Usability: Gaining a Competitive Edge
IFIP World Computer Congress 2002
J. Hammond, T. Gross, J. Wesson (Eds)
Published by Kluwer Academic Publishers

Evaluating Security Tools towards Usable Security

A Usability Taxonomy for the Evaluation of Security Tools based on a Categorization of User Errors

Johannes Kaiser and Martin Reichenbach
Institute for Computer Science and Social Studies, University of Freiburg, Germany.

Abstract: The main success of the internet is its openness. To guarantee security in the internet - for example to protect the user's privacy - the use of security tools is essential. Because today's internet users cover almost all educational levels and professional groups, we assume that in most cases they will be security novices. Unfortunately, the usage of today's security tools is mostly too complex and incomprehensible, thus opening security leaks caused by incorrect usage. In order to identify security leaks arising from the user interface, an *objective* measure for the usability of security tools is necessary. At present, such a measure does not exist. This paper develops such a measure for the usability of security tools. We propose problem categories for errors in security tools. Based on this categorization, we propose a taxonomy for the usability of security functions. Applying this taxonomy, security functions may be ranked according to the user's ability to avoid self-induced, security-critical user errors. Additionally, the taxonomy may explain possible causes of errors, introducing design alternatives to avoid these errors.

Key words: usability, multilateral security, security-critical user errors, usability evaluation

1. INTRODUCTION

Beyond doubt the main success of the internet is its openness. In order to protect the user's privacy or the security of online transactions, internet users have to be aware of security. Thus, the average user is confronted with security tools and embedded security functions in internet applications and therefore with the necessity to understand the underlying security concepts. In the following, the term security tool also implies embedded security

functions in internet applications.

In (Whitten, 1999), it is shown that the underlying security concepts are mostly unfamiliar and incomprehensible to the security novice user and hence the security tool is not usable.

For evaluating the usability of security tools and for developing criteria for the design of usable security tools, it is necessary to establish an objective measure. Unfortunately, such an objective measure for the usability of security tools does not yet exist.

In the following, we present the concept of multilateral security. By applying this concept, the relevance of usability problems for security may be identified.

1.1 Multilateral security and its basic functions

The protection goals of multilateral security were proposed to guarantee secure communication (Rannenberg, 1999). These are confidentiality, integrity, availability and accountability. The protection goals will be fulfilled directly by security functions (see figure 1) (Rannenberg, 1998).

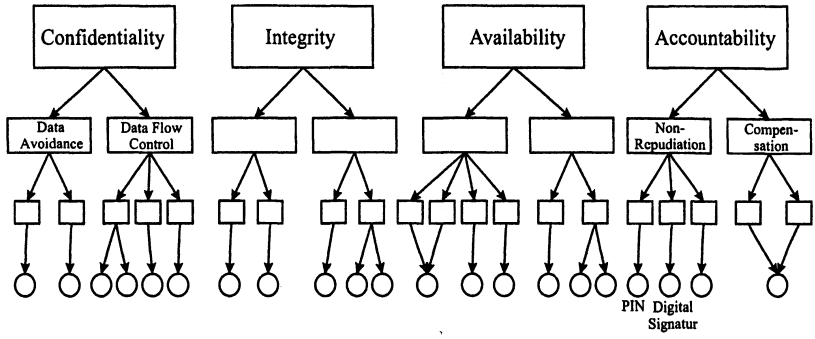

Figure 1: The hierarchy of protection goals, protection principles, functional building blocks and security functions.

These security functions can be controlled partly by the system, so the user is not burdened with having to deal with this. In most cases, however, security functions with their underlying security concepts stand directly in dialog with the users. Hence, user errors through an incorrect handling of the security functions are possible. Such a user error is critical for security, if at least one protection goal of multilateral security is threatened. These security-critical user errors are the main subject of this article. We are using

the terms security critical user error and security critical usability problem synonymously.

In the following section, we propose an essential assumption about the average user of security tools and discuss the meaning of the usability of security. In Section 2, we derive a taxonomy based on security-critical user errors as an objective measure for evaluating the usability of security tools. Section 3 describes an error database for the design of usable security, realized by collecting security-critical user errors and adequate design alternatives for avoiding these errors.

1.2 User profiles of security tools

In order to design usable security tools, the system's developer needs an idea of the user's understanding of underlying security concepts. The more the system design takes into account the user's security competence, the more securely the user is able to handle the security tool. Thus, the system design must adapt to the user's security competence.

