جامعة بيرزيت

BIRZEIT UNIVERSITY

Computer Security (COMP432)
Proposal for Security Evaluation

Instructor: Dr. Hafez Barghouthi
Group Names :

Aseel Khalaf 1160689
Reem Shamasneh 1162422
Nada Zalloum 1162147

Abstract

Currently, information security is crucial to all organizations in order to protect their information and conduct their business.

Information security is defined as the protection of information, system, and hardware that use, store and transmit that information.

A lot of security holes are caused by design or implementation faults. Most of the developers are not aware of the whole bandwidth of possible attacks on their systems. An analysis and evaluation of the system's security aspects are often never done. In addition, security rivals with other goals as costs, duration of the development process, and functionality.

So, it’s important to know about how to evaluate a system’s security, and what does security evaluation means.

Introduction

The world with information technology tends to be fully dependent on data infrastructure and information exchange networks. This trend is increasing by permanent technological development, the growing power of computer equipment, the need for flexible and functional communication systems.

So organizations now have an extra load to protect their data and to provide secure systems that are hard to be accessed from intruders.

In order to have this security done perfectly, the term Security evaluation is here, where it provides an examination for the system in different ways, this analysis is done in different ways first by examining the full system by verification and validation, and second by observing the functional behavior of the system, or finally by attempting to access the system using attackers techniques.

Discussion

Computer security is now recognized as an important consideration in modern business, with a variety of guidelines and standards currently available to enable different business environments to be properly protected. However, financial and operational constraints often exist which influence the practicality of these recommendations. Formal methods have long been recognized as central to the development of secure systems. Formal models of security policy and formal verification of cryptographic protocols have shown to be very useful to the development of real systems[6].

Evaluation Criteria is usually presented as a set of parameter thresholds that must be met for a system to be evaluated and deemed acceptable. These criteria are established based on a Threat Assessment to establish the extent of the data sensitivity, the security policy, and the system characteristics[7]. The system is evaluated, the evaluation is measured against the criteria, and then an assessment is made of whether or not the system security assurance is high or low.

1. TCSEC or Trusted Computer System Evaluation Criteria:

This is a standard set by DoD (United States Government Department of Defense) regarding basic needs to assess the effectiveness of security controls of companies, which are built into computer systems. It was used for evaluation, classification, and selection of computer systems which were considered to process, store and retrieve classified or sensitive data[8].

2. ITSEC or Information Technology Security Evaluation Criteria:

This is a structured criterion set to evaluate the security of computer systems as well as related products. It was established for the first time in May 1990 based on the work done in the UK, Netherlands, Germany, and France. Consequently, it was started first in these countries. In June 1991, an extensive international review was published (Version 1.2) for operational use in certification and evaluation systems of the Commission of the European Communities. ITSEC evaluation validity has been recognized by many European countries since 1990.

The product or system being evaluated, called the *target of evaluation*, is subjected to a detailed examination of its security features culminating in comprehensive and informed functional and penetration testing. The degree of the examination depends upon the level of confidence desired in the target. To provide different levels of confidence, the ITSEC defines *evaluation levels*, denoted E0 through E6. Higher evaluation levels involve more extensive examination and testing of the target[9]. The ITSEC did not require evaluated targets to contain specific technical features in order to achieve a particular assurance level. For example, an ITSEC target might provide authentication or integrity features without providing confidentiality or availability. A given target's security features were documented in a *Security Target* document, whose contents had to be evaluated and approved before the target itself was evaluated. Each ITSEC evaluation was based exclusively on verifying the security features identified in the Security Target.

3. CTCPEC or Canadian Trusted Computer Product Evaluation Criteria:

This standard of computer security was published by the Communications Security Establishment in 1993 to offer an evaluation criterion to different IT products. It can be regarded as a combination of the TCSEC and ITSEC.

4. CC or Common Criteria for Information Technology Security Evaluation :

CC was prepared predominantly by unifying the above-mentioned pre-existing standards (TCSEC, ITSEC, and CTCPEC) to make sure that companies selling computer-related products for government departments (particularly for use in Defense and Intelligence) may have a standard set to be evaluated against. The development of CC was done jointly by the governments of the UK, the U.S., the Netherlands, Germany, France, and Canada. It is taken as the international standard (ISO/IEC 15408) regarding computer security certification.

CC is more of a framework where users of the computer systems can state their requirements related to security functions and assurances, i.e. SFRs and SARs respectively by using the Protection Profiles or (PPs). Through PPs the vendors can actually make claims and/or implementations regarding their products' security attributes. Moreover, the evaluation of the products can be done through testing laboratories to determine whether the products are truly meeting the claims. In a real sense, CC provides the assurance that the specification process, its implementation, and evaluation of the products related to computer security have been carried out through rigorous and standard protocols in a repeatable way at a level corresponding or analogous to the target environment for actual use.

Conclusion

IT systems and smart devices are nowadays part of our daily lives. They perform variously sophisticated, and sometimes safety-critical tasks.

Security has a direct impact on safety. Lack of security can cause loss of reputation, loss of revenue, and even liability claims.

so we conclude that A security evaluation is a crucial part of high-quality system development. With a security evaluation during the development process, threats can be detected and corrected early. But also after the end of a project, a security evaluation can be useful to know existing threats and potential vulnerabilities of your system, to avoid them in future systems.

All the first three evaluation systems are to some extent obsolete or outdated and currently replaced by a more modern approach known as the Common Criteria model, which offers similarly-defined evaluation levels, implementation of evaluation concept target, as well as the document of Security Target[8].

References

https://www.uniassignment.com/essay-samples/information-technology/importance-of-information-security-in-organizations-information-technology-essay.phpابستراکت

https://www.encyclopedia.com/computing/dictionaries-thesauruses-pictures-and-press-releases/security-evaluation ابستراکت

[6]https://link.springer.com/referenceworkentry/10.1007%2F978-1-4419-5906-5_224
[7] https://link.springer.com/chapter/10.1007/978-0-387-35586-3_6
[8]https://resources.infosecinstitute.com/category/certifications-training/cissp/domains/security-engineering/security-evaluation-models/#gref
[9]https://en.wikipedia.org/wiki/ITSEC