How HCI Design Influences Web Security Decisions

Kenneth Radke **Colin Boyd** **Margot Brereton** **Juan Gonzalez Nieto**
Queensland University of Technology
Brisbane, QLD 4001
k.radke, c.boyd, m.brereton and j.gonzaleznieto@qut.edu.au

ABSTRACT
Even though security protocols are designed to make computer communication secure, it is widely known that there is potential for security breakdowns at the human-machine interface. This paper reports on a diary study conducted in order to investigate what people identify as security decisions that they make while using the web. The study aimed to uncover how security is perceived in the individual's context of use. From this data, themes were drawn, with a focus on addressing security goals such as confidentiality and authentication. This study is the first study investigating users' web usage focusing on their self-documented perceptions of security and the security choices they made in their own environment.

Author Keywords
Online, retail, trust, security, diary study, phishing, design, HCI, participation.

ACM Classification Keywords
H5.3. Information interfaces and presentation

INTRODUCTION

The human-machine interface is acknowledged as one of the primary challenges in designing secure human-computer security systems (Patrick, Long and Flinn, 2003). Cryptographers create security protocols which are considered theoretically (mathematically) unbreakable, and yet when used by humans in reality, the protocols do not provide the security level that the theory promised. The combination of (potentially multiple) cryptographic protocols, the various systems which the humans use to interact with the protocols, and the human users themselves, may be described as a "security ceremony" (Ellison, 2007).

Our analysis of security ceremonies known to be broken (Ellison, 2007; Murdoch et al, 2010), has revealed that one source of security flaws may be attributed to the designers of the systems and software.

From the human perspective, with respect to web usage, we do not have a good understanding of how people make security decisions. Our research program therefore aims to examine the security system in its entirety from both the human perspective in the context of use, the interaction design perspective and the perspective of security protocols.

OZCHI 2010, November 22-26, 2010, Brisbane, Australia.

OZCHI 2010 Proceedings ISBN: 978-1-4503-0502-0

In this study we examine people's security decisions made in the context of using the web. Understanding such decision making processes aims to improve future designs of interfaces so that they better protect people's security.

Specification

The central figure in Human-Computer Interaction (HCI) is "the user" (Satchell and Dourish, 2009). Specifically, we have investigated users' web usage. Whether they are aware of it or not, when using the web, users make many security related decisions. However, little research has been done to understand the range of security decisions.

The three questions investigated in this study were:

1. What do web users perceive to be security decisions?
2. Having recognised a security decision is required, on what do users base their security decisions?
3. What was the final decision made?

Our exploratory study used a qualitative approach to investigate users' web usage in their natural environment. The approach we settled on was to ask our 12 participants to keep a log/diary of the security decisions made in their web usage for one week. From this data we have distilled common themes about users' security decisions concerning web usage.

BACKGROUND AND RELATED WORK

First we will discuss the related work, and then give some background into three topics used for the rest of the paper: security; trust; and extended validation certificates.

Related Work

Our work is focused on mainly design aspects of security of online programs and entities, particularly web browsers and websites. As such our work may be seen as similar to the empirical work of Patil and Lai (2005), who investigated the privacy settings of MySpace users. Lampe, Ellison and Steinfield (2006), in their study of 1085 Facebook users which explored users' expectations of privacy, found that 90% of participants believed that no one from outside their university would read their Facebook page, and that 97% of participants believed that no law enforcement agency would look at their Facebook page. Sasse et al (2001) argue that existing HCI techniques are sufficient to address security issues in the design of systems. While this may be true, we will argue that it is necessary to understand the security requirements and tools available, prior to employing standard HCI techniques.

Various studies concerning trust on the internet, such as Lee et al (2000), have been conducted using surveys.

Schechter et al (2007) created a study in which bank websites were progressively changed, to become less and less secure, and the researchers determined whether the participants entered their password each time. In a departure from the survey method in which researchers frame the questions and the context of use is generalised, we have chosen to use a diary study so that participants identify what they perceive to be security questions in their own contexts of use.

Security

In all communications with study participants, the term *security* was used, with no further delineation provided. The main commonly accepted goals of security, as we will use the term, are defined (ISO/IEC 27001):

Confidentiality The goal of confidentiality is to ensure that no communication between the parties may be overheard by a third party.

