Available online at www.sciencedirect.com

SciVerse ScienceDirect

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

Computers & Security

Exploring attack graph for cost-benefit security hardening: A probabilistic approach

Shuzhen Wang [a,2], Zonghua Zhang [b,*,1], Youki Kadobayashi [c]

[a] School of Computer Science, Xidian University, China
[b] Institute Mines-Telecom/TELECOM Lille 1, France
[c] NAIST, Japan

ARTICLE INFO

Article history:
Received 15 July 2011
Received in revised form
15 August 2012
Accepted 23 September 2012

Keywords:
Security management
Vulnerability analysis
Risk assessment
Attack graph
Security hardening
Security metrics

ABSTRACT

The increasing complexity of today's computer systems, together with the rapid emergence of novel vulnerabilities, make security hardening a formidable challenge for security administrators. Although a large variety of tools and techniques are available for vulnerability analysis, the majority work at system or network level without explicit association with human and organizational factors. This article presents a middleware approach to bridge the gap between system-level vulnerabilities and organization-level security metrics, ultimately contributing to cost-benefit security hardening. In particular, our approach systematically integrates attack graph, a commonly used effective approach to representing and analyzing network vulnerabilities, and Hidden Markov Model (HMM) together, for exploring the probabilistic relation between system *observations* and *states*. More specifically, we modify and apply dependency attack graph to represent network assets and vulnerabilities (*observations*), which are then fed to HMM for estimating *attack states*, whereas their transitions are driven by a set of predefined cost factors associated with potential attacks and countermeasures. A heuristic searching algorithm is employed to automatically infer the optimal security hardening through cost-benefit analysis. We use a synthetic network scenario to illustrate our approach and evaluate its performance through a set of simulations.

1. Introduction

Theoretically, an exhaustive vulnerability searching and patching may lead to a secure system. This is a mission impossible in practice, however, due to the fact that the complexity and diversity of today's computer systems keep continuously increasing, introducing countless zero-day vulnerabilities. Also, a comprehensive vulnerability analysis usually costs much time, labor and resource, causing undesirable consequence to network and organization assets. A best practice is to prioritize the vulnerabilities and handle the key ones via cost-benefit analysis. This is extremely important in a resource-constrained network which has security budget limit. To that end, three issues must be carefully considered: (1) evaluating the criticality of individual vulnerabilities; (2) examining the implicit associations among a set of vulnerabilities exploited by an attack; (3) quantify the expected effectiveness of countermeasures.

To date, three issues have attracted much attention from both industry and academia. For instance, Common

* *Corresponding author*. Tel.: +33 320436422.
E-mail address: zonghua.zhang@telecom-lille1.eu (Z. Zhang).

[1] Most of the work reported in this paper was done when the author was with NICT, Japan. This paper subsumes a short version reported in (Zhang, 2012).

[2] The first author was financially supported by the National Natural Science Foundation of China under grant No. 61100156.
0167-4048/$ – see front matter © 2012 Elsevier Ltd. All rights reserved.
http://dx.doi.org/10.1016/j.cose.2012.09.013

Vulnerability Scoring System (CVSS) has become a widely accepted industry standard, which rates severity and risk of individual vulnerabilities based on a suit of predefined security metrics and formulas (Mell et al., 2006). Also, a variety of graphical models, such as attack tree (Ray and Poolsappasit, 2005; Schneier, 1999) and attack graph (Ammann et al., 2002; Sheyner et al., 2002; Swiler et al., 2001), can serve as formal approaches to analyze the interdependency and causal relations between vulnerabilities, although their accuracy, adaptability, and scalability remain challenging. Recent years have witnessed increasing research attention to the interactions between system, human and organizations, ranging from security metrics (Jaquith, 2007) and security economics (Anderson and Moore, 2006) to security policies and cost-sensitive response (Kheir et al., 2010). One of the primary goals of these research is to facilitate security administrator's (SA for short) understanding on network threats and risk assessment, eventually achieving the most cost-effective security investment (Dewri et al., 2007; Noel et al., 2003). However, a systematic approach to bridging the gap between low-level vulnerability analysis and high-level security management has never been seen so far.

