Available online at www.sciencedirect.com

ScienceDirect

journal homepage: www.elsevier.com/locate/cose

Computers & Security

Incorporating attacker capabilities in risk estimation and mitigation

Lotfi ben Othmane [a,*], Rohit Ranchal [b], Ruchith Fernando [b], Bharat Bhargava [b], Eric Bodden [a]

[a] Secure Software Engineering Group (SSE), Fraunhofer Institute for Secure Information Technology, Darmstadt, Germany

[b] Department of Computer Science, Purdue University, West Lafayette, IN 47907, USA

ARTICLE INFO

Article history:
Received 3 May 2014
Received in revised form
26 February 2015
Accepted 4 March 2015
Available online 25 March 2015

Keywords:
Risk estimation
Attack potential
Attacker capabilities
Risk mitigation
Threat
Uncertainty
Empirical research

ABSTRACT

The risk exposure of a given threat to an information system is a function of the likelihood of the threat and the severity of its impacts. Existing methods for estimating threat likelihood assume that the attacker is able to cause a given threat, that exploits existing vulnerabilities, if s/he has the required opportunities (e.g., sufficient attack time) and means (e.g., tools and skills), which is not true; often, s/he can perform an attack and cause the related threat only if s/he has the ability to access related resources (objects) of the system that allow to do so. This paper proposes a risk estimation method that incorporates attacker capabilities in estimating the likelihood of threats as conditions for using the means and opportunities, demonstrates the use of the proposed risk estimation method through two examples: video conferencing systems and connected vehicles, shows that changing attacker capabilities changes the risks of the threats, and compares the uncertainty of experts in evaluating the likelihood of threats considering and not considering attacker capabilities for two experiments. The results of the experiments suggest that experts are less uncertain about their estimations of threat likelihoods when they consider attacker capabilities.

© 2015 Elsevier Ltd. All rights reserved.

1. Introduction

Developing a secure Information System (IS) requires assessing the risks to the IS and mitigating the identified threats. However, organizations have business goals and budget constraints that require addressing only a subset of the threats to the ISs they develop. Thus, they estimate the risk exposures of the threats (A function of the likelihood of the threat and the severity of its impacts (Wheeler, 2011)) and use the information to prioritize addressing the threats (McGraw, 2006).[1] The accuracy of risk exposure estimates leads to more realistic prioritization of the threats and therefore better return on investment.

Security experts produce widely different risk estimates because they have different opinions about the difficulty attackers have in exercising the threats against the system. The high uncertainty in the estimated risk exposure, indicated by

* Corresponding author.
E-mail addresses: lotfi.ben.othmane@sit.fraunhofer.de (L. ben Othmane), rranchal@purdue.edu (R. Ranchal), rfernand@purdue.edu (R. Fernando), bb@purdue.edu (B. Bhargava), eric.bodden@sit.fraunhofer.de (E. Bodden).

[1] Note that the goal of risk estimation is not to produce a set of numbers but to enable ordering the threats (Apostolakis, 2004).

http://dx.doi.org/10.1016/j.cose.2015.03.001
0167-4048/© 2015 Elsevier Ltd. All rights reserved.

the high differences between the estimates, leads the business managers to view the exercise as of uncertain practical value and limits the ability of using the information to prioritize the threats (Boehm, 1991; Bonnette, July 2003; Wheeler, 2011). The main causes of the failure of security assessment according to Hubbard (Hubbard, 2009) are: failure to measure the effectiveness of the proposed method, use of methods that are found to include errors and biases, and do not use methods that are proven to work.

A commonly practiced approach in risk estimation is to identify all possible attack scenarios and estimate their risks (using maximum details). This approach is very costly and is not preferred in business projects. The alternative approach is to use a set of factors for estimating the risks of the threats grouped into classes using specific logic. (The methods we enumerate in this section fall in this category.) For example, the OCTAVE (Alberts and Dorofee, 2002) uses the factor classes: (1) motives to cause the threats; (2) means, which include required skills and knowledge to execute attacks and availability of tools; and (3) opportunities, which include time to perform the attack and number of allowed failed attempts. The factor classes used by NIST SP 800-30 (Stoneburner et al., 2002) are: (1) capabilities of the attacker, such as resources, expertise, and opportunities to perform attacks; and (2) intent of the attacker; that is, perseverance in attacking a specific asset to obtain sensitive information. (The definitions of the terms used in this paper are summarized in Table 1). Unfortunately, there is little formal guidance about the selection of the factors to use in the estimation models (Pardue et al., 2009).