Authentication The goal of authentication is to ensure that the parties involved are who they claim to be. There is one way authentication, for example where a user proves to an online bank that they are a specific account holder at the bank; and mutual authentication where the website also proves to the user that they are the bank.

Integrity The goal of integrity is to ensure that the message that leaves one party for another party, cannot be manipulated in some way before being received by the target party.

Non-repudiation The goal of non-repudiation is to ensure that parties cannot deny sending information that they have committed to. A similar real world concept is a signature on a legal document, where the signatory should not be able to deny signing the document.

Availability The goal of availability is to ensure that a system is available for use. An example decision is, "What will happen after three failed login attempts?"

Trust

Literature from the past fifteen years is replete with papers concerning trust on the web. These may be broken down into what makes users trust a website, the role of trust in customer loyalty, and how to address the issues of trust across cultural boundaries, which the reality of a "world wide" web necessitates.

Attempts to establish trust with the user the first time they visit a website are usually targeted at a range of triggers upon which users have been "trained" to base their decision to proceed. These triggers include listing measures taken to ensure data is transferred, processed and stored securely, and displaying seals of independent trusted third party auditors (Egger, 2001).

HTTPS and Extended Validation Certificates

Most people have used websites with an address starting with "HTTPS", which should mean that a secure connection has occurred between the web browser and the web site being viewed, accomplishing the security goal of *confidentiality*. Designers should be aware that not just the currently viewed page, but also the page targeted by the form on the currently viewed page, need to use HTTPS for the data to be transferred privately. This means that simply looking for HTTPS on the current page is not sufficient.

Note that there is nothing in HTTPS which states who the other party is. All the user can be assured of is that they are securely connected to *someone*, and unfortunately that someone may not be the entity that the user hoped they would be connected to (Ellison 2007). To help combat this, to gain some measure of *authentication*, Extended Validation Certificates have been introduced.

The process of acquiring an extended validation certificate enforces that the holder of a certificate, required for HTTPS communication, is who they claim to be (http://www.cabforum.org/). This allows web browsers to display the name of the company who owns the website, in addition to the company's web address.

METHODOLOGY

Twelve participants were recruited to log their security decisions for a week. All participants were tertiary qualified. Six of the participants recruited were researchers in the area of computer security, and six were not. Of the security researchers, 33% were female and 66% were male; whereas the participants who were not security researchers were 66% female and 33% male.

Every attempt was made to leave the participants in their natural setting, and to allow the participants to continue to utilise the web as they would normally. Potential participants were asked, via group email and in person, to keep a one week log of their security decisions made while using the web. A template for the log file was provided to each participant. The template, a Microsoft Word document, consisted of a table with three columns. The columns were titled: "Screen image (of the web page)"; "Thoughts about the security decision"; and "Your security decision".

In the template, above the table, were detailed instructions concerning how to take a screen image for Microsoft Windows and for Mac OS users, and how to insert the image into the document.

Also in the instructions were words describing what the second and third column should contain. Specifically, the column titled "Thoughts about the security decision" was to contain what information was available to the participant, and what extra information they felt they needed to make an informed decision. Finally, the third column contained the decision the user made.

This methodology provided us with rich information, typically 3-7 security decision entries per participant, about how each individual uses the web in their normal environment. We then analysed the collected data, drawing common themes from the responses.

FINDINGS

A number of themes could be found in the responses provided by the participants. Quotes in the findings below are as written by participants. As English is a second language for some participants, the authors' interpretation

is added (in brackets) for clarification.

1. Prior use as a security indictor: A very common theme was that participants based their security decision on having used the website in question previously. As one participant stated "This is one of the websites I frequently visit. I have been using this for many years. I did not have any problem with this". Similarly, "I unblocked this pop-up many times before without any consequences". Knowledge from previous use even allowed users to overlook specific security warnings: "…Firefox browser warned me about un-trusted connection; however, I know the website and I can trust it." Lack of previous use was a reason for caution, and in some cases avoidance: "I do not proceed to the website because I do not know about this website and I found it using Google Search" (having clicked the link and received a security warning).

