Issues in User Authentication[1]

Sonia Chiasson
Carleton University
Ottawa, Ontario, CANADA
chiasson@scs.carleton.ca

Robert Biddle
Carleton University
Ottawa, Ontario, CANADA
Robert_Biddle@carleton.ca

ABSTRACT
In this brief paper we outline our recent work on usability studies of user authentication systems. In particular, we have conducted studies on password managers and graphical password systems, using in-lab experiments, interviews, and broader field studies. We then discuss some of the important issues arising, including mental models of security, the role of persuasion, and the nature of identify theft.

Author Keywords
Usable security, usability, security, authentication

ACM Classification Keywords
H.1.2 User/Machine Systems, Human Factors, Security

INTRODUCTION
The idea of having to identify oneself before being allowed to perform certain actions is quite acceptable, and expected, in today's society. People understand that this is a required step in the process of maintaining a secure environment and generally accept it. Regardless of this understanding and acceptance, however, authenticating users in a computer environment both unobtrusively and securely remains problematic.

Our work focuses on the problem of user authentication, and we have conducted several user studies examining different aspects of this issue. In this paper we describe how we have successfully tested these different aspects, where we ran into problems, and some of the overarching issues we feel remain to be addressed in user authentication.

BACKGROUND
Even though their shortcomings are well-known, standard alphanumeric passwords remain the most common method of user authentication in place today. The "password problem" stems from the fact that users are required to have an ever-increasing number of passwords, each with different requirements (i.e. "must contain a number", "must be 8 characters long", "must be changed every 3 months"), making it unwieldy for even the most security-conscious person to remember them all. In an effort to cope, users resort to unsafe practices. They select easy-to-guess passwords, they re-use passwords across different accounts, and they write them down. Not only do users have to remember all of these passwords, but they must also accurately determine where and when to enter them which is an increasingly difficult task. Besides being a usability nightmare, the current state of user authentication allows for compromises in security, namely in the form of identity theft. If attackers can either guess passwords or trick the user into revealing them, then they can assume the legitimate user's identity.

Recent work in user authentication has focused on designing alternatives to text-based passwords, on designing interfaces to help users manage passwords, and on helping users identify when it is safe to enter a given password. While progress is being made, many open problems linger.

USER STUDIES
In the last year and a half, we have conducted several user studies in the area of user authentication. We briefly present each of these studies to provide context in which to discuss issues we believe remain to be addressed.

Password Managers
Password managers are intended to reduce the burden on users by requiring them to remember only one "master" password to activate the system. Once activated, the

[1] Version: March 8, 2007

CHI 2007 Workshop: Security user studies: methodologies and best practices, April 2007.

password manager generates and enters strong passwords for each of the users' accounts as needed. Ideally, this increases both usability and security since users are now responsible for only one password and each user account is protected by a stronger password than would normally be selected.

We conducted an independent, in-lab user study of two such password managers positioned as usable and beneficial to users [3][6]. We uncovered that both had major usability problems which led users to make dangerous errors that put their passwords at risk [1].

In this user study, we gave 26 participants typical tasks that would need to be accomplished with these programs such as logging on to a website and changing a password. One difficulty was maintaining ecological validity – how to ask participants to perform the tasks and provide enough information about the programs without guiding them step-by-step through the process since in practice users would not have such guidance. We compromised by giving users a brief verbal introduction and providing them with written instructions about the systems that they could reference as needed throughout the session.

A primary finding was that users' mental model of the password managers, and more broadly of passwords in general, were inaccurate and did not reflect the system models. This caused users to make "dangerous errors" and often left them confused about what had just happened or what to do next.

In an effort to gain further understanding of users' mental model of authentication and passwords, we conducted interviews with a small number of users. Combining this information with the comments provided by users during the in-lab studies, we saw that users have a very limited mental model of authentication. In their view, they enter a password, the computer does "magic computer stuff" and they are given access to their account. They also have misconceptions of what constitutes a "good" password, believing that attackers would be unable to guess their dog's name, favorite flower, or a word from a language other than English. In their view, an attacker would need to know them personally in order to know this information.

One of the problems that arise from trying to get a sense of users' mental models is that the very act of asking them about their understanding can change their mental model. For example, many times it was obvious that users had never considered these questions before and as such were struggling to form a mental model "on-the-fly". Their response may reflect what they had just deduced, but it did not reflect what they previously had in mind when interacting with the system.

Graphical Passwords

Due to the problems with alphanumeric passwords, many alternative authentication methods are being investigated. By creating passwords based on images, one set of alternatives capitalize on the fact that humans have better memory for pictures than text [5]. Several schemes have been proposed, including drawing a sketch using a grid, recognizing correct images from within a larger pool, and clicking on points within an image [4].

