Rational Choice of Security Measures Via Multi-parameter Attack Trees

Ahto Buldas[1,2,3,⋆], Peeter Laud[1,2], Jaan Priisalu[4],
Märt Saarepera[5], and Jan Willemson[1,2,⋆⋆]

[1] Cybernetica, Akadeemia tee 21, Tallinn, Estonia
[2] University of Tartu, Liivi 2, Tartu, Estonia
{ahto.buldas,peeter_l,jan}@ut.ee
[3] Tallinn University of Technology, Raja 15, Tallinn, Estonia
[4] Hansapank, Liivalaia 8, Tallinn, Estonia
jaan.priisalu@hansa.ee
[5] Independent researcher
marts@neoteny.com

Abstract. We present a simple risk-analysis based method for studying the security of institutions against rational (gain-oriented) attacks. Our method uses a certain refined form of attack-trees that are used to estimate the cost and the success probability of attacks. We use elementary game theory to decide whether the system under protection is a realistic target for gain-oriented attackers. Attacks are considered unlikely if their cost is not worth their benefits for the attackers. We also show how to decide whether the investments into security are economically justified. We outline the new method and show how it can be used in practice by going through a realistic example.

1 Introduction

Rapid growth of society's dependence on computers and the Internet has drawn attention to the vulnerability of this technical infrastructure. Increasing numbers of IT security incidents all over the World have emphasized the importance of risk analysis methods capable of deciding whether an organization (e.g. a company) is sufficiently protected against attacks. The protection mechanisms are often costly, or at least, not for free. Managers of an organization would like the investments into security to be reasonable and worth their price. The security experts should, more and more often, explain to their managers what benefits exactly the organization is getting for the money that is invested into security [1,2].

In contrast to the cryptographic techniques, the IT risk management techniques are still in an embryonic stage. This is one of the reasons of an increasing gap between theory and practice of information security [3]. Occasional stochastic risks (natural disasters, general criminal activity) can be evaluated rather easily, since there is enough statistical data concerning both the frequency (probability) and losses associated with such threats. Targeted gain-oriented attacks are much harder to model because their

⋆ Supported by Estonian Science Foundation grant #5870.
⋆⋆ Supported by Estonian Science Foundation grant #6096.

J. Lopez (Ed.): CRITIS 2006, LNCS 4347, pp. 235–248, 2006.

occurrence does not usually follow any reasonable statistical patterns and they tend to be rather victim-specific, which makes it difficult to find suitable risk metrics for attacks [1].

In the risk management field, risk is mostly defined as an expected loss, which is caused by *threats* – events that are considered bad (namely because they cause losses). Hence, the risk caused by threat $\mathcal{T}$ can be computed by $\mathsf{Risk}[\mathcal{T}] = \mathsf{Pr}[\mathcal{T}] \cdot \mathsf{Loss}[\mathcal{T}]$, where $\mathsf{Pr}[\mathcal{T}]$ denotes the probability of $\mathcal{T}$ and $\mathsf{Loss}[\mathcal{T}]$ denotes the associated loss. Hence, to estimate the security risk of a company we have to find all possible threats $\mathcal{T}$, to estimate the corresponding losses $\mathsf{Loss}[\mathcal{T}]$ and the probabilities $\mathsf{Pr}[\mathcal{T}]$, and finally to sum everything up

$$\mathsf{Risk} = \sum_{\mathcal{T}} \mathsf{Pr}[\mathcal{T}] \cdot \mathsf{Loss}[\mathcal{T}] \ . \tag{1}$$

Once we are able to do so, the security management is a trivial task: (A) compute the risk by (1), (B) if the risk seems to be too high, introduce some measures and compute the risk again, (C) if the cost of the measures is lower than the difference of risks, then decide that the measures are worth their price. Otherwise, the measures are unreasonable because it would be more beneficial not to take any measures.

Unfortunately, such an approach is hard to adopt in practice. Even if we are able to estimate the losses associated with the threats, their probabilities are often very hard to judge. This is especially true for targeted attacks that for a given setting may occur only once. It is also the case that companies are rather reluctant to share information concerning their vulnerabilities and the previous security incidents. For some typical attacks there exist rough expert estimates [4]. However, such estimates can generally be given for elementary vulnerabilities, but not easily to the primary (loss causing) threats. For instance, in [4] we see estimates for the events "Attempted Unauthorized System Access by Outsider", "Abuse of Access Privileges by Other Authorized User", etc., but not for "Loss in Drop of Company's Shares due to Bad Publicity".

Thus, we need a methodology to deduce probabilities of complex attacks from the parameters of simple vulnerabilities. Note that it is insufficient to consider only the occurrence probabilities of the vulnerabilities, since the attacker may consider more parameters when deciding whether to attack or not (e.g. the probability of getting caught and the associated penalties).

One of the methods used in practical security analysis is the *threat tree* method, which has been used in several security-oriented tasks like fault assessment of critical systems [5] or software vulnerability analysis [6,7], and was adapted to information security by Bruce Schneier [8,9]. In order to apply this method, only the rational attackers are taken into account. As the latter ones attack only when the attack is profitable, their behavior can be modeled by estimating the cost of attacks. Threat trees help us when reasoning about the decision-making process of the attackers and they work by splitting complex attacks into simpler and easier to analyze sub-attacks. Hence they are suitable for computing costs and success probabilities of attacks and are useful tools for practical security management.

Even though the threat trees (also called attack trees to emphasize the attack modeling domain) can provide valuable insight to the system's security, their applications have been rather simplistic so far. Most of the reported studies only consider one specific parameter for the nodes like cost or feasibility of the attack, skill level required,