2 Checking for security indicators: When deciding if a website was secure, the most common method was to check that the web address started with "HTTPS" and that there was a padlock present. Participants noted "The web page address contains the HTTPS and the lock sign". Further, participants stated "not HTTPS" for websites lacking this attribute.

3. Lack of knowledge of security indicators: Further to Finding 2, not one participant mentioned even one point, be it name of organisation or colour coding (depending on browser), regarding extended validation certificates.

4. Perception of reputation as a security indicator: Perceptions of security, and security choices made, were strongly based on the company's reputation. Some participants stated the only information that they based their decision of whether or not to proceed on, was their trust in the company that they thought they were dealing with. A typical quote was, "Believe in <name withheld for review> reputation, thus believe (in) online security".

5: Opaque website designs: Participants found various websites where they could not tell if the website was secure, even when explicitly looking for security indications. Websites, for example some banks, used techniques that embed webpages inside other webpages (e.g. using iframes). This ensures that even people very knowledgeable about computers and how HTTPS works, could not be sure if their communication was secure. Some participants went to the extent of viewing the source code for the page to see if the embedded form was secure. Others simply felt they had no knowledge or basis to judge as they did not know what could be falsified easily and what could not.

6: Unrecognisable website addresses: Participants found that they had no way of deciding if a website was who they claimed to be, when the website used their IP address (eg a number such as 66.102.11.104 as the web address, instead of www.google.com as the web address).

7: Mixed secure and insecure items on a web page: Participants noted that security warnings such as "You have requested an encrypted page that contains some unencrypted information" (very common) had little point. Further, they stated that what was secure and what was not secure was in no way defined and hence could not be used to make a decision. A response to this was "I thought (that it is) worthless to make HTTPS page if such a security warning appears as now I more conscious about sharing my personal information". More significantly, some pages were found to be HTTPS pages with forms on them, but the forms targeted http webpages.

8. Unintelligible security warnings: In many cases, security warnings were unintelligible or were misinterpreted by lay users.

DISCUSSION

A key part of this research was gaining from the participants what they regarded as a security decision. The method of acquiring the information, a diary rather than a questionnaire, meant that one person's interpretation of what "security" meant, and therefore what a "security decision" was, could be quite different from the next person's security definition and security decisions. For example, four of the participants logged only decisions related to money, and all but one participant had security decisions related to accessing and paying money.

One of the most consistent themes throughout the participants' responses was that past usage of websites is a key input to decision making (Finding 1). Previous use, and lack of immediately perceived issues, became a form of validation that the website was secure, and that communicating with the website was secure. This is not a strong foundation to build a security decision on, for two main reasons. Firstly, there is a lack of awareness of the changing list of computers on the path between the user and the target website. If an eavesdropping attack occurs, it is likely to come from a computer on the ever changing path. Also, just because a web site was OK yesterday does not mean it will not have been hacked into overnight without any visible difference to the site itself.

Secondly, particularly on social networking sites, having provided personal information over unsecured channels in the past without immediate ramification does not mean that it is a safe practice. It is possible for a third party attacker to collect such personal information in order to mount an attack sometime in the future.

The only actual security indicator used when making a security decision was that users looked for "HTTPS" and a padlock symbol when connecting to a website on which they would like their information and communication protected (Finding 3). This shows that users have been educated to this practice, probably due to the long period in which HTTPS has existed (since 1994) (Walls, 2006).

However, there appears to be little or no education about what HTTPS actually does for the user. Most participants indicated that they regarded HTTPS as a "silver bullet", that the presence of HTTPS meant that the site could be trusted and was secure. To talk in terms of the security goals defined in the earlier Background section, the only security goals that HTTPS provides are confidentiality and integrity. There is no authentication, i.e. the other

party may not be who they claim to be.

Finding 3 highlights that not one participant mentioned looking for extended validation certificate information in making their security decisions while using the web. This emphasises that while the public are aware of HTTPS, education is lacking concerning extended certificates, and that there is an opportunity to improve interaction design of warnings and certificates.

