CRC Press
Taylor & Francis Group

INTEGRATING USABLE SECURITY PROTOCOL AND PATERNS INTO USER AUTHENTICATION SERVICES DESIGN PROCESS

CHRISTINA BRAZ, BILAL NAQVI AND AHMED SEFFAH

ABSTRACT

Both security and usability are essential in user authentication process. One of the biggest challenges faced by heterogeneous organizations is providing access control services (*to logical/physical resources*) that are both secure and usable. To achieve this, it is initially necessary to implement three indispensable components such as Identification (*Who does this user claims to be?*), Authentication (*Is this user in fact who s/he claims to be?*), and Authorization (*Is this user authorized to have the resource or service that s/he is requesting?*). Inquiry particularly on user authentication is vital. Without authentication, a system often has no foundation for establishing if access should be granted or not.

So far, there has been very little research on usable security of user authentication methods, although a considerable body of research work has been made for computer security mechanisms in general other than authentication methods. Therefore a usable security protocol is needed for user authentication. There is an intrinsic conflict between creating systems that are secure and systems that are usable. But usability and security can be made synergistic by providing requirements and design tools with specific usable security principles earlier in the requirements and design phase. In certain situations it is possible to concurrently increase usability and security by revisiting design decisions that were made in the past. In other situations it is possible to align security and usability by changing the regulatory environment in which the computers operate.

The main goal of this book is not to address usability and security after the product (authentication method) has been manufactured, but to make security a natural outcome of the requirements and design phase of the authentication method development life cycle.

INTRODUCTORY CHAPTER

All systems require some form of user account. A user is a single entity whose behavior is solely identified within a computer-based system (i.e. Personal Digital Assistant (PDA), workstation, server login, Web sites, etc.). Individual users classically correspond to individual people, but they might also represent particular system services or resources. Most accounts are protected by an easy keyboard password that even a novice hacker can crack in less than 10 minutes. Once inside, hackers use the attacked account for a diversity of nefarious activities, such as launching distributed denial of service (DDOS) attack, distorting Web sites, stealing billing and credit card information or making counterfeit purchases.

A report from Penn (2008) Forrester Research shows that security spending is on the rise in some enterprises. The Cambridge, Massachusetts-based research firm interviewed practically 1,000 firms for its State of Enterprise IT Security: 2008-2009 report and found that the security segment of Information Technology (IT) budgets is expected to increase 12.6 percent in 2009, up from 7.2 percent in 2007 and 11.7 percent in 2008. As a matter of fact even during difficult economic conditions, IT security remains an essential portion of business operations as enterprises try to preserve their current environment as well as plans for the implementation of novel initiatives. Security is getting a bigger portion of the IT pie, with less focus on reactive vulnerability defenses and more on looking at what is required to protect businesses. The focus now is more on protecting the data itself which means information security.

Distribution of budget for new security initiatives, information security, has increased from 17.7 percent in 2008 to 18.5 percent in 2009. There has been a major shift from what was the broadly recognized state of security just a few years ago. Protecting the organization's information assets is the top concern facing security programs: data security (90 percent) is most frequently mentioned as a vital concern for IT security organizations, followed by application security (86 percent), and business continuity/disaster recovery (84 percent). Data security as well tops the list of business objectives for security, with 89 percent mentioning protection of corporate data and 87 percent mentioning protection of personal data as essential business objectives. Most of this 2008 spending on information security countermeasures focused on purchasing confidentiality and integrity solutions: products like firewalls to protect the information perimeter of an enterprise (or encryption), Virtual Private Networks (VPNs)[1], and anti-virus and intrusion detection to safeguard the actual information.

Spending on user authentication products to safely identify users has followed in the security market. Inefficient user authentication marginalizes perimeter security and access controls, showing vulnerabilities in the confidentiality and integrity areas. The growing trend towards identity theft, or employing stolen names, birthdays and identification numbers to perpetrate fraud, would meet firm resistance if strong authentication practices were universally employed. Privacy violations take place as well due to compromised user authentication. Authentication is behind confidentiality and integrity because exactly identifying huge number of users has proven a costly and overwhelming task.

[1] A VPN is a network that uses a public telecommunication infrastructure, such as the Internet, to provide remote offices or individual users with secure access to their organization's network.

