Usability of Security in Ubiquitous Computing

Joaquin Loustau

October 16, 2014

Abstract

Describe your paper in 100-200 words, give or take. The command-line `wc` utility is really useful here! This particular sample paper is meant to demonstrate a variety of LaTeX directives for producing a well-structured, consistently-formatted scholarly document. The actual content and outline may vary according to the needs of your specific research topic.

Contents

1 Introduction

The International Telecoms Union, the UN agency reported that mobile phones will outnumber people on Earth by the end of 2014. Today, demonstrating the most convincing the value of ubiquitous computing, the cell phone, or more precisely the smart phone, takes center stage crossing a threshold of processor performance, memory/disk capacity, and connectivity both cellular and local, making it the most widely adopted and ubiquitous computer there has ever been.

Smartphones have become an indispensable part of our daily lives. Smartphone penetration in the US has risen to 56

As people become more connected electronically, the ability to achieve a highly accurate automatic personal identification system is substantially more critical (Jain)

This paper aims to...

2 Background, Preliminary, and Related Work

he term ubiquitous computing was coinned by Mark Weiser, chief technology officer at Xeroxs Palo Alto Research Center (PARC) in 1988 to describe a future in which invisible computers, embedded in every day objects, replace PCs. In his ground-breaking article, The Computer for the 21st century, Dr. Weiser expresses the most profound technologies are those that disappear. They weave themselves into the fabric of everyday life until they are indistinguishable from it.

Nowadays, ubiquitious computing, or ubicomp, is the term given to the third era of modern computing. The first era was defined by the mainframe computer, a single large-time shared computer owned by an organization and used by several individuals at the same time. Second, came the era of the PC, a personal computer predominantly owned and used by one individual, and dedicated to them. Finally, the third era, ubiquitous computing, representative of the present time, is characterized of small networked protable computer products, such as smart phones, tablets, and embedded computers built into many of the devices we own -resulting in a world in which each person owns and uses many computers.

The five properties of Ubiquitous Computing. From Rich Gold, The Plenitude Sensuous Reactive Communicative Embedded Socially Colonizing

User authentication is a basic theme in computer security and covers establishing who the user is (identification), verifying this identity (verifaction or authentication), and providing proper access to the resource that the user is allowed to use (authorization).

Mechanisms and policies for increasing security, like frequent change of passwords or requesting a password of a certain length, had the opposite effect because users then made easy-to-remember passwords and wrote them down, thereby lowering security. Hence, security mechanisms incompatible with work practices may be circumvented by users and thereby undermine system security overall.

Adams and Sases investigations also demonstrate that users are certainly motivated to support the security of the system, but often unable to determine the security implications of their actions. Zurko and Simon and later Flechis et al. call for doing user-centered security to create security models, mechanisms, systems, and software that have usability as a primary motivation or goal. Microsoft Passport.net aims at solving the increasing problem of typing in usernames and passwords on numerous web sites by creating a centralized authorization mechanism.

The use of biometric systems is receiving an increasing attention currently. Biometric identification is a common term for using a persons biological traits as a way of identifying him. They are basically eight biometric types that are used in systems at the moment: face geometry, fingerprint, hand geometry, iris patttern, retinal pattern, signature, voice print,

and facial thermogram. Even though it is also being marketed as a new user-friendly user authentification mechanism, there is little research so far into the usability of these systems. Most work and reasearch on biometric systems focus on security and accuracy.

Login using usernames and passwords are designed for, and often used in an office situation, characterized as being individuals working while sitting down at a desk using the same personal computer for a long period of time -typically a whole working day.

The traditional login schema completely disrupts a smooth flow of work in settings characterized by workers being mobile, often interrupted, cooperating and using many different computers during a working day. The design of ubiquitous computer sytems for these kind of working environments needs to accommodate such challenges, rather than unconsciously adopt existing user authentication mechanisms.

Remembering usernames and passwords is just plain difficult even for experienced computer users and typing them in, created a breakdown in the interaction with the computer, forcing the user to focus on the computer instead of his or her task at hand.

