PART 1

Network Security Risk Assessment

1

Introduction to Information System Security Risk Management Process

Currently, network security is an important part of a network design process. Information System Security Risk Management (ISSRM) allows network engineers to maximize the network security level they want to achieve. Usually, ISSRM processes follow an overall framework composed of classical and common steps. Nevertheless, these steps can differ from one method to another and do not necessarily put the same weight on each step. For instance, some methods focus on security controls and countermeasures whereas others put more effort on risk assessment and treatment procedures.

However, a general ISSRM framework can be drawn and considered as a basis for any information security management-related work, as illustrated in Figure 1.1.

This general ISSRM framework is composed of six steps:

a) *Context and asset identification*: first, the communication system and its environment are described with an emphasis on the sensitive assets (devices, data, etc.) to protect.

b) *Security objectives identification*: security needs are then defined. Based on the previous step, security objectives are usually expressed

in terms of basic security services (confidentiality, authentication, integrity, non-repudiation, availability and authorization).

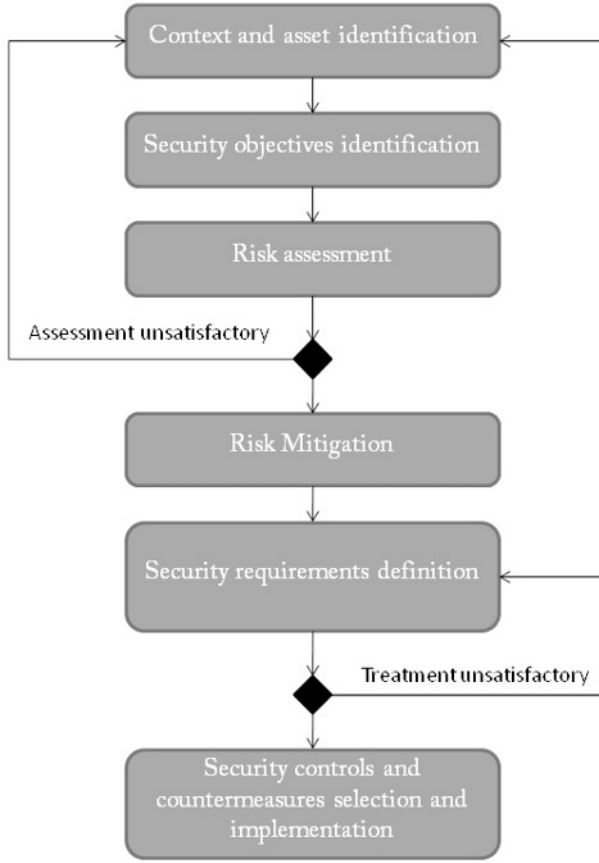

Figure 1.1. *General information system security risk management process*

c) *Risk assessment*: this step consists in estimating potential risks that can harm the assets identified in step (a) and threaten the security objectives of step (b). The risk assessment procedure can be based on a qualitative or quantitative study. Note that if the risk assessment is

unsatisfactory, it could be possible to go back to previous steps and restart the analysis.

d) *Risk mitigation*: once the risk has been clearly identified, risk treatment actions can be taken. For instance, such a measure could be to decide to retain the risk (e.g. accept the risk because it is considered low enough), reduce it (e.g. reinforce security policies) or avoid it (e.g. deactivate a risky network device).

e) *Security requirements definition*: security requirements can now be determined as security solutions to mitigate the identified risks, mainly if the risk reduction strategy has been chosen.

f) *Security controls and countermeasures selection and implementation*: finally, security requirements are instantiated into explicit security controls and countermeasures. For instance, firewalls have been selected to protect the aeronautical network we consider in the case study developed in Chapter 5 of this book.

