Chapter 24
The Rigorous Security Risk Management Model: State of the Art

Neila Rjaibi
Institut Supérieur de Gestion de Tunis (ISG), Tunisia

Latifa Ben Arfa Rabai
Institut Supérieur de Gestion de Tunis (ISG), Tunisia

ABSTRACT

This chapter presents the security concepts terminologies (threat, risk, security risk management, security risk management process, security threat model) and present the state of the art of security risk management models, compare and discuss strengths and weaknesses of such models. Then it presents the Mean Failure Cost (MFC) model for quantifying security threats as a rigorous measure of cyber security, and as a cascade of linear models in order to estimate the system security using the loss of a given stakeholders as a result of security breakdown. Finally it presents an overview of the applicability of the MFC measure to e-systems. In the conclusion, the chapter criticizes the MFC Cyber Security Measure and presents an overview of different perspectives.

INTRODUCTION

Actually the Internet is the main source of all threats and illegal activities. Consequently, E-systems are threatened exponentially, statistics have shown that organizations are currently investing in security resources. It has been shown that through 2005 the total global revenue for security products and service vendors amounted to $21.1 billion. Another source indicated that from 1999 to 2000, the number of organizations spending more than $ 1 million annually on security nearly doubled. So, expenditures have increased from 12% of all organizations revenues in 1999 to 23% in 2000 (Ekelhart et al., 2009). In fact, it is a challenging task for organizations to put the emphasis on security risk management in order to measure and assess security risk and provide a good plan for risk mitigation.

DOI: 10.4018/978-1-5225-5634-3.ch024

They are obliged to put emphasis on security risk management in order to measure and assess security risk and provide a good plan for risk mitigation.

This chapter:

- Presents the security concepts terminologies (threat, risk, security risk management, security risk management process, security threat model)
- Presents the state of the art of security risk management models, compare and discuss strengths and weaknesses of such models
- Presents the MFC model for quantifying security threats as a rigorous measure of cyber security, and as a cascade of linear models in order to estimate the system security using the loss of a given stakeholders as a result of security breakdown.
- Presents an overview of the applicability of the MFC measure to e-systems
- Criticizes the MFC Cyber Security Measure and present an overview of different perspectives.

SECURITY TERMINOLOGIES

The Threat Concept

In the first step it is necessary to define the term 'risk' and 'threat' because there is an important distinction between them. According to Bruce Schneier (2003) a threat is defined as: "a potential way an attacker can attack a system". Commonly known, threats for computers are viruses, network penetrations, theft and unauthorized modification of data, eavesdropping, and non-availability of servers.

A threat is also defined as a category of object, person or other entities that present a danger. Like spam, Trojan horse and fishing (Whitman & Mattord, 2004 ; Stoneburner et al., 2002).

The Risk Concept

A risk is the product of the probability that a particular threat will occur and the expected loss.

According to Bruce Schneier (2003), when we talk about risk, it is the likelihood of the threat and the seriousness of its successful attack. For example a threat is more serious because it is more likely to occur.

Another definition supported the same concept than the product of the financial losses associated with security incidents and the probability that they occur. The risk of security threat as a quantitative measure is a suitable input to decision making (Ryan & Ryan, 2006; Tsiakis & Stephanides, 2005; Mili & Sheldon, 2009; Sommestad et al., 2010). Therefore the purpose of considering risk as a financial measure leads to making decision from business perspective. For example, the return on security investment: ROI measure (Aissa et al., 2010 a; Cavusoglu et al., 2004; Bojanc & Jerman-Blazic, 2008) and the mean failure cost: MFC measure presented in (Mili & Sheldon, 2009; Aissa et al., 2010 a; Aissa et al., 2010 b).

Finally, security is defined as the inverse of risk, because there is a secure system when nothing happens, risk refers to the loss but it is a concept that is difficult to measure (Ryan & Ryan, 2006).