Realtime Intrusion Risk Assessment Model based on Attack and Service Dependency Graphs

Alireza Shameli-Sendi, Michel Dagenais, Lingyu Wang

PII: S0140-3664(17)30732-6
DOI: 10.1016/j.comcom.2017.12.003
Reference: COMCOM 5615

To appear in: *Computer Communications*

Received date: 28 June 2017
Revised date: 29 October 2017
Accepted date: 10 December 2017

Realtime Intrusion Risk Assessment Model based on Attack and Service Dependency Graphs

Alireza Shameli-Sendi[1], Michel Dagenais[2], and Lingyu Wang[3]
[1]Faculty of Computer Science and Engineering, Shahid Beheshti University (SBU), Tehran, Iran
[2]Department of Computer and Software Engineering, Polytechnique Montreal, Canada
[3] Faculty of Engineering and Computer Science, Concordia University, Montreal, Canada
Email: a_shameli@sbu.ac.ir, michel.dagenais@polymtl.ca,wang@ciise.concordia.ca

Abstract

Network services are becoming larger and increasingly complex to manage. It is extremely critical to maintain the users QoS, the response time of applications, and critical services in high demand. On the other hand, we see impressive changes in the ways in which attackers gain access to systems and infect services. When an attack is detected, an Intrusion Response System (IRS) is responsible to accurately assess the value of the loss incurred by a compromised resource and apply the proper responses to mitigate attack. Without having a proper risk assessment, our automated IRS will reduce network performance, wrongly disconnect users from the network, or result in high costs for administrators reestablishing services, and become a DoS attack for our network, which will eventually have to be disabled. In this paper, we address these challenges and we propose a new model to combine the *Attack Graph* and *Service Dependency Graph* approaches to calculate the impact of an attack more accurately compared to other existing solutions. To show the effectiveness of our model, a sophisticated multi-step attack was designed to compromise a web server, as well as to acquire root privilege. Our results illustrate the efficiency of the proposed model and confirm the feasibility of the approach in real-time.

Index Terms

Network attack graph, Network service dependency graph, Attack impact, Forward impact propagation, Backward impact propagation, Response cost computation, Response system, Trace, Kernel event.

I. Introduction

Today, cyber attacks and malicious activities are rapidly becoming a major threat to the security of organizations [1]. Usually, the attacker exploits security goals: the confidentiality and integrity of data, and the availability of service (referred to as CIA), by targeting vulnerabilities in the form of flaws or weak points in the security of network services or software applications. Attackers can combine related vulnerabilities to incrementally penetrate networks, potentially leading to devastating consequences [2]. Such composition of vulnerabilities can be modeled through attack graphs (AG). Attack graph can help to extract all attack paths through a network and can help to make plans to secure paths.

To secure paths the tradeoffs between attack damage, security costs and security benefits should be analyzed properly. Therefore, we can avoid over investing in security measures when they do not pay off [4]. Examples of security measures include disabling/restarting a daemon, killing a process, or adapting the firewall configuration. Note that the more an attacker progresses in attack graph, the more devastating damage can be inflicted. Thus, the proper candidate security countermeasures in each node of attack graph to mitigate attack are varied.

Therefore, the attack impact and security cost should be attuned properly. If an attack with a high damage is going to befall, a strong response should be selected. For example, imagine an attacker is close to the end of attack graph, and he may compromise the database presumably. In this case, the strong countermeasures like ”Blocking All Traffic by Firewall” or ”Disabling the Database” are the best options to deploy in the network. In contrast, if an attacker is in the beginning of the multi-step attack, the weak