Our studies examined PassPoints, a graphical password system designed by Wiedenbeck et al [7] where a user's password is a sequence of mouse clicks on particular points within a given image. We conducted both an in-lab study and a longer field study where the system was deployed in practice.

With the in-lab study, we observed 43 participants as they created graphical passwords on 17 different images. For each image, users created a password, confirmed it by re-entering it, performed a distraction task which tested their spatial ability, and then attempted to log in again. Besides usability information on different types of images and measures of accuracy and time in password entry, we can use the collected passwords to see what points become "hot spots" (frequently selected areas) and which types of images are more prone to such hot spots. We can also perform a security analysis to determine the "guessability" of passwords.

We then selected two of these images for use in the long-term study. Approximately 376 students used graphical passwords to access their class notes over a period of two months. This provided real-world usage data, showing how usable these systems are in practice as well as comparison data to see if the results of our in-lab study reflect realistic usage.

Based on early results, we developed an alternative graphical password scheme that addresses some of the usability and security concerns of PassPoints. We are currently finishing an in-lab 25 user study of this new prototype which shows promising results.

ISSUES RAISED BY OUR STUDIES

Over the course of conducting these studies, we began to see that some issues are prevalent across the area of user authentication and perhaps more broadly throughout usable security. We believe that these overarching issues need to be investigated and addressed in order to progress towards our goal of truly usable security.

Mental Models

When reading usable security literature, and within our own studies, we find that discussion invariably turns to the problem of mental models. User interfaces for security fall short of fostering useful mental models for users. One frequently cited explanation is that security is a complex issue and that users need more education in the area. We disagree with this argument. Not only is it shortsighted to assume that users will be adequately trained, but it is unrealistic to place such a burden on users.

The user interface should convey the information necessary for users to be able to easily predict and understand the consequences of their actions. This does not mean that users need to know the intricate details of how the system operates, but that they can form a reliable explanation in their minds that lets them interact successfully. The file managing metaphor is a good example – users understand that files can be placed in folders, opened, closed, thrown into the recycle bin, and so on. But at no point do users need to know the underlying details of file storage and manipulation, such as disk blocks, index tables, and disk head scheduling.

Security interfaces do not yet help users form such mental models and still assume that users will have an understanding of underlying security concepts. This places users in a vulnerable position. They lack the necessary knowledge, they must rely on inadequate interfaces to deduce what is happening, and they must make decisions that could potentially place them at risk. A wrong decision can give attackers valuable information or leave a user's system vulnerable. Alternatively, a wrong decision can also hinder a user's productivity because the security mechanisms now prohibit desired activities. It is not surprising that users prefer not to deal with security issues if they can avoid them.

Security interfaces must foster useful mental models. As researchers and designers, we must also be careful to accurately identify users' mental models when running usability studies so that we get an accurate and unbiased understanding of the usability of our systems. We acknowledge that these are not easy tasks, but ones that must nevertheless be accomplished to achieve usable security.

Persuasive Technology

When we re-examined the results of our password manager study in hopes of finding ways to improve the user interface, it occurred to us that many of the usability problems could potentially be addressed by "persuasive technology" principles.

Persuasive technology is a fairly new area of HCI that looks at how interfaces can be designed to motivate and influence users to behave in the desired manner [2]. In terms of security, this has two important implications. First, since an often cited problem in security is the "unmotivated user" who bypasses security, any strategies that could convince users to perform the required security tasks is worth investigating. Secondly, it is important to understand how interfaces persuade users for defensive purposes as well since attackers will be using such strategies to lure users into behaving in unsafe manners.

Some of the principles of persuasive technology [2] are a natural fit for password managers. For example, the Principle of Reduction aims to make the desired path one of least resistance. If designers can make using password managers easier than having to deal with multiple passwords, then users will be motivated to employ password managers. The Principle of Tunneling advocates an interface that guides users into performing the desired actions by limiting alternatives. If it is unsafe for users to enter passwords directly into websites, then why is this action allowed?

It is worth noting however that these principles cannot be blindly applied. They need to be carefully studied and potentially modified as to not compromise security. For example, while persuasive technology advocates giving users clear feedback throughout the course of the interaction, in a security interface this may actually leak information to attackers.

The idea of using principles of persuasive technology also alludes to another overarching problem of usable security – there is a lack of any cohesive theoretical framework to describe how to design of usable security interfaces. As with any young discipline, current usable security principles and guidelines tend to be either narrow in application or too general to be of any use to designers. A "framework of usable security" is needed to provide designers with concrete guidelines on how to create truly usable security interfaces.