As system design based on automatic recognition of an individual user's competence is too complex and the results are mostly unsatisfactory, it seems reasonable to design security tools for user profiles according to their security competence. Examples for profiles based on the security competence are security novices, security interested persons and security experts.

Considering the demographic development of internet users, today's internet users cover almost all educational levels and professional groups. We assume, therefore, that today's average internet users are not internet experts, much less security experts. In consequence, we propose the following assumption of the user's security competence: In most cases, the average user of the internet will remain a security novice.

Based on this assumption, it is important to develop security tools according to the user's low security competence without reduction or abandonment of security functionality. This assumption also implies that a security tool will be widely used if it can be used securely by users with little security knowledge and little security experience.

It is important to take user profiles into account in the design of security systems because the design may be completely different for security experts than for security novices.

For these reasons, we consider the average user as being a security novice. After all, security is usable even if the average user as security novice is able to use the security tool in a secure way, i.e. without producing security-critical errors.

In the following, we define and categorize security-critical user errors, resulting in a taxonomy that enables system developers and system administrators to evaluate the usability of security tools.

2. CATEGORIZATION OF USABILITY AND SECURITY PROBLEMS

2.1 Sets of usability and security problems

Security systems may be considered to be secure if they fulfil, for example, the Common Criteria for Information Technology Security Evaluation (CCITSE, 2000). By certifying security systems according to the CCITSE, security problems on the technical layer can be avoided.

Security problems can also stem from the user interface, however. Usability problems can be divided into the following two sets:

- Security-non-critical usability problems;
- Security-critical usability problems.

Assuming security-non-critical usability problems are avoidable by ergonomic guidelines for software design as stated in (ISO 9241, 1996), these problems may be ignored.

Usability problems, on the other hand, are security-critical if at least one protection goal of multilateral security (Rannenberg, 1999) is threatened. In the following we discuss whether security-critical usability problems exist in security tools, despite certified security (CCITSE, 2000) and despite common usability guidelines.

Considering usability guidelines, we point out that security aspects are not yet considered. This is illustrated below by two examples of security-critical user errors occurring in security systems certified by the CCITSE, and that are not addressed by present usability guidelines:

1. The user wants to send an encrypted e-mail. He encrypts the e-mail correctly for the receiver. Because the e-mail tool is using the S/MIME standard, the security concept behind the e-mail tool means that the header of the e-mail with the subject is not encrypted. So it is security-critical if the user reveals information in the subject about the possible confidential content of the encrypted e-mail. The protection goal confidentiality is threatened.
2. For authentication by digital signature, a password is frequently used to activate the private key. Due to so-called PIN inflation, the user writes down his PIN or password on a paper list. So attackers on the digital signature can steal or copy this list. This user error is security-critical because if the attacker has also stolen the private

key, he can take the identity of the attacked person in the internet. The protection goal accountability is threatened.

According to the above mentioned assumption that users will be mostly security novices, these security-critical user errors are real.

Altogether, three essential sets of problems in security applications could be identified (see figure 2):

- Usability problems which are not security-critical;
- Security-critical usability problems;
- Security problems (on the technical layer) which do not arise from user interactions.

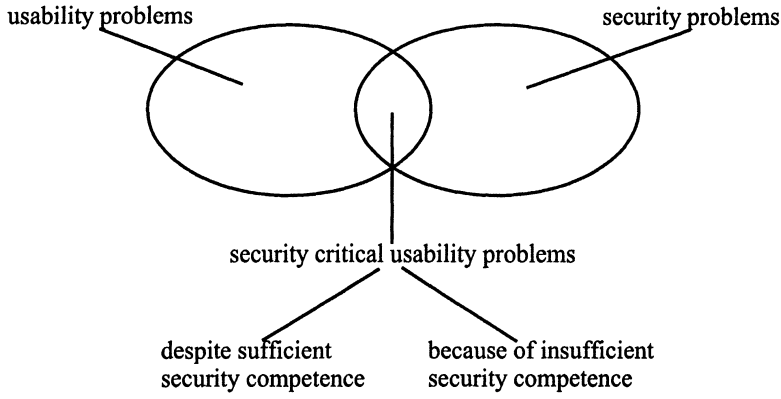

Figure 2: Three essential sets of problems in security applications.

2.2 Problem categories

Usability problems which are not security-critical are represented in the following by problem category I. Security problems which do not arise from user interactions are represented in the following by problem category IV.

