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

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
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:

1. **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:

2. **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.

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


