranor, L.F. Trust modelling for online transactions: a phishing scenario. *Proceedings of the 2006 International Conference on Privacy, Security and Trust: Bridge the Gap Between PST Technologies and Business Services*, ACM (2006), 11:1–11:9.

[11] Lin, E., Greenberg, S., Trotter, E., Ma, D., and Aycock, J. Does domain highlighting help people identify phishing sites? ACM (2011), 2075–2084.

[12] McKnight, D.H., Choudhury, V., and Kacmar, C. Trust in e-commerce vendors: a two-stage model. *Proceedings of the twenty first international conference on Information systems*, Association for Information Systems (2000), 532–536.

[13] Sheng, S., Holbrook, M., Kumaraguru, P., Cranor, L.F., and Downs, J. Who falls for phish?: a demographic analysis of phishing susceptibility and effectiveness of interventions. *Proceedings of the 28th international conference on Human factors in computing systems*, ACM (2010), 373–382.

[14] Tsow, A. and Jakobsson, M. Deceit and Deception: A Large User Study of Phishing. *Indiana University. Retrieved September 9*, (2007), 2007.

[15] Urban, G.L., Amyx, C., and Lorenzon, A. Online Trust: State of the Art, New Frontiers, and Research Potential. *Journal of Interactive Marketing 23*, 2 (2009), 179–190.

[16] Social Engineering: The Basics. *CSO*, 2010. http://www.csoonline.com/article/514063/social-engineering-the-basics.

[17] phishing (computing) -- Britannica Online Encyclopedia. http://www.britannica.com/EBchecked/topic/1017431/phishing.