Identity Theft

One of the reasons for the increasing public concern regarding user authentication is "identity theft", meaning fraudulent access and use of credentials. While thinking of this larger picture, we noticed an interesting asymmetry in the current authentication process. The asymmetry represents a weakness that can lead to identity theft. This weakness is targeted by "phishing", whereby attackers persuade users to enter their credentials at fraudulent sites. Phishing can be seen as forging the credentials of a legitimate site and then using this forgery to lure users into divulging their information. So in some sense, the phisher commits identity theft against the legitimate site, and subsequently uses the forgery to commit identity theft from the user.

The forgery, and consequently the identity theft, is very easy because the legitimate site only authenticates to users through its trademarks and styles. So in essence, the phishers commit trademark infringement. But whereas some fraudsters might commit trademark infringement to get business opportunities from people mistaking them for the trademark holders, phishers plan far worse. The first example is like someone fraudulently calling their hotel a "Holiday Inn" to attract guests; the second example is like then burgling their rooms.

An issue that arises concerns responsibility: it is not only the responsibility of users to defend against identity theft. This is interesting for many reasons, but in particular we wish to point out that it can be the legitimate site's lack of

safeguards against theft of their identity that is instrumental in allowing the phishers to steal the identity of its users.

Computer security has long discussed "mutual authentication", which views authentication as mutual and symmetric process. This means that prior to performing a transaction, each party must determine the authenticity of the other. There are various algorithms for mutual authentication, and these typically require that the parties demonstrate shared knowledge by each providing challenges and responses in several passes. Typical authentication systems in place today provide only one-way authentication, where users authenticate themselves to the system they want to access, but not vice versa. A phisher simply needs to make a site that looks like a bank, then convince users to visit the site and reveal their key. Other than basic visual cues, users have no way of knowing whether they are really interacting with a legitimate second party.

While mutual authentication is clearly desirable in terms of security, the problem is one of usability, and the related issue of user acceptance. We believe that this suggests important obligations and opportunities in addressing these issues. Users must be reliably made aware that they are interacting with a legitimate site in the same way that websites expect users to authenticate themselves.

CONCLUSIONS

In this brief paper we have outlined our recent work on usability studies of user authentication systems. In particular, we have conducted studies on password managers and graphical password systems, using in-lab experiments, interviews, and broader field studies. Though in-lab studies have limitations in terms of ecological validity, we have found them to be a useful first step in identifying usability problems and providing directions in which to improve the interface. These in-lab studies also offer insight into users' mental models because during a session, the experimenter can observe the user's behavior and reactions, record comments, and probe for further details while the interaction is still fresh in the user's mind. In terms of practical security evaluations, longer term studies provide a better indicator since users have a chance to incorporate the behavior into their daily life. Longer term studies are also recommended to confirm the practicality and usability of systems that perform well during in-lab studies since users may behave differently outside of a structured testing environment. This multi-stage evaluation process is often recommended in HCI, but we believe that it is especially important for usable security due to the "security is a secondary task" problem.

Though work in specific areas of usable security is necessary, we believe that the larger issues raised here also need to be addressed. In particular, we have found that the mismatch between user mental models and security systems is a deep issue that must be resolved. We need to address this mismatch, but to do so we also need to develop accurate methods for identifying users' mental models in the first place. Secondly, there is a lack of theoretical frameworks to guide the design of usable security. We believe that principles of persuasive technology may assist in developing such a framework. More practically, persuasive technology may help us in building and supporting user appropriate user behavior. Finally, we believe that the problem of identity theft needs to be examined from a wider perspective; one that removes the burden from users.

REFERENCES

1. Chiasson, S., van Oorschot, P.C., and Biddle, R. *A Usability Study and Critique of Two Password Managers*. Proceedings of the 15th USENIX Security Symposium, Vancouver, BC, August 2006.
2. Fogg, B.J. *Persuasive Technologies: Using Computers to Change What We Think and Do*. Morgan Kaufmann Publishers, San Francisco, CA, 2003.
3. Halderman, J., Waters, B. and Felten, E. *A convenient method for securely managing passwords*. Proc. of the 14th International WWW Conference, 2005.
4. Monrose, F. and M.K. Reiter. *Graphical Passwords.* Chapter 9 in Security and Usability: Designing Secure Systems That People Can Use. L.F. Cranor and S. Garfinkel (eds). O'Reilley, 2005.
5. Nelson, D.L., U.S. Reed, and J.R. Walling. *Picture Superiority Effect*. Journal of Experimental Psychology: Human Learning and Memory 3, pp. 485-497, 1977.
6. Ross, B., et al. *Stronger password authentication using browser extensions.* Proc. of the 14th USENIX Security Symposium, Aug. 2005.
7. Wiedenbeck, S., Birget, J.C., Brodskiy, A., and Memon, N. *Authentication Using Graphical Passwords: Effects of Tolerance and Image Choice*. Symposium on Usable Privacy and Security (SOUPS) 2005, July 6-8, 2005, Pittsburgh, PA, USA.