According to the user's competence, it is important to divide security-critical usability problems into two further sub-categories. These sub-categories are presented by problem categories II and III (see Figure 2):

Problem category I

Usability problems which are non-critical to security.

Problem category II

Usability problems which are critical to security and arise despite the user's sufficient security competence.

Problem category III

Usability problems which are critical to security and arise from the user's insufficient security competence.

Problem category IV

Security problems which do not arise from user interactions.

This differentiation of security-critical usability problems in problem categories II and III is important for the design or redesign of security tools. A redesign based on problem category II will be extremely different from a redesign based on problem category III. For instance, user errors of problem category II can more likely be avoided by emphasising the underlying security concept. The redesign aiming at avoiding category III errors, however, would more likely succeed by concealing the underlying security concept and searching for an adequate comprehensible security concept as a substitute.

The cause of category III errors is the user's insufficient security experience. In order to detect the causes of category II errors, further investigations of security-critical usability problems are necessary as discussed in the next section.

At this point, user errors act as indicators for the conformance between the real world as perceived by the user, and the system world (Prabhu et al, 1997). That is, if a security concept is not well known to the user, he may still be able to handle the dialog correctly if he knows an adequate rule or analogy from the real world. The real world as perceived by the user is conform to the system world.

On the other hand, if the user is familiar with the underlying security concept, we can also talk about a conformity of the real world perceived by the user and the system world. For the design of security tools, it is important to know if the real world perceived by the user conforms with the world mapped by the system.

2.3 Familiarity with security concepts

Category II errors strongly depend on the degree of the user's familiarity with the underlying security concept. With a higher familiarity with system dialogs, less errors will be made by users in everyday use. Therefore, the degree of familiarity of security concepts may show how well the user is able to avoid category II errors by himself.

A first approach for identifying the user's familiarity with the underlying security concept is the subdivision of errors into slips and mistakes (Prabhu et al, 1997):

- Slips: The plan of the action may be correct but the action does not go as planned.
- Mistakes: The action may go as planned but the plan itself is wrong.

If a security concept is very familiar to the user, a probable error cause might be a slip, i.e. the action does not go as planned. If the security concept is known without sufficient familiarity to the user, a probable cause of the user error might be a wrong plan (mistake).

Slips occur on an action level (skill-based level), whereas mistakes occur on a plan level (Rasmussen, 1986). This plan level is differentiated by Rasmussen into two further levels: the rule-based level and the knowledge-based level (Rasmussen, 1998). If a user is not able to solve the problem on the rule-based level, he might change to the knowledge-based level. The mental effort or cognition complexity on the knowledge-based level is higher than on the rule-based level. The higher the cognition complexity, the more likely user errors become (Reason, 1990).

Generally, in order to recognize the user's familiarity with a security concept, the deployment of usability tests is recommended (Nielsen, 1993).

The following section uses the above-mentioned categorization of security-critical usability problems to rank security tools according to their usability.

2.4 Usability taxonomy of security tools

By the differentiation of security-critical usability problems into problem categories II and III, user errors may be ranked according to the user's ability to avoid errors by himself. If a security tool's user interface presents the user with an unfamiliar security concept (problem category III errors), the ability of the user to avoid errors is lower. On the other hand, with a security tool's user interface reflecting familiar security concepts (problem category II errors), user-driven error prevention is more likely.

This is illustrated by the following inequality:

$$\text{user error}_{\text{problem category II}} < \text{user error}_{\text{problem category III}},$$

where "<" means "... is easier to avoid by the user than ..."

If the user error belongs to problem category II, the error arises in spite of the user's familiarity with the security concept. The three performance levels (skill-based, rule-based and knowledge-based level) suggest a ranking of category II errors by their inherent cognitive familiarity (Reason, 1990).

Errors on the skill-based level occur in a familiar environment, while errors on the rule-based level occur in a somewhat familiar environment and

errors on the knowledge-based level occur in a unfamiliar environment (Rasmussen, 1986).

This is reflected by the following inequality:

$$\text{user error}_{\text{problem category II, skill-based}} < \text{user error}_{\text{problem category II, rule-based}} < \\ < \text{user error}_{\text{problem category II, knowledge-based}}$$

According to transitivity, we are proposing the following taxonomy of user errors in security tools:

$$\text{user error}_{\text{problem category II, skill-based}} < \text{user error}_{\text{problem category II, rule-based}} < \\ < \text{user error}_{\text{problem category II, knowledge-based}} < \text{user error}_{\text{problem category III}}$$

For detecting user errors in security tools, either the cognitive walkthrough or the heuristic evaluation method may be used (Nielson, 1993). User errors may be identified as critical for security by simply examining whether at least one protection goal is threatened.

