Using Attacker Capabilities and Motivations in Estimating Security Risk

Lotfi ben Othmane
Dept. of Mathematics and Computer Science
Eindhoven University of Technology
Eindhoven, 5612MB, Netherlands
l.ben.othmane}@tue.nl

Harold Weffers
Dept. of Mathematics and Computer Science
Eindhoven University of Technology
Eindhoven, 5612MB, Netherlands
h.t.g.weffers@tue.nl

Martijn Klabbers
Dept. of Mathematics and Computer Science
Eindhoven University of Technology
Eindhoven, 5612MB, Netherlands
M.D.Klabbers@tue.nl

ABSTRACT

Risk of a given threat is a function of the likelihood of exercising the threat and the severity of its impacts. This paper proposes incorporating attacker capabilities and motivations in estimating the likelihood of exercising threats. Attacker capability is the ability to use appropriate means (e.g., knowledge, time, expertise, and tools) and opportunity (e.g., enough time to perform the attack) to exploit the vulnerabilities that could cause the related threat. Attacker motivation is the benefit the attacker gains from successful exercise of a threat.

1. INTRODUCTION

Modern Information Systems (ISs) are getting more complex. For instance, they use more software and hardware components, use services managed and controlled by third parties, use devices controlled by the customers, and are more distributed. Business developers of these ISs aim to leverage the full potential of their systems while minimizing the security risks associated to their use.

Risk is a function of the likelihood of a given threat agent exercising a particular vulnerability, and the resulting consequences (aka impacts) of that event [3]. Risk combines the likelihood and severity estimate of a given threat.[1] The common approach to estimate the likelihood and severity is to evaluate a set of factors for each threat. For instance, to estimate the likelihood of a threat we could use the factors required level of skills and required time to develop an attack.

Technical experts[2] have often difficulty to estimate the likelihood of threats to ISs using the factors they are given. They also find that attacker motivations are conditions for exercising threats, not factors contributing to the likelihood estimate. Our position is to integrate attacker capabilities and motivations in the risk assessment. (We define capability and motivation in the next section.)

We discuss in the following two limitations of the current methods for security risk estimates and we propose an estimation method that addresses them.

2. LIMITATIONS OF THE RISK ESTIMATION METHODS

Risk associated to a threat is measured in terms of likelihood and severity. *Likelihood* measures the expectation that an attacker exercises the threat and *severity* measures the expectation of loss or damage that the threat may cause.

Several methods for risk assessment, such as OCTAVE [1] and NIST SP 800-30 [3] are commonly used to identify the threats to systems and measure their risks. Each of these methods uses a set of factors for the likelihood estimates. For instance, the OCTAVE [1] [3] method uses the factors: motive, which is eagerness to trigger the threat and attack the system; means, such as required skills to execute an attack and difficulty of the attacks; and opportunity, such as existence of vulnerabilities in the system. Also The NIST SP 800-30 [3] [4] uses the factors: capabilities of the attacker, such as resources, expertise, and opportunities to support multiple successful attacks; intent of the attacker, e.g., seeks to obtain critical or sensitive information, undermine, severely impede, or destroy a core mission or business function; and targeting, which is the use of acquired information and perseverance in attacking a specific target.

These methods assume that an attacker is capable of exercising an attack if he/she has the appropriate means and opportunity. Means includes the factors: time taken to identify a vulnerability related to the threat and to develop an attack, required security expertise to exercise the threat, required knowledge of the system, required equipment and tools. Opportunity includes the factor window of opportunity. The assumption may not be true because the attacker needs a specific *capability* to perform a specific attack; that is, the ability to use appropriate means and opportunity (e.g., enough time) required to exploit a vulnerability which

[1] A *threat* is a circumstance or event with the potential to harm a system [2].

[2] We refer to technical experts who know the IS being investigated and have basic knowledge about attacks and threats.

[3] See page 186.

[4] See Appendix D.

Workshop on Risk Perception in IT Security and Privacy, July 24, 2013, Newcastle, UK.

causes the related threat.[5] For example, an attacker who intends to tamper with an embedded device and he/she has physical access to it, does not need the same tools, time, and skills, as an attacker who has only remote access to the same device. A second example is: a security monitoring system that uses sensors to detect movements and send alarm requires the sensors to be placed in locations that potential attackers may reach; that is, potential attackers may have the capability ”physical access to the sensor.” (In this case, the attacker capability is in-built in the architecture of the IS.)