The most significant observation that can be made when reading design papers on trust is that most, if not all, of the suggestions and observations on how to get a user to trust a website are based on ideas other than any of the reasons a user *should* trust a website. For example, providing items such as "company details" and "prominent links to the privacy policy" (Egger, 2001) are listed as guidance on how to get a user to trust a website (Koehn, 2003). However these items are easily utilised and copied by adversaries. Since such guidance is not based on any underlying security protocol, it could read as a "how to design a fraudulent website" guide.

Findings 5, 6, 7 and 8 all relate to design choices, which impact the user's ability to make good security decisions.

CONCLUSION

The findings of the research showed that, based on self-reported security decisions made in their own context of use, by far the biggest, and in some cases "only", item of tangible security that users based their security decisions on, was whether or not the website's address was HTTPS, and whether there was a padlock symbol in the web browser. Conversely, the research showed that the concepts of extended validation certificates have not permeated into the general public.

After this, the main factor that participants based their security decision on was the reputation of the company whose website they thought they were browsing. While company reputation is an important factor, security decisions should not be based upon reputation prior to authenticating that company is who they claim to be. Further, when private transactions are being made with the company, the channel of communication should have the confidentiality property (ie HTTPS).

Designers need to be aware of the security goals, and design their browsers and websites with these security goals in mind. Designs should highlight, rather than hide, the key information that users need to make informed security decisions. This will involve the designers either acquiring the knowledge of security fundamentals themselves, or liaising with security professionals.

Extended validation certificates remain the best way to authenticate to the user that they are dealing with a specific company, and communicating with them securely. Web browsers need to be adapted to more clearly indicate, and educate, users on the significance of the extended validation certificate information.

Finally, the method used of participants keeping a diary of their security decisions for a week, yielded very rich results about self reported security decisions made in the participants context of use. Commonality across all participants was found regarding firstly, looking for HTTPS, secondly, that not one participant listed any extended validation certificate information in their decision process, and finally, how the company's reputation was a significant factor for many. That said, each participant was different and this yielded other very useful information, such as that using IP addresses, iframes, or mixed secure and non-secure content, obstructed the security decision making process.

ACKNOWLEDGEMENTS

We are indebted to the participants in our study. Also, we appreciated the reviewers' comments.

REFERENCES

Egger, F.N. Affective design of e-commerce user interfaces: How to maximise perceived trustworthiness, Proc. Intl. Conf. Affective Human Factors Design, Citeseer (2001)

Ellison, C. Ceremony design and analysis, Cryptology ePrint Archive, Report 2007/399, 2007. http://eprint.iacr.org/

ISO/IEC 27001 Information technology - Security techniques - Information security management systems - Requirements (2005)

Koehn, D. The nature of and conditions for online trust, J. Business Ethics, vol 43, no.1,3-19,Springer (2003)

Lampe, C., Ellison, N., and Steinfield, C.A Face (book) in the crowd: Social searching vs. social browsing, Proceedings of the 2006 20th anniversary conference on Computer supported cooperative work, ACM (2006)

Lee, J., and Kim, J., and Moon, J.Y. What makes Internet users visit cyber stores again? Key design factors for customer loyalty, SIGCHI, ACM (2000)

Murdoch, S.J., Drimer, S., Anderson, R., and Bond, M. Chip and PIN is Broken, IEEE Symposium on Security and Privacy (2010)

Patil, S., and Lai, J. Who gets to know what when: configuring privacy permissions in an awareness application, ACM SIGCHI (2005)

Patrick, A., Long, A.C., and Flinn, S. HCI and Security Systems. HCISEC Workshop, ACM CHI (2003). http://www.andrewpatrick.ca/CHI2003/HCISEC/patrick-HCISEC-proposal.pdf

Sasse, M.A., Brostoff, S. and Weirich, D. Transforming the 'weakest link'- a human/computer interaction approach to usable and effective security, BT Tech Journal, vol 19, no. 3, 122-131 Springer (2001)

Satchell, C., and Dourish, P. Beyond the User: Use and Non-Use in HCI, OZCHI (2009)

Schechter, S.E., Dhamija, R., Ozment, A., and Fischer, I. The Emperor's New Security Indicators: An evaluation of website authentication and the effect of role playing on usability studies, Proceedings of the 2007 IEEE Symposium on Security and Privacy, Citeseer (2007)

Walls, C. Embedded software: the works, Newnes (2006)