

# Usability of Security Mechanisms in Ubiquitous Computing Environments

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  $\text{\LaTeX}$  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

<b>1</b>	<b>Introduction</b>	<b>3</b>
<b>2</b>	<b>Background, Preliminary, and Related Work</b>	<b>3</b>
<b>3</b>	<b>Methods</b>	<b>4</b>
<b>4</b>	<b>Discussion</b>	<b>5</b>
<b>5</b>	<b>Conclusions</b>	<b>7</b>

# 1 Introduction

The International Telecommunication Union, a specialized agency of the United Nations (UN) responsible for issues that concern information and communication technologies, reported that the number of mobile-cellular subscriptions will reach almost 7 billion by end 2014, corresponding to a penetration rate of 96% . [9] Today, demonstrating the value of ubiquitous computing (ubicomp), the cell phone, or more precisely the smart phone, takes center stage crossing a threshold of processor performance, memory capacity and connectivity both cell and local, making it the most widely adopted and ubiquitous computer there has ever been.

However, the smartphone is just one of several ubiquitous computing devices we encounter during any given day. The future of ubiquitous computing foresees networked microprocessors embedded in everyday objects: not just smart phones and home appliances but furniture, books, sprinklers, etc. —hundreds of internet-enabled computers communicating to each other over wireless links. As the number of ubiquitous computing devices continues to grow, the sheer amount, nature and complexity of the information exchanged will grow exponentially. If the ubicomp systems deployed in our homes, workplaces and vehicles are as vulnerable as todays personal computers, the implications could be catastrophic. For example, inadequate manipulation of data handled by heart monitors in a clinic or an alarm system for a nuclear power plant could be fatal. The examples are endless. Security is needed to ensure exact and accurate confidentiality, integrity and authentication.

This paper aims to examine the security issues for ubiquitous computing and analyze the usability of the log-in/password mechanism of securing information, along with a brief story of previous works and accomplishments in the corresponding areas.

# 2 Background, Preliminary, and Related Work

The term ubiquitous computing was coined by Mark Weiser, chief technology officer at Xeroxs Palo Alto Research Center (PARC) in 1988 to describe a future in which computers, embedded in everyday objects, replace personal computers (PCs). In his ground-breaking article, “The Computer for the 21st Century,” 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.”[13]

Presently, ubiquitous 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 and present era, ubiquitous computing, is characterized of small networked 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 hundreds of computers a day.

Rich Gold, a member of Dr. Weisers team at PARC, proposed a taxonomy of properties for ubiquitous computing based on Weisers formulations. The properties were: sensuous, reactive, communicative, embedded socially and colonizing.[6]

In addition to ubiquitous computing, the other major topic that this paper will cover is security. Amoroso[2] defines computer security as risk management: assessing threats, vulnerabilities and attacks, estimating costs for the threats, estimating probabilities for the attacks given the vulnerabilities, developing appropriate safeguards (a priori vaccines) and counter-measures (a posteriori remedies), and implementing the ones for which the certain price of the defense is worth spending compared to the uncertain loss that a potential threat implies.

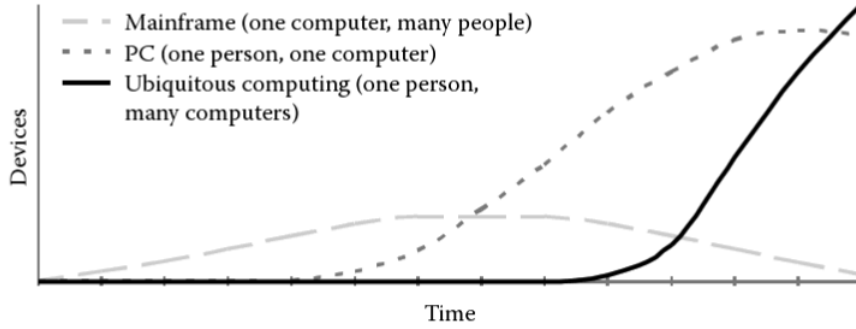


Figure 1: The three eras of computing: Number of devices per person over time.

The required characteristics such secure systems are often summarized in the acronym CIA. This does not refer to the Central Intelligence Agency but is instead a widely used benchmark for evaluation of information systems security, focusing on the three core goals of **confidentiality**, **integrity** and **availability** of information. Confidentiality refers to limiting information access and disclosure to authorized users. Integrity is the property that refers to the trustworthiness of information resources and is violated whenever information is altered in an unauthorized way. Finally, availability is the property of a system which always ensures that information is accessible when needed.