The central research question of this book is the following:

> *How is it possible to ensure usability of user authentication without compromising security and vice-versa?*

Security and usability are both essential in the authentication process. It is broadly held that security and usability are two opposing goals in system design (Cranor and Garfinkel, 2005; Jøsang *et al.*, 2007; Nielsen, 2000) but there are several cases in which security and usability can be synergistically enhanced by reviewing the usable security approach. In addition, the human portion of computer security is effortlessly exploited and continually overlooked. Companies spend millions of dollars on firewalls, encryption and secure access devices, but most of the times they forget to address issues related to the weakest link in the security chain: the human being.

In considering the extent that users are important in the authentication process, a company's goal is to select an Authentication Method (AM) that is suitable to cater the risk involved and as easy to use as possible. Applying too low a level of security might compromise the integrity of the company's process. But applying too high a level for a low-risk process means the process will be too hard and will confront low adoption rates. As stated by Penn (2008), the key criteria when assessing such solutions are ease of use, portability, cost, security, manageability, and cross-channel utility.

Our book focuses on the fact that since there is an intrinsic conflict between creating systems that are secure and systems that are usable. To these ends, this book's goal is not to address usability and security after the product (authentication method) has been manufactured, but to make security a natural outcome of the requirements and design phase of the authentication method development life cycle.

The importance of usability of authentication services

Security and usability are both essential in user authentication processes. One of the biggest challenges facing heterogeneous organizations is providing access control systems, to logical as well as physical resources, that are both secure and usable. To achieve this, it is necessary to implement three indispensable questions:

- *Who does this user claims to be?*
- *Is this user in fact who s/he claims to be?*
- *Is this user authorized to have the resource or service that s/he is requesting?*

The majority of contemporary computer users for example need to authenticate to a company network several times *during* their work *day*. Another particular concern in authentication according to Cranor and Garfinkel (2005) is that authentication systems *do not fail gracefully*. It means that if an average consumer computer user forgets her username but gets right the password the system does not enable her partial access to an online magazine, for instance, or for an average corporate computer user access to the system's less important files, or an emergency or temporary access. However there are a few companies that are in the initial stages of implementing some of these "*fail gracefully*" functionalities[2] in the corporate area. There is

[2] Users who have lost their hardware authenticator, for instance, can still log in to their accounts with an emergency access code through the on-demand authentication method, without having to contact the system

no established and recognized mechanism to accommodate user error, which means that most likely the productivity will be strongly compromised and the user's dissatisfaction with the system will be high. Figure 1.1 models the relationship between usability and security.

General principles for User Interface Design (UID) have already been well recognized in the Human Computer Interaction (HCI) field**.** These general principles are called "heuristics" because they are more in the nature of rules of thumb than specific usability guidelines (Molich and Nielsen, 1990) (e.g. "U**ser Control and Freedom" is one of these principles).**

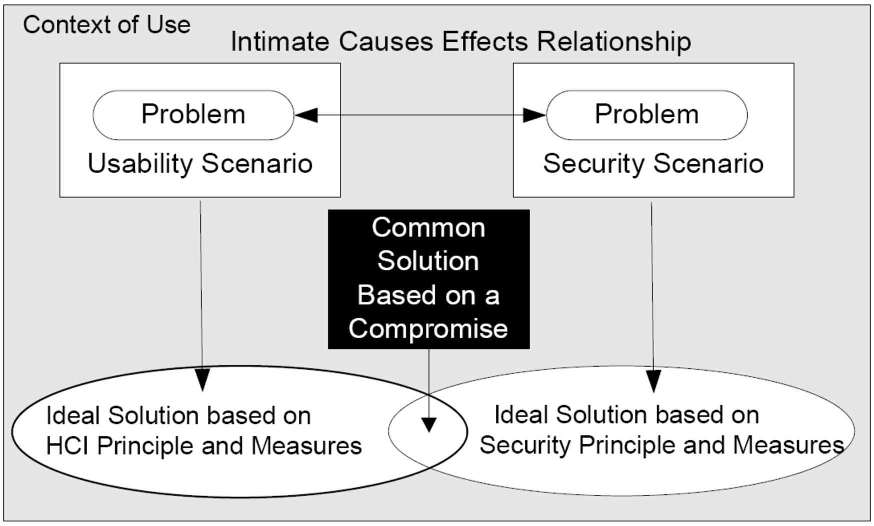

Context of Use
Intimate Causes Effects Relationship
Problem
Usability Scenario
Problem
Security Scenario
Common Solution Based on a Compromise
Ideal Solution based on HCI Principle and Measures
Ideal Solution based on Security Principle and Measures

Figure 1: Usability and Security Trade-off: A Common Solution Based on a Compromise

So far, there has been very little research on the security usability of user authentication methods, although a considerable body of research work in usable *security* (a terminology adopted in this book when referring to security and usability) has been made for computer security mechanisms in general other than authentication methods. Therefore a usable security protocol is needed for user authentication.