1.1. On the importance of network security for network designers

Network security is a critical step in IT network and system design. Security countermeasures (firewalls, virtual private networks (**VPNs**), authentication, authorization and accounting (**AAA**) servers, etc.) are the first protection layer against threats and malicious actions targeting the system resources. In order to provide an effective and robust network, a sound risk analysis and a well-thought security policy are required. Hence, before deploying the network security system, network designers have to carefully think about security by respecting the following guidances:

– Security has to be a *built-in* feature instead of a *built-on* ingredient to be added when security issues begin to show up.

– Several layers of security should be deployed in order to complement each other when needed (e.g. if a firewall goes offline, another firewall will be able to provide data flow filtering). Also, security devices should be physically located into different entries of the network in order to avoid a single "point of failure". This is usually called "*defense-in-depth*" security.

– IT system resources should be dispatched into different security demilitarized zones (**DMZs**) according to their sensitivity and criticality.

– Intrusion prevention systems (**IPS**) are different from firewalls and should be used because they do not perform the same role: IPS devices are about intrusion detection for later effective actions whereas firewalls are about monitoring traffic flows, compartmentalizing the network infrastructure, and controlling the communications.

– Network security should not be limited to security devices only, it should be extended to other network management and configuration tasks (e.g. setting configuration files on network devices, monitoring resource consumption activities, analyzing logging events).

– A good network security design necessary goes primarily through an efficient risk analysis and vulnerability assessment that focuses on most critical resources in the system and highlights the security flaws to be considered later when the network is effectively designed.

1.2. On the impact of risk assessment in the decision-making process for network security designers

This very general picture of the ISSRM process highlights the importance of the intermediate risk assessment step, generally considered as the nucleus of risk management processes' lifecycle. As a matter of fact, next steps, such as security controls and countermeasures implementation, highly depend on the success of the risk assessment step. For instance, if the risk has been overestimated, administrators will likely implement high-cost protection devices to mitigate a risk that actually necessitates cheaper equipments.

Many approaches can be used to evaluate the risk related to information and network security systems. Most often, the security risk is expressed as:

$$Risk = Likelihood * Impact \qquad [1.1]$$

Indeed, risk assessment is usually conducted on the basis of threat likelihood and impact, which are, respectively, the probability of a threat occurrence and its potential damages to the system. A threat is defined as the possibility for an intruder to attack a system by exploiting existing vulnerabilities. However, this is one general expression among many, and as involved factors (e.g. likelihood, impact) could be modeled in many ways, numerous security risk assessment methods have already been proposed as described in section 1.3 and in Chapter 2.

1.3. Quantitative versus qualitative risk assessment approaches

As we mentioned in step (c) of Figure 1.1, risk assessment techniques can be undertaken in a quantitative or qualitative approach.

Typically, qualitative risk assessment relies on security specialists expertise and, most of the time questionnaires are used to gather their opinions, like in [BEN 92]. This can be costly as security expertise is expensive for companies. Furthermore, a data collection process is considered complex as it requires much time and effort, and might induce some computation errors (because they are performed manually). Besides, the qualitative results are mostly based on a ranking scale, and cannot be substantially evaluated because of their subjective nature.

For instance, it is possible to compare two security risk levels (e.g. between high and low) but impossible to estimate the distance between these measures (e.g. between two levels ranked as high). Moreover, the security expertise is generally based on the expert's intuitiveness and past experiences in the field, which does not always reflect the current and real situation. Then, qualitative risk assessment techniques likely suffer from a lack of sound theoretical bases, which do not give concrete knowledge about the information security risk.

Quantitative risk assessment allows a more accurate analysis of risk events and, to some degree, solves the issues related to qualitative techniques. In fact, a plethora of parameters involved in the risk

assessment process can be used and are designed in many ways owing to mathematical and theoretical models. For instance, some designers might focus on modeling the impact of threats on business assets, whereas others decide to concentrate their efforts on attack progression modeling using Petri's network [JIN 09]. This allows a sharper analysis of risk events compared to qualitative techniques.

