Security Controls for Database Technology and Applications

Zoltán Kincses
Eötvös Loránd University of Sciences, Hungary

INTRODUCTION

The word *security* has many meanings, even for the programmers and other members of the computer science community, but it is often inferred by frequently used keywords, such as *threat*, *vulnerability*, *exploit*, *risk*, and related expressions such as *attack*, *circumvention*, *manipulation*, *sniffing*, *denial of service*, *malicious*, *privacy*, and so forth.

Every system is at risk of being attacked, and the risk analysis of the system will discover the severity of these risks, the protection measures, and their efficiency. There may be situations in which the risk analysis concludes that the system is not well protected against an attack, or even that new risks arose during a periodical analysis. The important thing is to implement the analysis and, based on the results, decide how to proceed with the next steps.

Without the risk analysis there is no guarantee that all the protections will be sufficient, and the owner or maintainer of the system will be consciously regarding the security of the system. We can conclude, therefore, that *security is conscious risk taking*.

WHAT IS INFORMATION SECURITY?

Information security can be defined in different ways, depending on the starting point. The word *security* has different meanings for society, for the government, for a citizen, for a mother, for a company leader, for a developer, for a user, or even for a hardware object. The specific rules for information security can be learnt from good books and descriptions found on the Internet.

The “security way of thinking,” however, can be learnt from a fewer number of books, publications, and newsletters (see, e.g., Anderson, 2001; Schneier, 1996, 2000, 2003). Beginners should, and professionals may, read these papers before editing configuration files, using security applications, and applying security protocols, procedures, and policies to their systems.

Information security is realized through settings and installations, but without built-in concepts of the security policies (i.e., concepts built in from the beginning, in the planning state of the system), information security has less value and, in many cases, is worthless because of the bad concept. As Schneier explained, “security is a process, not a product.” But he also says that “security is a trade-off”, therefore we must be careful with applied security measures.

Security is a conscious risk taking, and, based on this idea, security means that the manager (user, developer, etc.) must consciously manage the risk of the system. Risk can be managed with the cycle of monitoring (MO), planning and organization (PO), acquisition and implementation (AI), and delivery and support (DS) processes defined by the ConIT system (Information Systems Audit and Control Association [ISACA], 2003). In this system the control measures can be placed, which will help us find possible security problems.

The relations among the security parameters (technical and managerial) and their effect on each other is shown in Figure 1.

MAIN THRUST OF THE CHAPTER

Controls will help us find possible security problems in a system. The best controls are *preventive*, followed by *detective* controls. At the least, *corrective* controls must be provided, because the business continuity is served in that way (Stoneburner, Goguen, & Feringa, 2002).

Additional controls exist, such as administrative controls, but this article will detail only the three previously introduced. Administrative controls have a strong relation to the quality assurance system (i.e., ISO9001 series), because the existence, the content, and the form of policies, documentations, and instructions are regulated by that standard. After introducing such a system, it is easier to complete the system with the security-related parts.

Samples and Rules

A sample of controls, and their types, are picked from different areas of everyday life, and include locks (preventive control), house alarms (detective control), and
insurance (corrective control). Samples from IT systems include firewalls (preventive control), intrusion detection systems (detective controls), and backup systems (corrective control).

Which security tool or defence technique can resolve certain controls, and which security tool or defence technique implements certain control or controls? The answer to these two questions must produce the same result at the end of the system’s security planning. If we consider the two sets of controls (C) and tools (T), then the C → T relation must fulfil the following rules:

1. ∀ t ∈ T, ∃ c ∈ C: C(c) → T(t) and
2. ∀ c ∈ C, ∃ t ∈ T: C(c) → T(t)

The first rule means that in set of tools there are no unused tools, and the second rule means that in set of controls there are no unsupported controls by at least one tool. In many-to-many relations, the segregation of duties must be applied, which means the avoidance of overlapping. It is not very efficient to use two virus scanners on a computer or think that every control can be supported by one universal tool. Of course, well-considered cases can be suitable (e.g., one firewall can stop e-mails that contain viruses or can have intrusion-detection system features).

Multiple controls and separate tools can be applied on different levels (e.g., a virus scanner can be on a firewall and on a single computer, also). The borders of the levels must be defined in advance, and every change in the borders or in the level membership of the computer must be followed by an audit, the topic of which is the consistency of the system and its security. The result may be that the change cannot be done in that way or that additional controls must be applied to ensure consistency.

**Threats**

The control measures concern the basic threats to the system. There are three basic threats: confidentiality (C), integrity (I), and availability (A).

Confidentiality means that unauthorized users or processes cannot access the protected information (e.g., data, application, configuration settings, operating system, network). Considering the information life cycle, from its appearance till the unrecoverable removal, confidentiality exists only till the first unauthorized access. The accesses can be controlled by authentication and authorization (preventive), or by access alerter and monitoring the access logs (detective). The corrective control also could start with the monitoring of access logs and, in case of unauthorized access, the cause must be eliminated. Unfortunately, many or all parts of the information system might become nonconfidential, that is, only the new entries after the elimination of the unauthorized access possibility can be treated as confidential.

Confidentiality generally can be resolved with encryption techniques. Symmetric encryption ensures that only those users who possess the key for the access can access the information. If it is necessary for only one user to access the information, then an asymmetric or public key encryption system can be used. In the case of managing many users and public keys, the public key infrastructure (PKI) is used.

For database technologies and applications, this means that in case of unauthorized access or manipulation, the manipulated data must be replaced with the original data. In case of unauthorized access, the data confidentiality cannot be restored, but the confidentiality of new entries can be resolved by replacing the insufficient confidentiality control with a sufficient one.

Integrity means that the information was not modified in part or in whole. The integrity can be checked with the backup copy, but there are also encryption techniques for this problem. The hash algorithms with one-way function methods produce a standard output from any input, and the probability of having the same the output values from two inputs is very low. This short
Related Content

Where Do Time Constraints Come From? Where Do They Go?
[www.igi-global.com/article/time-constraints-come-they/51161?camid=4v1a](www.igi-global.com/article/time-constraints-come-they/51161?camid=4v1a)

An Evaluation of UML and OWL Using a Semiotic Quality Framework
Yun Lin, Jennifer Sampson, Sari Hakkarainen and Hao Ding (2005). *Advanced Topics in Database Research, Volume 4* (pp. 178-200).
[www.igi-global.com/chapter/evaluation-uml-owl-using-semiotic/4374?camid=4v1a](www.igi-global.com/chapter/evaluation-uml-owl-using-semiotic/4374?camid=4v1a)

Concurrency Control for Replicated Data in Distributed Real-Time Systems
[www.igi-global.com/article/concurrency-control-replicated-data-distributed/51162?camid=4v1a](www.igi-global.com/article/concurrency-control-replicated-data-distributed/51162?camid=4v1a)

A Study of Open Source Software Development from Control Perspective
[www.igi-global.com/article/study-open-source-software-development/49722?camid=4v1a](www.igi-global.com/article/study-open-source-software-development/49722?camid=4v1a)