Risk estimation methods, currently, separate the treatment of insider threats (violations of security policy by misusing granted privileges (Yasinsac, 2010).) and non-insider threats. However, in many cases, the same threat could be performed by insiders (entities that have access to data or resources (Bishop and Gates, 2008)) and non-insiders. For instance, an attacker who intends to cause the threat "interruption of a security camera of a corporation" and knows how to push the power off button of the camera, or knows how to cut the communication cable, cannot cause the threat unless s/he has the capability "physical access to the camera," where *attacker capability* is the ability to access a set of resources (objects) of the IS to exercise threats. Also, an attacker who plans to exercise the same threat and has time, expertise, knowledge, and tools to craft command messages to the camera to power it off cannot cause the threat unless s/he has the capability "inject messages to the network of the organization." Thus, attacker capabilities often conditions the use of acquired means and opportunities to cause threats (ben Othmane et al., 2013a).

Existing risk estimation methods commonly consider attacker capabilities as the resources (e.g., malware, scripts), knowledge, and expertise that could be used to cause threats, e.g., (Stoneburner et al., 2002). However, threats, often, could be exercised only if specific conditions are satisfied. These conditions include successful exercise of specific threats (e.g., getting insiders to collaborate), specific system configuration (e.g., VB script or ActiveX are enabled in the browser), and access to object resources that could be used in the attack scenarios. In this paper we investigate the use of attacker capabilities to access the resources (perform actions on the system resources) of the given system as conditions to use means and opportunities. (We consider attacker resources, knowledge and expertise as means to cause threats.) Previously, Duggan et al. considered accesses to resources (i.e., attacker capabilities) as a risk estimation factor (Duggan et al., Sep. 2007), but not as conditions for exercising the threats, which we do in this paper.

This paper discusses the use of attacker capabilities in estimating the likelihoods of threats and shows how considering attacker capabilities, as extra information given to the

Table 1 – Definitions of used risk-related terms.

Term	Definition
Access	A specific type of interaction between a subject and an object that results in the flow of information from one to the other (National Computer Security Center (NCSC), 1988).
Asset	Things that have values and are required to achieve the goals of the IS (Dubois et al., 2010).
Attacker capability	The ability to access a set of resources (objects) of the IS to exercise threats.
Impact	The potential consequence of a risk that may harm the assets of a system or an organization (Dubois et al., 2010). It could be financial, legal, operational, damage reputation, and privacy violation.
Means	The tools, skills, and knowledge required to perform actions that cause the given threat. (cf. (Alberts and Dorofee, 2002)).
Resource	An entity (Object) that contains or receives information, such as records, files, programs, video displays, and devices (National Computer Security Center (NCSC), 1988). We use the terms object and resource in this paper interchangeably.
Opportunities	The circumstances that make attacking the system possible, such as the time to perform the attack and the number of allowed failed attempts (cf. (Alberts and Dorofee, 2002)).
Risk	The combination of a threat with one or more vulnerabilities leading to an impact harming one or more of the assets (Dubois et al., 2010).
Risk exposure	A function of the likelihood of the threat and the severity of its impacts (Wheeler, 2011) (Bohem used close terms to define risk exposure (Boehm, 1991)).
Security policy	A statement of what is, and what is not, allowed (Bishop, 2012).
Threat	Potential attacks, carried out by agents, that target ISs's assets (Dubois et al., 2010). In general, it is a potential violation of security policies of the given system (Bishop, 2012).
Threat agent	An agent that can cause harm to assets of the ISs (Dubois et al., 2010).
Threat likelihood	Measures the frequency and possibility that the given threat occurs (cf. (Wheeler, 2011)).
Threat severity	Measures the impacts of the given threat in terms of losses and damages (cf. (Wheeler, 2011)).
Vulnerability	A characteristic of an IS asset or group of IS assets that can constitute a weakness or a flaw in terms of IS security (Dubois et al., 2010).

Download English Version:

https://daneshyari.com/en/article/454728

Download Persian Version:

https://daneshyari.com/article/454728

Daneshyari.com