Besides, the quantitative results are mostly accurate and can be expressed either in business or technical languages. Thus, this makes it easier for enterprises to reach their financial objectives. Furthermore, it could be helpful for administrators willing to enhance the security of their networks. Quantitative risk assessment methods are usually supported by automated tools, which have the advantage of accelerating the assessment process and avoiding some computational errors.

Furthermore, quantitative risk assessment techniques can be used either for a preventive risk analysis or a reactive risk analysis depending on the context of the study. A preventive risk analysis often relies on the annual loss expectancy (**ALE**) index [MIC 04], which is the annual monetary loss that can be expected by a company according to the identified likely risk events. From a financial point of interest, ALE is an important metric that can be used directly in a cost-benefit risk analysis.

Quantitative risk assessment techniques also support reactive analyses, which are generally conducted to identify security countermeasures when an alert corresponding to an attack is triggered by a monitoring system. This could be done using, for instance, a NIDS system. For this purpose, several decision criteria are used and modeled in various ways. The most prominent models are detection and reaction cost models (e.g. the number of security countermeasures to deploy, the percentage of intrusions into the supervised network, the monetary or processing resources required to face an attack) [BAR 09], attack models (e.g. scenarios-based or tree-based graphs) [WIN 08], and threat impact models (e.g. impact distribution laws, impact progression over the network) [LAO 08].

Succinctly, qualitative and quantitative information security risk assessment approaches could be compared from three points of view: subjectivity, efficiency and cost. Table 1.1 depicts a summary of the advantages (denoted by +) and drawbacks (denoted by −) of each approach according to these three axes.

Criteria	**Quantitative Approaches**	**Qualitative Approaches**
Subjectivity	− At a design level + Solid theoretical models + Several factors are modeled	− Security experts intuitiveness and past experiences − Pedestrian risk evaluation
Efficiency	+ Numerical risk estimation (comparison is always possible) + Automated procedures/ tools (less errors) − Based on advanced aspects (not adapted for beginners)	− Ranking scale (difficult to compare) − Computation errors (human in the loop) − Preventive/reactive analyses are difficult to conduct
Cost	+ Relatively fast (only time needed by the tool) + No extra-expense	− Time-consuming procedures (e.g. questionnaires collection) − Financially expensive

Table 1.1. *Qualitative versus quantitative risk assessment approaches*

Looking at the comparison made above, it makes sense to confirm that a quantitative risk assessment approach is strongly preferred. A lot of work has been done in this area and we provide further a summary of the major research in this field (section 2.2).

Consequently, our methodology will be based on a quantitative assessment of each parameter involved in the global risk processing. However, the survey of these quantitative risk assessment methods emphasized another point that should be considered when the so-called

risk assessment methodology has to be designed for an information system network, namely the network security risk propagation.

1.4. Network security risk propagation concept

1.4.1. *Impact of node correlation*

To understand the importance of the network security risk propagation concept in the design of a risk assessment methodology, let us see what could be the simplest definition of the word "network". According to the online Cambridge Dictionary, it is "*a large system consisting of many similar **parts** that are **connected** together to allow movement or **communication** between or along the parts or between the parts and a control centre*"[1]. Starting from this definition, we can deduce three important concepts that must be considered carefully when a risk assessment method has to be designed for a network information system:

– *Nodes*: these are the main components of a network information system, such as end systems (terminals, servers) and intermediate systems (hubs, switches, gateways). Every node has its own set of vulnerabilities that can be related to hardware, software, protocol stack, etc.

– *Physical interconnection between nodes*: as we have seen in the definition, nodes are interconnected by physical supports in a network. For example, nodes can be interconnected using cables (shielded twisted pair cable for instance) in a wired LAN or radio waves in a wireless LAN (**WLAN**) such as WiFi.

– *Communication (i.e. data flows) between nodes*: some nodes are able to provide services (FTP (File Transfer Protocol) transfer, HTTP (HyperText Transfer Protocol) browsing, database access, etc.). When two nodes want to communicate together, they must be interconnected physically and logically.

