Scientific and Practical Cyber Security Journal (SPCSJ) 2(2):13-17
Scientific Cyber Security Association (SCSA), 2018 ISSN: 2587-4667

MODERN APPROACHES TO THE SECURITY EVALUATION: A ROADMAP TO SECURE AND USABLE SYSTEMS

A. Fesenko, H. Papirna
Taras Shevchenko National University of Kyiv

ABSTRACT

There is a huge number of different methodologies for evaluating the security of the systems. However, even the most reasonable of them turn out to be incompetent due to the omission of the importance of keeping user convenience in mind. This disadvantage has been resulted in the spread of secure, but useless, from the point of the performance of user tasks, systems. The aim of the article is to process and systemize the existing researches on the development and evaluation of systems, that include the human factor and users' needs. In addition to this, working recommendations has been considered to help developers and auditors of secured systems.

KEYWORDS: security evaluation, Human Computer Interaction (HCI), Human Computer Interaction and Security (HCISec).

1. Formulation of the problem

In a modern information world, where the use of computer systems has become widespread: from state structures and critical objects to large and small businesses, the problem of evaluating the security of the information system is urgent.

This need is due not only to state and international standards for the protection of information resources and information, the protection requirement of which is established by law, but also financial factors for business that arise in case of loss of critical information, unauthorized access to resources, or failure of the system.

When evaluating the level of security of information systems, there are problems associated with the following factors:

- variety of existing regulatory documents, regulatory data processing procedures, composition and content of organizational and technical measures for the protection of informational resources of various levels of confidentiality;
- lack of quantitative criteria for evaluating the security of information systems in normative legal documents;
- complexity, multicomponent structure of the evaluated information system;
- conditions of uncertainty and insufficient knowledge about threats and the probability of their realization for an information system;
- constantly changing information security incident statistics, including cyber threats that occur when connecting to the Internet [1].

2. Statement of the main material

After analyzing current international regulations of technical information protection, it becomes clear that approaches to evaluating the security of systems need some improvement.

Although actual criteria allow to evaluate the security of the system, they do not consider another important factor. The Human Computer Interaction (HCI) and Human Computer Interaction and Security (HCISec) have long been developing in the world. The popularity of these areas is due to the eternal struggle between the simple use of the system and the provision of an adequate level of security. Therefore, the evaluation of the security of the system is no longer possible in isolation from the convenience and ease of use.

The gaps and conflicts between security and usability have been carefully studied by several researchers. In [2] the author proposed to evaluate the security of the system by following guidelines or by using frameworks.

A working guideline with criteria for evaluating usability of secured systems has been outlined in [3]. It focuses on providing a checklist for software developers of secured systems.

According to this publication, the first and the main point is opened and understandable security for all users. It is the responsibility of the developer / deployer to hide as many security mechanisms as possible from the user. For those security mechanisms that are exposed to the end user it is necessary to get security awareness.

The second key point emphasizes the reduction of prohibitions for a user. A usable security mechanism should not be used to restrict the user in what he is doing but protect the user. This allows end users to efficiently fulfill their tasks. Any security-motivated restriction of the user should be carefully evaluated regarding necessity for system security and adequateness.

The next requirement highlights the minimum interaction of the security mechanism with a user and its role to grasp the user's attention. In addition to this, an efficient security system should not require the user to remember a lot of data. For example, the user can use an existing account to login and does not have to remember another password.

The following item considers the assurance that the average user is capable to make an informed security decision on the appeared issue. If it is not clear if the user can decide on an issue, the decision should be avoided.

Also, the user should not have to configure security when he first starts the system. It should always come preconfigured such that it is reasonable secure and usable. Another important issue is that a secured system should not use fear to force users to obey security policies or get a wanted reaction. It must always support a positive attitude of the user towards itself. Finally, a secured system should take into account that users tend to make mistakes, so the system must provide an explained response to the user and route the one to the right solution.Apart from guidelines, different frameworks and models can also be found in literature, that assist in addressing the conflicts between usability and security and provide critical factors to be investigated for evaluation of security and usability. A suitable example of such a framework has

been presented in [4]. According to this approach, to assess the security of the system, it is necessary to build a security–usability model.

To assess usability, the following criteria has been applied:

Effectiveness is measured by whether users can perform a specific task or not.