To bridge the aforesaid gap, we develop a middleware approach to explore AG-represented vulnerability information by using Hidden Markov Model (HMM). A holistic design framework is shown in Fig. 1, where our design is emphasized with bold blocks. In particular, we slightly modify dependency attack graph to represent network assets and vulnerabilities. HMM is then applied to capture the uncertainties of those *explicit observations* and estimate *attack states*, whose transitions are driven by a set of cost factors associated with potential attacks and security hardening. As a result, a probabilistic mapping between *network observations* and *attack states* can be established, and those *root-cause vulnerabilities* are indicated with higher probabilities. More generally, the interleaved two-tier model enables SAs to predict system evolution in the presence of vulnerabilities (both known and zero-day ones), identify the root causes (namely those significant observations) of attacks, and eventually take appropriate countermeasures. The probabilistic nature of AG-HMM determines that only heuristic algorithms can be used to infer the critical network states and cost-effective security hardening. To the best of our knowledge, this is one of the first attempts to develop a systematic approach to automatically take cost-effective security hardening based on vulnerability analysis.

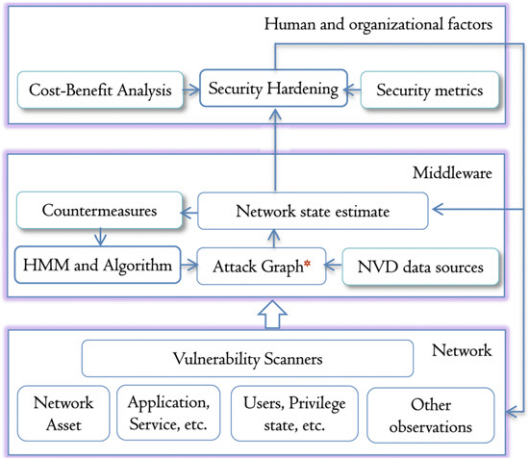

Fig. 1 – A holistic design perspective. Shown are our design focus (bold blocks and arrows).

The rest of this article is organized as follows. We review some relate work in Section 2. A motivating example is given in Section 3 for illustrating the design objective of our approach. We present our approach in details in Section 4, and report our experiments in Section 5. The article is then concluded in Section 6.

2. Related work

Our work is a cornerstone of three research topics: generation of attack graph, post-processing of attack graph, and its applications to risk assessment.

2.1. *Generation of attack graphs*

Attack graph, which is viewed as a useful method for network vulnerability analysis, has attracted much research effort in the last two decades (Lippmann and Ingols, 2005). Their construction generally falls into two categories: the first form is to represent network states as a whole in terms of known vulnerabilities and enumerate state transitions via model checking (Sheyner et al., 2002; Swiler et al., 2001); the second type is to combine and encode individual vulnerabilities by identifying their causal dependency (Ammann et al., 2002; Ingols et al., 2009; Ou et al., 2005). Since the first form suffers from state explosion problem as the increase of the number of vulnerabilities, the second form has gained more popularity for its better scalability.

2.2. *Post-processing of attack graphs*

In order to make AG more useable, two ranking algorithms were designed for reducing complexity (Mehta et al., 2006; Sawilla and Ou, 2008), visualization techniques were applied to improve understandability (Lippmann et al., 2007; Homer et al., 2008), an incremental algorithms was designed for improving adaptability (Saha, 2008), and a number of systems and tools were developed, such as NetSPA (Ingols et al., 2009), CAULDRON (Jajodia and Noel, 2009), MulVAL (Ou et al., 2005). Our work does not focus on the specific generation of AG or system-level vulnerabilities, it rather slightly modifies dependency AG as a design basis of our holistic approach.

2.3. *AG-based risk assessment*

Using AG-based vulnerability analysis for risk assessment and proactive defense is a well-studied topic. In Noel et al. (2003), Wang et al. (2006), dependency AG was applied to compute minimum cost-hardening measures by identifying those key attack paths (AG edges). Then security metrics were introduced to AG for measuring network security risks using dynamic Bayesian network (Frigault et al., 2008), which was recently used to capture uncertainties implied by AG (Xie et al., 2010), such as uncertainties in attack structure, attacker action, and intrusion alerts, whereas the