1 http://dictionary.cambridge.org/dictionary/british/network_1

Considering all these factors, it is not easy to deduce exactly the total risk of a large network, even if we can evaluate this risk node-by-node. In fact, apart from individual vulnerabilities, the global network security can be seriously compromised by the interconnected nodes. Indeed, many endogenous and exogenous factors have to be analyzed in order to determine as accurately as possible the risk level for the whole network.

On the one hand, the global network risk can be very low even if the risk related to a single node is very high (e.g. this node is isolated from the rest of the network and does not communicate with many other nodes). On the other hand, the security of the whole network can be heavily compromised by nodes that have strong interconnections and data flow exchanges with the rest of the network, even if those nodes have individually a low network risk.

Therefore, a network security risk should no longer be evaluated individually, but rather globally taking into account the service dependencies and node correlation. The security risk propagation within an information system network consolidates this idea that network intrusions are likely transitive processes.

1.4.2. *Network security risk transitivity*

When an attack occurs on a network node, it is highly likely that the intruder will try to attack the interconnected nodes when this is allowed by the network topology. The attacker would be able to do so if there were some system assets that could help him to break into a connected node. These assets could be applications, services (intruded on the associated port), user logins (e.g. root privilege access) or database access accounts. Strong dependencies between these system facilities imply some kind of transitivity in the network risk propagation process.

By way of an example, let i and j be two correlated nodes in the network and t an exploitable vulnerability on node j as shown in Figure 1.2.

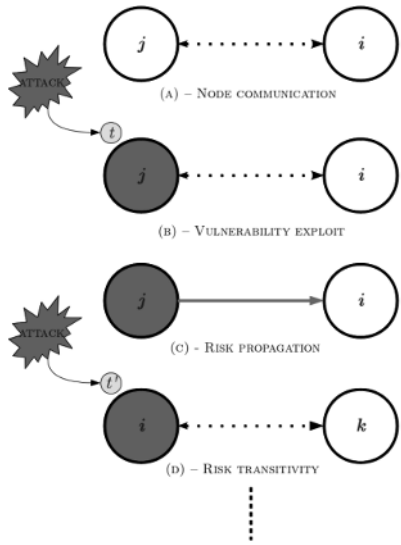

Figure 1.2. *Risk transitivity between correlated nodes*

Since node *j* has some vulnerabilities that could be exploited by an attack (step B), it might transmit its correlative risk to the connected node *i* (step C). This risk will propagate to the different nodes connected with node *j*. Besides, as long as the risk has been propagated from node *j* to the correlated node *i*, there is a strong probability that the intruder continues along his way and tries to break in to nodes connected with *i* (node *k* in step D). To provide a deeper understanding of the network security risk transitivity, we illustrate the risk propagation concept through a practical intrusion scenario in the following section.

1.4.3. *Network security risk propagation illustrative case*

Figure 1.3 illustrates an example of a step-by-step network security risk propagation into a simple LAN network. Let us say that administrator users on node A are allowed to log on a Web server (node B) using the Secure SHell (SSH) [YLO 06] service in order to manage a Website and refresh its content. Users possessing root privileges on node B are allowed to access a database (node C) that

contains confidential data (e.g. Website user information like emails, credit cards, addresses). Only root users on node B are allowed to access the database on node C: for this purpose, a firewall (node D) is deployed and configured to filter the access to node C, meaning users from node A (even those with administrator privileges) are prevented from logging in to the database.

However, node A could suffer from a vulnerability that is still exploitable (i.e. not already fixed). An intruder may first exploit this specific vulnerability to node A (e.g. Operating System (OS) vulnerability) to get administrator privileges. He would probably face some issues trying to access directly node C from node A, but he could gain access to node B using the SSH service. In a second phase, he may try to grant root privileges on node B, then access the confidential data on node C without being intercepted.