This book defines the concept of Usable Security as the study of how security information and usability factors should be handled in either front-end or back-end user authentication processes, taking into consideration resources and costs. But why take front-end/back-end processes into consideration? Graphical User Interface (GUI) Developers should have knowledge of user interface design, and tools for implementing designs correctly. This knowledge will result in better front-end design, minimize the number of bugs in the software, and result in lower development costs per feature. GUI Developers should be assigned responsibility for accurate implementation of front-end design, as well as back-end functionality. GUI Developers should understand interface issues sufficiently well to know when to raise design issues during implementation, rather than disregarding them or implementing them inaccurately.

It is crucial to note that the term -*interface*- in this book is not only related to GUI, but also to a shared limit through which the information flows (Maffezzini, 2006). It consists of a hardware or software component that makes the junction between the interface and the user

administrator. RSA SecurID® On-demand (SMS) Authenticator. RSA - The Security Division of EMC <http://www.rsa.com/node.aspx?id=3481>

with the purpose of transiting information between them (e.g. an OTP token is an interface between the authentication server and the user) (Figure 2).

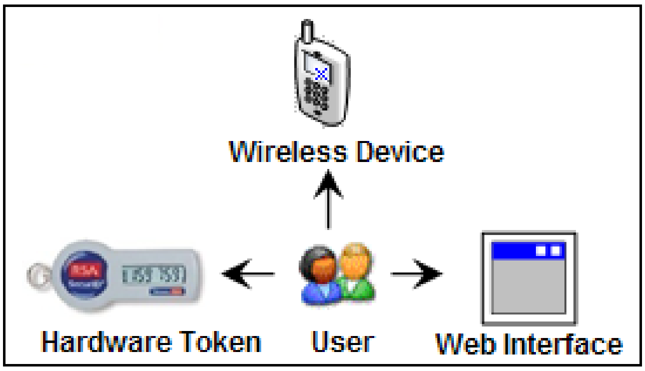


Figure 2: Objects with which users might interact: An authentication token[3], a wireless device, and a Web interface.

According to Sasse (2004), one of the most recognized researchers in usable security-, “Don’t focus on UIs to security tools - the big problems are in security requirements, job design and user involvement.” That is exactly what this book is all about: requirements and design. Additionally, according to Whitten and Tygar (1999), most of the research in HCISec focuses on providing better UIs, but it is obvious that usability problems with secure systems are more than only UIs and need application of HCI factors and design methodology. Whitten and Tygar *(*1999) claim that using conventional methods for usability evaluation that concentrate on the impact of usability on security effectiveness will assist developers to discover usability problems that threaten-1 security. Both analytical and empirical evaluations were performed in testing the usability goals of Pretty Good Privacy (PGP) Desktop E-mail software (i.e. public key *encryption software for desktops and laptops)* (Whitten and Tygar, 1998).

A number of usability problems causing security failures were discovered in the study, providing the foundation in the Whitten and Tygar (1999) study that specific usability goals are needed for usability evaluation of security mechanisms. It is important to note that the PGP software has been cited throughout this dissertation as an example of public key authentication. This is due to the fact that PGP is one of the most common solutions for email encryption, supports -major email security standards, and interoperates with most accepted email security software solutions.

The value of usable security was pointed out as early as 1883 by the Belgian cryptographer and linguist Auguste Kerckhoffs in two articles on cryptography. Kerckhoffs is most famous for establishing the principle that security should not be based on obscurity. Moreover, four out of six of Kerckhoffs’ cipher principles of design (Kerckhoffs, 1883) are related to usable security (3 to 6) in bold) as follows:

1. The system must be practically, if not mathematically, indecipherable;
2. It must not be required to be secret, and it must be able to fall into the hands of the enemy without inconvenience;
3. Its key must be communicable and retainable without the help of written notes, and changeable or modifiable at the will of the correspondents;
4. It must be applicable to telegraphic correspondence;

[3] http://www.rsa.com/node.aspx?id=3049

5. It must be portable, and its usage and function must not require the concourse of several people;
6. Finally, it is necessary, given the circumstances that command its application that the system should be easy to use, requiring neither mental strain nor the knowledge of a long series of rules to observe.