Hence, user errors and their security relevance are objectively measurable. This taxonomy can, therefore, supply an objective measure for the usability of security tools.

3. IDENTIFYING USER ERRORS BASED ON THE CONCEPTS OF MULTILATERAL SECURITY

An important aim of research into usable security must be to investigate the usability of security functions of multilateral security. If security-critical user errors are possible, the introduced taxonomy shows how well the user may avoid the errors by applying his security competence. Based on these results, design alternatives for avoiding security-critical user errors have to be found.

In accordance with the threatened protection goals of multilateral security, the design alternatives and the alternative security functions will lead us to a collection of usable security functions. An alternative security function on the one hand substitutes the entire security function. A design alternative on the other hand avoids the security-critical user error through better design of the original security function (see Figure 3).

This collection of user errors will be realized as a publicly available database in order to support the work of designers of security tools, for example, to implement usable tools for novice users. The database can also support system administrators or system officers to find out how secure a security system really is during use. Additionally, a user may use this

database to find security tools which can be easily and securely used with his degree of security competence.

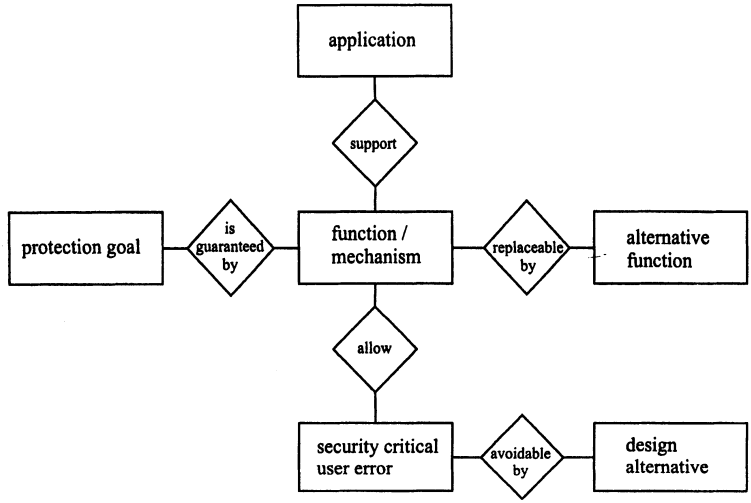

Figure 3: Entity-relationship-model of the error-database.

4. CONCLUSION

This paper puts forth a taxonomy for a usability evaluation of security tools. In further work, currently deployed security functions in security tools will be evaluated according to the taxonomy introduced. According to the results of usability tests, these concepts will be improved in order to avoid further security-critical user errors.

Avoiding security-critical errors in spite of the user's low security competence may finally lead to an increased acceptance of security tools.

5. REFERENCES

CCITSE - The Common Criteria for Information Technology Security Evaluation (2000): Common Criteria Version 2.1 / ISO IS 15408.

Common Criteria for Information Technology Security Evaluation V 2.1, Version 2.1.

ISO-Standard, no. 9241-part 10 (1996): Guidlines for dialogue design.

Nielsen, J. (1993), *Usability Engineering*, Academic Press.

Prabhu, P.V. & Prabhu G.V. (1997), *Human Error and User-Interface Design*, in Helander, M., Landauer, T.K. & Prabhu, P.V., *Handbook of Human-Computer Interaction.*

Rannenberg, K., *Zertifizierung mehrseitiger IT-Sicherheit – Kriterien und organisatorische Rahmenbedingungen* (1998); Reihe DuD-Fachbeiträge im Verlag Vieweg, Braunschweig u.a.

Rannenberg, K., Pfitzmann, A., & Müller, G. (1999), *IT Security and Multilateral Security.* In Müller, G. & Rannenberg, K. (Eds.), Technology, Infrastructure, Economy, Volume 3 of *Mulitlateral Security in Communications*, pages 21-29, Addison Wesley Longman Verlag GmbH.

Rasmussen, J. (1986), *Information Processing and Human-Machine Interaction*, Amsterdam: North Holland.

Reason, J. (1990), *Human Error*, Cambridge University Press.

Whitten, A. & Tygar, J.D. (1999), Why Johnny Can't Encrypt: A Usability Evaluation of PGP 5.0, in *Proceedings of the 8th USENIX Security Symposium.*