Another fundamental aspect of the login concept is that it is personal. This is caused by the security need for traceability -the system should record (log) who is doing what.

The aim is to put special focus on the design and usability of user authentication mechanisms, which is an often overlooked feature of a computer system.

In our design of new user authentication mechanisms, we have put special emphasis on four things: (1) to suppport proximity-based user authentication, where users are logged in by just approaching a display, (2) to support silent login where users can seamlessly alternate between being logged in, (3) supproting migrating user sessions, enabling users to carry with them their work on the move, and (4) to support suspendable user sessions. The use of smartcards can be used as a combined identification and authentication token. However, as a physical token smart cards are subject to be lost or stolen.

The use of biometric systems is an appealing solution to the trouble of typing usernames and passwords. By using biometrics systems people can be identified by something they are instead of something they have (e.g, a smart card) or know (e.g, their password).

A common way of testing a biometric system is to measure the tradeoff between the false-acceptance rate (FAR) (the percentage of imposters incorrectly matched to a valid users biometric) and the false-rejection rate (FRR) (the percentage of incorrectly rejected valid users). This tradeoff is still rather high for most systems, leaving us to choose whether we want a highly secure system, that rejects a lot of valid users, or a more useful system that potentially can allow incorrect access to imposters (see e.g. the test report from the British CESG authorities [16])

User authentication mechanisms in ubiquitous computing. From a usability point of view, we have described how the conventional login procedures caused considerable usability problems. Usability cannot be ignored when addresing computer security. A highly secure system from a technical point of view can be made insecure if the authentication mechanisms are difficult or tedious to use. The result is that users find ways to circumvent and shortcut the security system, which leads to vulnerable systems.

DeAlvare found that once a password is chosen, a user is unlikely to change it until it has been shown to be compromised. Users were also found to construct passwords that contained as few characters as possible. the term user-centered security to refer to security models, mechanisms, systems, and software that have usability as a primary motivation or goal. Secure systems have a particularly rich tradition of indifference to the user, whether the user is a security administrator, a programmer, or an end-user. Gasser reports a similar problem with Unix systems, which support the settinf of default access modes for new files on a per-session basis. As a user's work moves from public to private files, the user is unlikely to remember to restrict their default access mode. A better solution, provided by Multics and VMS, is to tset

the default access modes on a per-directory basis. This example shows that considerations for users' natural working patterns can strengthen the security of the system.

Since user-interface technology is constantly evolving and user needs are so diverse, no particular technology or architecture is always "user friendly." Contextual Design, Discount Usability Testing, In Lab Testing and Contextual Inquiry.

The first security application to articulate a user-centered design philosphy was Privacy-Enhanced Mail (PEM). (Linn) "The set of supported measures offers added value to users, enhancing rather than restricting the set of capabilities available to users." This was a startling vision in the security community that largely perceived security requirements as watching and restricting users. While usability problems with the certificate authority infrastructure kept PEM form being widely deployed, its primary motivation to offer users desirable security services such as privacy for their daily electronic mail remains a laudable goal still unmet today. (User-Centered Securty, Zurko-Simon)

3 Methods

To evaluate the

4 Conclusions

We would, however, argue that the aspects of mobility, cooperation, interruption, and sharing of material are core aspects of much real-world work. (as also demonstrated by numerous studies in the CSCW literature).Such aspects play an increasing role these yars as we are turning to ubiquitous computing with its overall concept of creating computer support that enables the usert to move away from the office with its desktop computer. We cannot avoid addresing the fundamental usability challenges in login and authentication of users, if this vision is to become viable. The paradigm should be the full integration of security and usability concerns into the software development process, thus enabling developers to build secure systems that work in the real world. (Flechais).

The usability of security mechanisms is not just a question of improving interfaces to security tools, but designing security to work with the real-world task users perform, and within the physical and social context of that interaction (18)

AEGIS is a software engineering method for creating secure systems based on security requiements identification through asset[**?**] modelling, risk analysis and context of use. (Flechais)

References

[1] J. Krumm. *Ubiquitous Computing Fundamentals.* Chapman-Hall, CRC Press, 2009.