The efforts to mitigate the risks of threats to confidentiality, integrity and availability often take the form of user authentication. User authentication is a basic theme in computer security and covers establishing who the user is (identification), verifying this identity (verification), and providing proper access to the resource that the user is allowed to use (authorization).

Finally, this paper will analyze the usability of a specific authentication mechanism, the traditional log-in/password schema. It would therefore be desirable to define the term usability in this context. The ISO 9241-11 Guidance on Usability, issued by the International Organization for Standardization, defines usability as: The extent to which a product can be used by specified users to achieve specified goals with effectiveness, efficiency and satisfaction in a specified context of use.[8]

### 3 Methods

In order to investigate the topic of Usability of Security Mechanism in Ubiquitous Computing Environments, a top-down approach was employed. Firstly, one performed an exhaustive search of articles, books and journals covering Usability, Security and Ubiquitous Computing as independent concepts. The two main sources chosen for this search were the William H. Hannon Library at Loyola Marymount University and the Association for Computing Machinerys (ACM) Digital Library.

A narrower and more specific search for materials was then conducted, and sources cited in the selected articles were explored, thus unveiling a myriad of different publications. To assess the reliability of these new sources, Google Scholar was a significantly important tool. Google Scholar provides information such the number of times the given article has been cited as well as the sources of these citations. Articles that have been cited time and again and have been

published or cited by prestigious scientific journals are most likely to be reliable.

Organizations such as the Association for Computing Machinery (ACM) or the Institute of Electrical and Electronics Engineers (IEEE) are known for their academic rigor, and consequently provide an almost certain guaranty of the credibility and authority of the pieces appearing in their publications.

## 4 Discussion

While there is extensive bibliography on different strategies to secure information systems, the significantly smaller number of sources available on usability of security mechanisms sheds lights on the fact that the design and usability of user authentication mechanisms is an often overlooked feature of computer systems. As people become more connected electronically, the ability to achieve a highly accurate and user-friendly automatic personal identification system is substantially more critical. [10] 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. The most common and widespread security mechanism is the log-in/password schema. This approach is most suitable for office situations, where individuals work on a single personal computer for a long period of time —generally a whole working day. The usability of using a log-in and password for every ubicomp device does not seem to be clear.

The number of devices that a user will interact with will require multiple usernames and passwords for the user to remember. Remembering usernames and passwords is difficult even for experienced computer users and typing them in, creates a breakdown in the interaction with the computer, forcing the user to focus on the device rather than on his or her task at hand. De Alvare and Schultz [4] discovered that once a password is chosen, a user is unlikely to change it until he/she is aware that it has been compromised. Furthermore, to make memorization easier, users also tend to construct passwords that contain the least amount of characters as possible.

Similarly, mechanisms and policies for increasing the password strength like frequent change of passwords or requesting a password of a certain length that includes different kinds of symbols, often has the opposite effect as users make easy-to-remember passwords and write them down, thereby lowering security.[1] This shows how a highly secure system from a technical standpoint can be made insecure if the authentication is difficult or tedious to use. The result is that users find ways to circumvent and shortcut the security system, which leads to vulnerable systems.

The two alternatives to the log-in/password method often suggested are tokens and biometrics. A security token (also sometimes called authentication token) is a small hardware device that the owner carries to authorize access to a network service. The device may be in the form of a smart card or may be embedded in a commonly used object such as a key fob.

Security tokens may provide an extra level of assurance through a method known as two factor authentication: the user has a personal identification number (PIN), which authorizes them as the owner of that particular device; the device then displays a number which uniquely identifies the user to the service, allowing them to log in. However, as a physical token, smartcards or other forms of security tokens are subject to be lost or stolen. This consists the most significant disadvantage of authentication tokens.

On the other hand, biometric identifiers exploit certain physiological or behavioral characteristics that are distinctive to each person, and thus are more reliable and more capable than knowledge-based and token-based techniques in differentiating between authorized and unauthorized users. By using biometrics system people can be identified by something they *are* instead of something they *have* (e.g., a smart card) or *know* (e.g., their password and login). An

ideal biometric should be **universal**, where each person possess the characteristics, **unique**, where no two people should share the characteristic; **permanent**, where the characteristic should neither change nor be alterable; and **collectable**, where the characteristic is readily presentable to a sensor and is easily quantifiable.[10] In practice, however, a characteristic that satisfies all these requirements may not always be feasible for a useful biometric system.