In this section, we turned our attention to a second point of interest in network security risk assessment, namely the risk propagation. We showed that a risk should not be considered under a classical perspective (i.e. individually node-by-node), but instead at a higher level such that the impact of node correlation is taken into account in the risk computation.

The methodology presented later takes into consideration both quantitative assessment and risk propagation concepts. The proposed approach could help administrators willing to compare different security policies and find a cost-effective and secure policy. Besides, they will be able to evaluate the impact of any topological change in the network architecture (e.g. adding or deleting a node) on the network security. All the parameters involved in the network risk measurement will be explained and quantified: threat likelihood, risk impact (i.e. cost of damages), individual network risk (i.e. specific to a single node) and the total risk induced by the interconnection between the network components.

As the reader may notice, this methodology can be applied to any computer network and is not specific to a particular environment. Since

we are able to quantify the logical interconnection between network nodes, the security assessment framework would fit to measure the risk on that network. While specific characteristics (such as priority between network domains) have been included to support data link communications, the aeronautical network remains the case study of the presented methodology as we will see in the dedicated section.

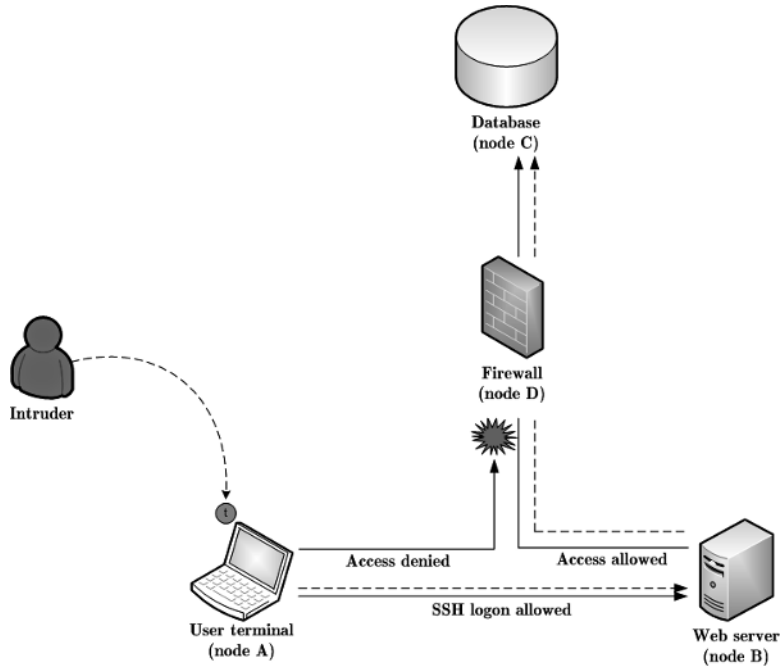

Figure 1.3. *Network security risk propagation example*

In Chapter 5 of this book, we apply our approach on the SESAR network architecture. In this context, we focused on the AeroMACS access network topology for airport communications. The goal was to discuss the risk results for the isolated AeroMACS scenario and to compare them regarding the intrinsic authentication/authorization security mechanisms in order to finally find which scenario holds the lowest network risk and to provide at the end some security guidances for future AeroMACS implementations.

The validation experiments relied on vulnerability statistics issued from the National Vulnerability Database (NVD)[2] and the Common Vulnerabilities and Exposures (CVE) database published by the National Institute of Standards and Technology (NIST). The NVD provides information about vulnerabilities such as type, class of severity and scores, extended descriptions, products or versions affected. Other vulnerability and statistical reports exist such as Secunia[3] or OSVDB (Open Source Vulnerability Database)[4] database: we picked the NVD database because it provides the Common Vulnerability Scoring System (CVSS) [SCH 05] severity score of a vulnerability, which is an essential quantitative parameter in our methodology.

2 http://nvd.nist.gov/

3 http://secunia.com/

4 http://osvdb.org/