A Survey of Security Models Using Effective Moving Target Defenses

B S Kiruthika Devi, Vellore Institute of Technology Chennai, Chennai, India
T. Subbulakshmi, Vellore Institute of Technology Chennai, Chennai, India
KV Mahesh Babu, Vellore Institute of Technology Chennai, Chennai, India

ABSTRACT

This article describes how nowadays, attackers are targeting valuable assets and infrastructures in networked systems causing an impact on enterprises and individuals. By implementing moving target defenses helps to prevent cyber-attacks by changing the attack surface. Some security models like Attack Graph (A.G) and Attack Tree (A.T) provide a formal method to access and compare the effectiveness of them. So, in this article, the authors incorporate moving target defenses in a security model, using a Hierarchical Attack Representation Model (HARM), to compare and access the effectiveness of the security. In addition, the authors are also taking important measures (IMs) for implementing MTD techniques to enhance the scalability of the network. Finally, they compare the scalability of an attack graph and HARM models by implementing MTD techniques to find the effectiveness of security in network.

KEYWORDS
Attack Graph, Attack Surface, Hierarchical Attack Representation Model, Moving Target Defenses

INTRODUCTION

Cyber-attacks are becoming major issue for the global enterprises and individuals. Cyber criminals (i.e., attackers) are focusing more on critical infrastructures and valuable assets in a networked system (e.g., cyber-physical systems and enterprise systems), which potentially has a high socio-economic impact in an event of an attack. Security mechanisms (e.g., firewalls) may enhance the security, but the overall in-depth security of the networked system cannot be estimated without a security analysis (e.g., cannot identify security flaws and potential threats). Moreover, attackers will find the vulnerabilities in the networked system. Therefore, it is important to reduce the attacks by changing the attack surface (Manadhata et al., 2011) continuously based on a security analysis.

Moving Target Attack (MTA) techniques and methods are used to bypass the defenders’ mechanisms, the Deception is one of the most effective weapons on both attacker and defender side of the game. Over the years, numerous techniques have been developed to enable recurring modifications of cyber-attacks. The most effective and insidious are deception techniques that make it impossible to anticipate the attacker’s next onslaught. With these new techniques, collectively known as Moving Target Attacks (MTA), new strike variations can be bred in a matter of hours.

All of these tactics involve recurring modifications of source, static signatures, and/or behaviour signatures. The most dangerous also hide their malicious intent from defense systems, appearing as benign or unknown behaviour.

DOI: 10.4018/IJISP.2018070107
There are eight main techniques that attackers use:

- **Polymorphism**: Encrypting the malware’s payload, code and data, in order to avoid AV detection. By using multiple encryption keys to generate different instances of the same malware, any signature-based anti-malware becomes useless and it is concealed from scanners.
- **Metamorphism**: A variation of polymorphism where the in-memory code is changed on the fly at every execution.
- **Obfuscation**: Creating code that is incomprehensible for a human understanding, thus evading manual code inspection.
- **Self-Encryption**: Changing malware signature and hiding malicious code and data.
- **Anti-VM/Sandboxes**: Deactivating when within a virtual or sandbox environments to avoid detection, but initiating malicious activity once released to real systems.
- **Anti-Debugging**: Malware begins malicious activity only when it detects no debugging tools or runtime inspection.
- **Encrypted and Targeted Exploits**: URL patterns, host servers, encryption keys and file names are changed at every delivery to avoid detection. They also can limit the number of access attempts to evade honeypots.
- **Behaviour Changes**: Only execute upon real user interaction such as web page scrolling.

The “Moving Target Defense” paradigm promises to break the symmetry between the attacker and the defender. Now the attacker must also operate under uncertainty and unpredictability, where previously these were the concerns of the defender alone.

Moving Target Defense (MTD) can continuously change the attack surface of the networked system and these techniques are used in various application domains (Paulos et al., 2013). (e.g., wireless-sensor network, dynamic network and adaptive execution environment in a virtualized system). However, the existing studies do not depend on any formal security models (also known as Attack Representation Models (ARM)), Attack Graphs (AG) and Attack Trees (AT). Consequently, it is difficult to measure and compare the effectiveness of MTD techniques (e.g., which MTD technique minimizes the system risk?). In this paper, the term effectiveness of the MTD techniques describes the increase in security of the system by minimizing the efforts of the defender (e.g., to minimize the system risk with a given resources) while maximizing the efforts of the attacker (e.g., to maximize the attack cost). To address this problem (R. Zhuang et.al 2012), we propose to incorporate MTD techniques into ARMs and assess the effectiveness of them.

We classify MTD techniques into three categories: (i) Shuffle, (ii) Diversity, and (iii) Redundancy. The Shuffle technique rearranges the system setting in various layers (e.g., address randomization, migration, topology rearrangements). The Diversity technique provides equivalent functions with different implementations (e.g., operating systems, variant inputs and interpreters, variant software stack component). The Redundancy technique provides multiple replicas of the network components (e.g., services, nodes, or paths) to make multiples of the same function. Further, these techniques may be applied in combinations to enhance the security. Scalability and adaptability of the ARMs must be considered before incorporating the MTD techniques (D. Evan Jin Hong et al., 2011), as the ARM must cope with the modification in the networked system when these techniques are deployed (i.e., the attack surface changes when the network components change). However, evaluating the ARMs is not scalable as well as the lack of adaptability studies. To overcome these problems, we use a HARM which is more scalable and adaptable.
Improving Reliability and Reducing Risk by Separation
[www.igi-global.com/article/improving-reliability-and-reducing-risk-by-separation/188680?camid=4v1a](www.igi-global.com/article/improving-reliability-and-reducing-risk-by-separation/188680?camid=4v1a)

Germany's External Trade Development: A Case of the German Automotive Industry
[www.igi-global.com/chapter/germanys-external-trade-development/171839?camid=4v1a](www.igi-global.com/chapter/germanys-external-trade-development/171839?camid=4v1a)