These methods assume also that a potential attacker (eventually) attacks the IS if he/she could perform the attack. This assumption may not be true because a potential attacker, who has the appropriate capability, means, and opportunities to attack the IS does not exercise the threat if he/she does not have a ”sufficient” motivation. For instance, insiders do not, often, perform attacks although they have required capabilities, means, and opportunities to do so because they commonly do not have ”sufficient” motivation to do so, e.g., high monetary reward.

The use of attacker capabilities and motivations increases the detailed information that experts need to collect; which increases the time required to estimate the risks of the threats. However, we believe that the information is crucial to identify the means and opportunities needed for the attack scenarios related to the threats–as we explained above.

In the next section we introduce attacker capabilities and motivations in estimating security risks of IS.

3. INCORPORATING ATTACKER CAPABILITIES AND MOTIVATIONS IN ESTIMATING RISKS

In the following, we discuss how to compute the risk associated to a threat considering the means, opportunity, attacker capabilities and attacker motivations.

Let c_k be the likelihood that an attacker has capability k to exercise threat t. Assume an expert evaluates the n factors $\{Fl_1(t), ..., Fl_n(t)\}$ for t in terms of scores based on his/her knowledge and experience. We compute the likelihood of successful exercise of threat t when the attacker uses capability k by summing up the evaluations of the factors and multiply the result and the capability likelihood, as in Equation 1.

$$S_t^{c_k} = (\sum_{j=1}^{j=n} Fl_j^{c_k}(t)) \times C_k(t) \tag{1}$$

Equation 2 provides the formula for computing the likelihood of successful exercise of threat t denoted by $S(t)$; that is, the maximum of the likelihood of successful exercise of threat t using all possible capabilities. The equation indicates the difficulty of exercising threat t.

$$S(t) = max\{S_t^{c_k}\} \tag{2}$$

Let M_j be a likelihood that a potential attacker has motivation j for attacking the system and triggering threat t. The likelihood of occurrence of threat t, denoted by $O(t)$, is the sum of the likelihoods of the related motivations as indicated in Equation 3.

$$O(t) = \sum_{j=1}^{j=n} M_j(t) \tag{3}$$

Equation 4 provides the formula for computing the risk of a threat t (denoted with $R(t)$), which combines the severity (denoted with $I(t)$) and likelihood of success in triggering the threat t and likelihood of its occurrence. The risk scores could be mapped to risk levels in the scale 0 to 1.

$$R(t) = I(t) \times S(t) \times O(t) \tag{4}$$

For each threat, we average the risk estimates of the experts to obtain the risk of the threat.

The use of attacker capability may affect the risk of a threat. For instance, the risk of service interruption of a banking system could be affected by whether the attacker is remote or local. The financial institution could rate the risk of the threat when caused by remote attackers high (We map risk levels to values: low, medium or high.) because the attacks are frequents although each interrupts the service for a short period of time. However, it rates the risk of service interruption due to power supply low because although the threat causes high losses if it occurs–because the interruption can last for extended period–it expects that it is unlikely to occurs.

4. FUTURE WORK

We used the approach in three projects. The approach helps the technical experts to evaluate the likelihood of threats. However, we currently do not have data to support our position that considering attacker capabilities in estimating the risk helps to get good estimates.

5. REFERENCES

[1] C. J. Alberts and A. Dorofee. *Managing Information Security Risks: The Octave Approach*. Addison-Wesley Longman Publishing Co., Inc., Boston, MA, USA, 2002.

[2] R. Shirey. Internet security glossary, version 2. `http://www.ietf.org/rfc/rfc4949.txt`, aug 2007. RFC 4949 (Informational).

[3] G. Stoneburner, A. Goguen, and A. Feringa. Risk management guide for information technology systems – recommendations of the national institute of standards and technology. `http://csrc.nist.gov/publications/nistpubs/800-30/sp800-30.pdf`, 2002. Special Publication 800-30, accessed in May 2013.

[5] Our definition of capability is different from the common use of attacker capabilities–as in NIST 800-30–which refers to available means and opportunities to perform the attack.