Assessing the Risk of an Information Infrastructure Through Security Dependencies

F. Baiardi[1], S. Suin[1], C. Telmon[1], and M. Pioli[2]

[1] Dipartimento di Informatica, Università di Pisa
[2] Enel Distribuzione, ENEL
{f.baiardi,stefano}@unipi.it

Abstract. We outline a framework for the risk assessment of information infrastructures that generalizes the notion of dependency with respect to security attributes such as confidentiality, integrity or availability. Dependencies are used to model an infrastructure at distinct abstraction levels, to discover attack strategies and to define risk mitigation plans. A plan is formulated in terms of set of countermeasures because single countermeasures may be ineffective due to alternative threat attack strategies. We do not detail the assessment steps and focus on the integration of their results to define risk mitigation plans. Lastly, we discuss the development of programming tools to support the assessment.

Keywords: risk assessment, mitigation plan, countermeasure, vulnerability, ranking.

1 Introduction

The output of a risk assessment of an ICT, or information, infrastructure [1,3,5,6] is a risk mitigation plan that defines the countermeasures to be applied to reduce the risk at an acceptable level for the owner. Risk is formally defined as the product of the probability of a successful attack and of the corresponding impact, the damage due to the attack. If vulnerabilities are known, then each vulnerability V may be paired with the risk it introduces because of the attacks it enables. The return of the investment to remove V [8] is the difference between this risk and the investment. The problem posed by this approach is that the probabilities it requires can be determined only if historical data about the infrastructure are available. For most information infrastructures this is seldom the case. Furthermore, to mitigate risk, several countermeasures have to be applied simultaneously because of alternative attack strategies that compose simple attacks into mo! re com plex ones [2,11,15,16]. Hence, the return of removing a single vulnerability cannot be easily estimated and approximated strategies are adopted. These strategies rank vulnerabilities to define a optimal order to remove them, i.e. to apply the corresponding attack countermeasures [3,13].

We present an approximated risk assessment strategy for an information infrastructure that defines cost effective risk mitigation plans by composing set of countermeasures rather than single ones. The framework models an infrastructure as a set of interdependent components, each defining a set of operations

J. Lopez (Ed.): CRITIS 2006, LNCS 4347, pp. 42–54, 2006.

working on an internal state and that are invoked by some users. Three attributes for each component are introduced, namely confidentiality, integrity and availability. Each may be controlled by invoking some component operations. The relations among components are described by security dependencies [3,10,9]. A security dependency involves some source components, a destination one and a security attribute for each component. The meaning is that the control of the attributes of the source components implies that of the attribute of the destination one. The infrastructure is modeled as a labeled hypergraph with a node for each component and a hyperarc for each dependency. The number of hyperarcs and of nodes depends upon the abstraction level of the model. Security dependencies are inspired to cascade failures and domino effect models [3,13]. Several approaches and tools have exploited this notion, sometimes without introducing it in an explicit way. An excellent survey of approaches and tools is [9]. To the best of our knowledge, our approach is the one that exploits this notion at distinct abstraction levels, according to the detail level of the assessment.

Sect.2 of the paper defines the modeling of the infrastructure, of attacks and threats. Sect.3 introduces the notion of minimal set of countermeasures. Sect. 4 defines the ranking of countermeasures and the deduction of mitigation plans. Sect.5 and 6 discuss, respectively, the notion of risk and the development of programming tool to assist the assessment. Important analyses such as the vulnerability or the impact ones will not be described, as their methodologies are fully orthogonal to our framework that aims to integrate their results to define a cost effective risk mitigation plan.

2 Modeling Infrastructures, Attacks and Threats

This section describes the modeling of entities of interest.

2.1 Component Dependencies and Infrastructure Hypergraph

The framework models the infrastructure as a set of interdependent components, each consisting of some internal state and of the operations it implements. Three security attributes of a component are considered:

1. confidentiality. Its control implies the ability of reading the component state;
2. integrity. Its control implies the ability of updating the state;
3. availability. Its control implies the ability of managing the component, i.e. of determining the users that can invoke its operations.

The framework does not describe the state or the operations and represents user rights as a set of pairs $\langle component, attribute \rangle$, where attribute $\in \{c, i, a\}$. A user controls an attribute because of either the component operations it can invoke or dependencies from other components. Each security dependency, or simply dependency, is characterized by the source components from where it originates, by a destination one and by a security attribute for each component. Distinct dependencies correspond to alternative ways of controlling an attribute.

A first example of dependency is the one between a password and the resources it controls. Anyone that controls the password confidentiality, i.e. can read it,