There are eight biometric types that are currently being used in systems: face geometry, fingerprint, hand geometry, iris pattern, retinal pattern, signature, voice print, and facial thermogram. Even though it is being ‘marketed’ as a new user-friendly user authentication mechanism, there is little research so far into the usability of these systems. Most work and research on biometric systems focus on security and accuracy.

A traditional way of testing a biometric system is to measure the correlation between the false-acceptance rate (FAR) —the percentage of unauthorized users incorrectly matched to a valid user’s biometric— and the false-rejection rate (FRR) —the percentage of incorrectly rejected valid users. Biometric specialists normally agree that the biometric rates of FAR and FRR are the equivalent of the password space in PIN/Password based authentication.[7] Biometrics do not provide perfect (unique) identification. The matching process is probabilistic and is consequently subject to statistical error. The UK Government Biometrics Working Group (BWG) expressed in their Biometric Security Concerns that current knowledge of biometric algorithm behavior and human feature randomness and variation does not permit theoretical analysis of biometric system performance. [7]

The key to finding an appropriate security mechanism for an ubicomp environment should consequently not focus so much on the technical aspect but should instead have usability as a primary motivation or goal. Zurko and Simon [14] refer to this approach as **user-centered security**, and one subscribes to this concept.

As it has already been mentioned, the traditional log-in/password schema completely disrupts a smooth flow of work in the settings prescribed by a ubiquitous computing environment. As users abandon a static room with its desktop computer for a world in which every device offers computer support, the aspects of mobility, cooperation, interruption, and sharing of material become core aspects of much real world work. The design of security systems for this kind of working environments needs to accommodate such challenges, rather than unconsciously adopt existing user authentication mechanisms.

Historically, the first security application to articulate a user-centered design philosophy was Privacy-Enhanced Mail (PEM).[11] “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 from 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.[14] This example shows that considerations for users’ natural working patterns rather than more complex techniques can strengthen the security of the system.

While the implementation details of a suitable security mechanism for an ubicomp environment may vary, one believes any security mechanism designed for this kind of environment should succeed in accomplishing the following five objectives:

1. **Allow for proximity-based user authentication.**  
The term proximity-based user authentication was first introduced by Jakob E. Bardram [3] in his article based on Donald Norman’s essay “The Trouble with UNIX.”[12]
2. **Support migrating user session within devices.**
3. **Easy transition between users in the same device/allow multi-user sessions.**
4. **Flexibility to create and/or delete new users (for users authorized to do so).**

5. **Common procedures and interfaces within devices when deemed possible.**

## 5 Conclusions

As user-interface technology continues to evolve and users' needs continue to diversify at an unprecedented pace, no single technology or architecture is always "user friendly."

The paradigm for designing security mechanisms in a ubicomp environment 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. [5]

## References

- [1] Anne Adams and Martina Angela Sasse. Users are not the enemy. *Communications of the ACM*, 42(12):40–46, 1999.
- [2] EJ Amoroso. Fundamentals of computer security. *PTR Prentice Hall. Englewood Cliffs, NJ*, 1994.
- [3] Eyvind Bardram. The trouble with login: on usability and computer security in ubiquitous computing. *Personal and Ubiquitous Computing*, 9(6):357–367, 2005.
- [4] Anne M. De Alvare and Eugene E. Schultze. *A framework for Password Selection*, 1988.
- [5] Ivan Flechais, M Angela Sasse, and Stephen Hailes. Bringing security home: a process for developing secure and usable systems. In *Proceedings of the 2003 workshop on New security paradigms*, pages 49–57. ACM, 2003.
- [6] Rich Gold. *The plenitude: Creativity, innovation, and making stuff*. MIT Press, 2007.
- [7] Biometrics Working Group. *Biometric Security Concerns*, 2003.
- [8] International Organization for Standardization. *International Standard ISO 9241-11*, 1998.
- [9] International Telecommunication Union. *The World in 2014: ICT Facts and Figures*, 2014.
- [10] Anil Jain, Lin Hong, and Sharath Pankanti. Biometric identification. *Communications of the ACM*, 43(2):90–98, 2000.
- [11] John Linn. *Privacy enhancement for internet electronic mail: Part I: message encryption and authentication procedures*, 1993.
- [12] Donald A Norman. The trouble with unix. *Datamation*, 27(12):139, 1981.
- [13] Mark Weiser. The computer for the 21st century. *Scientific american*, 265(3):94–104, 1991.
- [14] Mary Ellen Zurko and Richard T Simon. User-centered security. In *Proceedings of the 1996 workshop on New security paradigms*, pages 27–33. ACM, 1996.