The initial data gathered on usable security related to user authentication methods are basically research regarding an evaluation of Pretty Good Privacy (PGP) (Whitten and Tygar, 1998), a public key encryption program primarily intended for authentication and email privacy, anti-phishing authentication mechanisms (Dhamija *et al.*, 2006; Dhamija and Tygar, 2005), security toolbars (Wu *et al.,* 2006), user authentication mechanisms (pictorial passwords) (Angeli *et al.*, 2003), security user studies (Chiasson and Biddle, 2007), secure User Interface (UI) for network applications (i.e. authentication of the communication) (Jøsang and Patton, 2003), design principles and patterns for computer systems that are secure and usable (Cranor and Garfinkel, 2005), and some general white papers about user authentication. Although, Human Computer Interaction-Security (HCI-Sec) researchers have been applying HCI techniques in security software on a very small scale, there are no methods or techniques to effectively design secure and usable user authentication systems yet. This is area which this book is going to explore: integrating usable security in the requirements and design phase.

Moreover, authentication services are critical to authorization and auditing services. If users' identities are not appropriately authenticated, an organization has no guarantee that access to resources and services is correctly monitored. Regardless of how well controlled a company's authorization services are, everything stems from the exact identity of the users. Also, correspondingly, without accurately authenticated identities, audit trails, though complete and well monitored, will be untrustworthy and give no accountability (e.g., a forged user ID could be linked to auditing actions).

On October 12, 2005, the Federal Financial Institutions Examination Council (FFIEC) issued the updated guidance, "Authentication in an Internet Banking Environment." FFIEC requires that financial institutions provide consumers of online financial services with the same security protection enjoyed by customers buying groceries or gas with a debit card: strong authentication. The -FFIEC (2005) guidance states the following: "Single-factor authentication, as the only control mechanism, to be inadequate for high-risk transactions involving access to customer information or the movement of funds to other parties. The authentication techniques employed by the financial institution should be appropriate to the risks associated with those products and services. Account fraud and identity theft are frequently the result of single-factor (e.g., ID/password) authentication exploitation."

The Consequences of a Lack of Commitment to Usability

Without a proper user authentication system (the "door-entry" of any system), organizations are susceptible to potential attackers who can compromise the whole organization's computer and network system, and consequently undermine its infrastructure and assets as well. For example, the -CSI/FBI-- Computer Crime and Security Survey (2008) defined 13 types of attacks or computer mishandling resulting in direct financial loss to the survey's participants (Table 1). The survey asks about a number of different sorts of computer attacks and incidents. The areas marked with red squares in Table 1 highlight the type of incidents related to authentication. A significant percentage (44%) is responsible for attacks coming from inside an organization. In figure 3, a subset of the mentioned attacks is graphed, with data stretching back to 1999 by percentages of key types of incidents. In Particular, this chart illustrates the four categories of highest incidence: viruses, insider abuse, laptop theft, and unauthorized access to systems.