Satisfaction – although an objective analysis of usability is generally acceptable, a subjective evaluation of users is key to the success of the system.

Accuracy – requirements to which are driven by needs of users in providing the necessary information.

Effectiveness – using the system only to achieve a certain goal is not enough. The goal must be achieved within a reasonable time and effort.

To assess security, the following factors has been used:

Attention – security issues should not distract users from their work, as this will definitely lead to errors in security mechanisms and nervousness of users.

Vigilance – the system should provide users with the opportunity to be active and encourage them to instantaneously report about suspicious incidents in the system.

Motivation – users of the system should take every risk, as directed personally to them, in order to fulfill the security requirements more quickly.

Conditioning – the trivial types of frequently repeated security requirements should be avoided, as they are addictive and the user may inadvertently click on the wrong action in a critical situation.

Social context – users who work on one project are often inclined to share security secrets (shared passwords, certificates, etc.). The task of assessing the security of a system should take into account such a social experience.

As a general rule, there are two factors that combine security and usability:

Memorability – a large amount of information for authentication (passwords, secret words, etc.) threatens both usability (time to change the password) and security (writing down the secret information on a sheet of paper, etc.).

Knowledge and skills - the speed of user's learning of a system must be evaluated, especially to the security-related operations.

For a successful evaluation, both security and usability elements must be measurable. Therefore, auditors, after understanding the criteria listed above, should develop appropriate qualitative or quantitative metrics for system evaluation.

3. Development of recommendations

On the basis of the processed publications, it is possible to define recommendations [5] for the designers of the secured systems as well as for the system security auditors.

The first lesson to be concerned is that, the usable security cannot be retrofitted. The security community is completely sure that security must be designed into systems from the ground up; it cannot be "bolted on" to an existing system at the last minute. The same is true for usability of security. For example, adding explanatory dialog boxes to a confusing system is not the solution. Such fundamental design principles must be considered at the very beginning of the development process.

The second idea is that all the reliable security tools are not the complete solutions. Though, they are great resources in the hands of developers because they mean the reliance on proven protocols and implementations to give systems certain security properties, they are rather incomplete. This means that more high-level tools must be found to create user-oriented solutions.

The third important issue is that security is not something to handle only in the lower layers of the networking stack or in the depths of the operating system. If trying to solve the security problem purely in those lower layers, users inevitably have to deal with those layers when something goes wrong. Therefore, the security mechanisms must be compatible with what the user needs to accomplish.

The fourth recommendation is to put the users' needs first. The information security representatives often believe that security is more important than users' other needs, even when it results in a system that does not let users accomplish the tasks for which that system was designed. So, when designing a system, professionals must keep in
mind that they are not average users, and after they finish the system, their target audience should test it. Such studies can provide the basis for effective iteration cycles of design, implementation, and evaluation.

The last point is to try to think and act locally. Security solutions often seem to require generic, universal answers to problems, which do not actually exist in practice. Systems that follow the "think locally" principle are much easier to deploy, because they do not require administrators to coordinate with some larger infrastructure. As a result, they can offer greater opportunities for automatic configuration.

Conclusions

As the analysis of the publications shows, very few studies have been devoted to finding a balance between security and usability. However, when evaluating the security of a system, this

task is important in order to avoid a skew in the direction of cumbersomeness or weakness of the system. The solutions presented in the article are not a panacea for assessing the security of the system, but they set a new vector for development in this direction and expand the field of scientific and engineering activities in this area.

REFERENCES

1. Burkova E.V. The task of assessing the security of information systems of personal data // Bulletin of the Chuvash University. – 2016. – №1. – P. 113.
2. Alshamari M. A Review of Gaps between Usability and Security/Privacy // Int. J. Communications, Network and System Sciences. – 2016. – №9. – PP. 416-420.
3. Hof H.-J. Towards the enhanced usability of IT security mechanisms // User-Centric IT Security. – 2015.
4. Security and Usability: Analysis and Evaluation / R. Kainda, I. Flechais, A. W. Roscoe. // International Conference on Availability, Reliability and Security. – 2010. – PP. 277-279.
5. In search of usable security: five lessons from the field / D. Balfanz, G. Durfee, R.E. Grinter, D.K. Smetters. // IEEE Security and Privacy. – 2004. – PP. 21- 23.