Computers & Security (2005) **24**, 218—231

Computers & Security

www.elsevier.com/locate/cose

Multiple behavior information fusion based quantitative threat evaluation[☆]

Xiu-Zhen Chen[a,*], Qing-Hua Zheng[a], Xiao-Hong Guan[a,b], Chen-Guang Lin[a], Jie Sun[a]

[a] *Center for Networked Systems and Information Security (CNSIS) and SKLMS Lab, Xi'an Jiaotong University, Xian 710049, China*
[b] *Center for Intelligent and Networked Systems, Tsinghua University, Beijing 100084, China*

Received 27 May 2004; revised 11 August 2004; accepted 11 August 2004

KEYWORDS
Network security;
Information fusion;
Threat evaluation;
Evaluation index;
Markov model;
Evidence reasoning

Abstract How to evaluate network security threat quantitatively is one of key issues in the field of network security, which is vital for administrators to make decision on the security of computer networks. A novel model of security threat evaluation with a series of quantitative indices is proposed on the analysis of prevalent network intrusions. This model is based on multiple behavior information fusion and two indices of privilege validity and service availability that are proposed to evaluate the impact of prevalent network intrusions on system security, so as to provide security evolution over time, i.e., monitor security changes with respect to modification of security factors. The Markov model and the algorithm of D-S evidence reasoning are proposed to measure these two indices, respectively. Compared with other methods, this method mitigates the impact of unsuccessful intrusions on threat evaluation. It evaluates the impact of important intrusions on system security comprehensively and helps administrators to insight into intrusion steps, determine security state and identify dangerous intrusion traces. Testing in a real network environment shows that this method is reasonable and feasible in alleviating the tremendous task of data analysis and facilitating the understanding of the security evolution of the system for its administrators.

[☆] The research presented in this paper is supported in part by the National Outstanding Young Investigator Grant (6970025), National Natural Science Foundation (60243001) and 863 High Tech Plan (2001AA140213) of China.

* Corresponding author.
E-mail addresses: xzchen@sei.xjtu.edu.cn (X.-Z. Chen), qhzheng@mail.xjtu.edu.cn (Q.-H. Zheng), xhguan@sei.xjtu.edu.cn (X.-H. Guan), cglin@sei.xjtu.edu.cn (C.-G. Lin), sunjie@cpc.xjtu.edu.cn (J. Sun).

0167-4048/$ - see front matter © 2004 Elsevier Ltd. All rights reserved.
doi:10.1016/j.cose.2004.08.009

Introduction

Computer networks worldwide have become integral parts of the infrastructure on which many critical information services and applications rely. In defense related applications, network technology serves in the modern information warfare with the intention of obtaining relative information superiority, i.e., the capability to collect, process and disseminate information while exploiting or denying an adversary's ability to do the same (Ahvenaine et al., 2003; Hutchinson and Warren, 2001). Many attack strategies adopted by warring parties threaten the security of the computer network systems of the opponent, such as denying access to data, or destroying data (Hutchinson and Warren, 2001). Ensuring that networks can survive malicious intrusions is therefore very important. Currently, there are two broad kinds of techniques for protecting computer networks against intrusions: prevention-based techniques and detection and response-based techniques. But none of the current techniques provides complete protection. Experienced hackers can be expected to continue to try their best to evade security mechanisms in order to achieve their malicious intentions, such as obtaining confidential archives, or tampering with system files. Security is therefore an increasing concern for most administrators. It is vital for them to be able to evaluate system security, even in well-protected computer networks. Moreover, many administrators must make decision about the system security so as to timely adjust security policy for reliable and robust network.

Evaluating the security of computer networks has become a very important topic in the field of network security since 1993, when Dan Farmer and Wiestse Venema pioneered the work of network security evaluation in their seminal paper "Improving the security of your site by breaking into it" (Farmer and Venema, 2002). As is well known, the security of computer networks is tied to two factors: internal vulnerabilities and external threats. An internal vulnerability refers to a flaw or weakness that exposes the system to harm. An external threat refers to a deliberate or unintentional event, which could compromise the system. Accordingly, security evaluation of computer networks can be classified into two kinds: vulnerability evaluation and threat evaluation (Van der Walt, 2003). Vulnerability evaluation involves checking for internal vulnerabilities through active probing or passive listening, evaluating potential impact of any vulnerability on system security, and proposing appropriate solutions. It measures the security of computer networks itself without regard to threats it has to face. To date, the mainstream of network security evaluation products, which primarily originate from traditional network scanners, rely mainly on vulnerability evaluation. These products include Nessus (Deraison, 2003), ISS Internet Scanner (Internet Security System, 2002), passive scanner NEVO (Tenable Network Security Inc, 2003) and others. Ongoing developments in vulnerability evaluation continue to be reported in numerous advanced security conferences and authoritative security journals (Jajodia et al., 2003; Phillips and Swiler, 1998; Ortalo et al.,1999).

Threat evaluation focuses on measuring the potential impact of actual threats against the system. Threat information is obtained by sampling of intrusion detection sensor (IDS) alerts, by penetration tests, by analyzing selected metrics of network performance, or by combination of three techniques. At present, commercial products utilizing threat evaluation are still rare, but research is on-going (Porras et al., 2002; Cohen, 2004; Hariri et al., 2003; Snort Project, 2004). The accuracy of threat evaluation based on IDS alerts is undermined by false positives (Cuppens and Miège, 2002) and by the failure to distinguish between successful attacks and failed attacks (Lippmann et al., 2002). Moreover, IDSs also have the shortcoming of producing a large amount of alerts per sensor per day, which overwhelms administrators and makes it difficult for them to interpret the alerts accurately (Manganaris et al., 2000). It is time-consuming to achieve threat evaluation by penetration tests. Threat evaluation based on selected metrics of network performance can only evaluate one particular type of intrusion.

This paper presents a new approach to evaluate the impact of malicious external threats to the computer networks, one which focuses on monitoring the security evolution of a system with respect to the modification of security factors and on improving the accuracy of threat evaluation. Our approach is based on the observation that the most prevalent kinds of intrusions tend to have two intentions: obtaining illegal user privilege by performing a series of elementary intrusions or causing denial of service (DoS). A novel evaluation model based on multiple behavior information fusion (MBIF) relying on two indices of *privilege validity* and *service availability* is proposed. Our approach is applicable to all common remote intrusion cases. Experimental results in real network environment have shown that this method cannot only evaluate the impact of prevalent intrusions comprehensively and accurately,