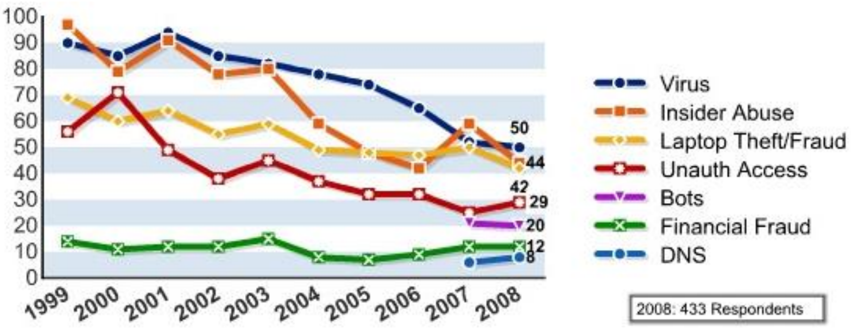
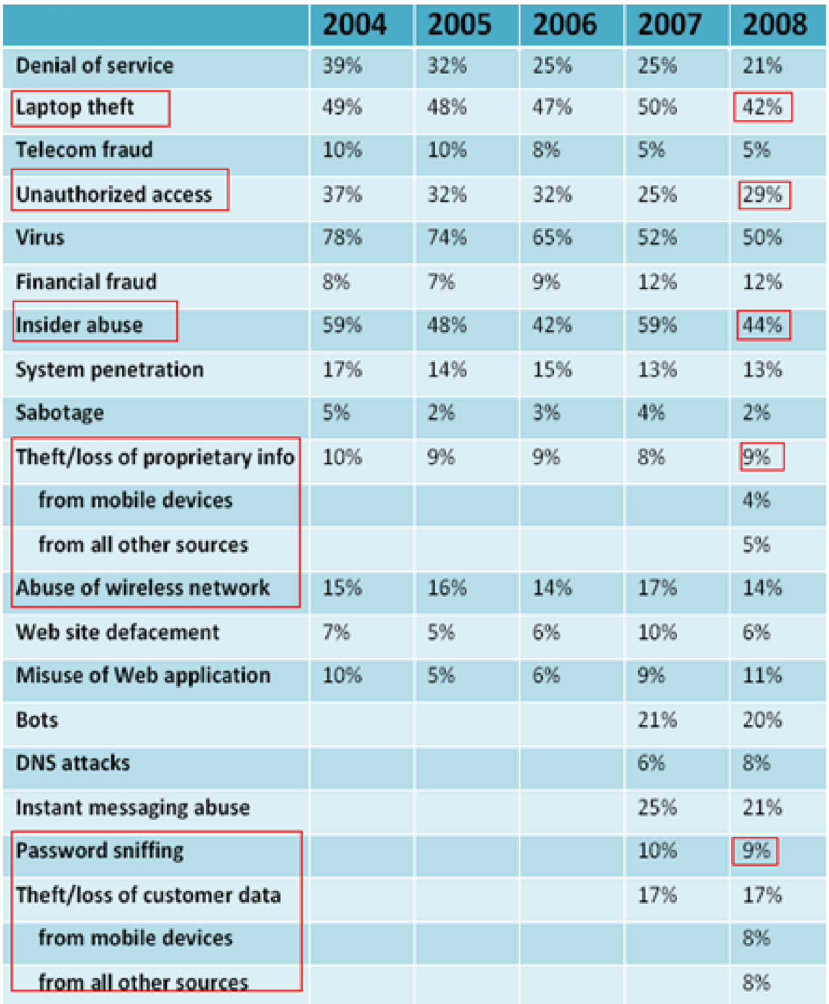


Figure 3: Percentages of key types of incident (CSI/FBI, 2008).



	2004	2005	2006	2007	2008
Denial of service	39%	32%	25%	25%	21%
Laptop theft	49%	48%	47%	50%	42%
Telecom fraud	10%	10%	8%	5%	5%
Unauthorized access	37%	32%	32%	25%	29%
Virus	78%	74%	65%	52%	50%
Financial fraud	8%	7%	9%	12%	12%
Insider abuse	59%	48%	42%	59%	44%
System penetration	17%	14%	15%	13%	13%
Sabotage	5%	2%	3%	4%	2%
Theft/loss of proprietary info	10%	9%	9%	8%	9%
from mobile devices					4%
from all other sources					5%
Abuse of wireless network	15%	16%	14%	17%	14%
Web site defacement	7%	5%	6%	10%	6%
Misuse of Web application	10%	5%	6%	9%	11%
Bots				21%	20%
DNS attacks				6%	8%
Instant messaging abuse				25%	21%
Password sniffing				10%	9%
Theft/loss of customer data				17%	17%
from mobile devices					8%
from all other sources					8%

Table 1: Percentages of key types of incident (CSI/FBI, 2008).

Virus incidence fell below insider abuse last year, but regained its position of the most common occurrence this year. That said, both categories dropped compared to last year, and actually all four of the most widespread types of incidents fell. There seems to be an obvious trend of lower and lower percentages of incidence being reported in these categories over the past several years. Table 1 also shows that only four categories showed to some extent increased percentages.

In the real-world, organizations struggle to enforce security policies—even the most basic ones (e.g. password). When a user has unsupervised physical access to a mobile device, for example, he can usually do whatever he wants with it, even authenticate himself through the software token installed in the mobile device since he knows his friend's username and password. As a result, most of these policies violate the Big Stick principle: *Whoever has physical access to the device is allowed to take it over* (Stajano, 2003) (as in the previous example). These policies are extremely hard to enforce and thus scarcely of practical usage. The Big Stick Principle is a very high level security policy model which identifies a set of cases in which authentication is superfluous.

In the Web area, it is worth noting that 5 out of the top 10 Web application security vulnerabilities are directly or indirectly related to authentication according to OWASP (2009).