Assessing The Energy and Strength of Moving Target Defenses using Security Models

Ms. R. Priyadharshini
[1]PG Scholar,
Department of Computer Science and Engineering,
Vivekanandha College of Technology for Women,
Elayampalayam, Thiruchengode Tamilnadu, India.

Mr. P. Prakash
[2]Assistant professor,
Department of Computer Science and Engineering,
Vivekanandha College of Technology for Women,
Elayampalayam, Thiruchengode. Tamilnadu, India.

***Abstract*— Cybercrime is an evolving issue for global enterprises and individuals. Cybercriminals (i.e., attackers) are focusing more on valuable assets and critical infrastructures in a networked system. Cybercrime is an evolving issue for global enterprises and individuals. Cybercriminals (i.e., attackers) are focusing more on valuable assets and critical infrastructures in a networked system. Scalability and adaptability of the ARMs must be considered before incorporating the MTD techniques, as the ARM must cope with the modification in the networked system when these techniques are deployed. To solve this problem, the proposed system is implemented with the Hierarchical Attack Representation Model (HARM) which is more scalable and adaptable. In this two process are done i.e., generate a two-layer HARM with the AG in the upper layer and the AT in the lower layer capturing the ability of VMs and vulnerabilities of each VM respectively. Tools, such as MulVAL can be used to generate the AG, and logic reduction techniques can be used to generate the AT.**

Keyword: ***Attack Graph, Attack Tree, Importance Measures, Moving Target Defense, Security Analysis, Security Model.***

I. INTRODUCTION

Network security is a very dangerous subject, periodically only tackled by well-trained and worked experts. However, as more and more peoples become connected, an increasing number of people need to understand the simple things of security in a networked world. This document was taken with the general computer user and information systems manager in mind, explaining the concepts needs to read through the hype in the marketplace and understand problems and how to deal with them. Some old techniques of networking are included, as well as an introduction to TCP/IP and internetworking. To consider risk management, network threats, firewalls, and more special-purpose secure networking devices. This is not intended to be a frequently asked questions reference, nor is it a hands document defining how to accomplish specific functionality. It is hoped that the user will have a wider perspective on security in general, and easily understand how to reduce and manage risk personally, at home, and in the workplace.

A. Risk Management: The Game of Security

It's very important to understand that insecurity; one simply cannot say what the best firewall is? One unplugged from the network, power supply, locked in a safe, and thrown at the bottom of the ocean. Unfortunately, it isn't terribly useful in this state. A machine with correct access is extremely applicable to use: it's easy there and will do whatever you tell it, without questions, authorization, passwords, or any other process. Unfortunately, this isn't terribly practical, either: the Internet is a not good neighborhood now, and it isn't long before some bonehead will tell the computer to do something like self-destructing, after which, it isn't terribly useful to you. This is no different from our daily lives. Constantly make decisions about what risks we're willing to accept. To get in a car and drive to work, there's a certain risk that we're taking. It's possible that something completely out of control will cause us to become part of an accident on the highway.

To get on an airplane, we're accepting the level of risk involved in the price of convenience. However, most people have a mental picture of what an acceptable risk is, and won't go beyond that in most circumstances. If it happens to be upstairs at home, and want to leave for work, do not go to jump out the window. Yes, it would be more convenient, but the risk of injury outweighs the advantage of convenience.

B. Types and Sources of Network Threats

Now, they covered enough background information on networking that they can actually get into the security aspects of all of this. First of all, to get into the types of threats there are against networked computers, and then some things that can be done to protect you against various threats.

II. RELATED WORKS

A. V.Casola

The computing becomes mobile and systems enable connectivity through mobile applications, the characteristics of the network communication of these systems change due to the instability of mobile nodes on networks. Mobile devices logically move by changing addresses throughout the course of their communication in the system. These mobiles nodes acquire characteristics of a moving target defense, in which nodes change addresses to avoid detection and attack. Yet, as mobile nodes change addresses, the critical points in the system that applications are set to communicate with, such as servers, cloud services, and peer registration servers, remain static and become easily identifiable.

Mobile-enabled systems are beginning to model heterogeneous moving target networks, in which some nodes move while others remain static. Heterogeneous moving target networks expose relationships and dependencies between nodes, helping an attacker easily identify the static, critical nodes within a mobile-enabled system. Homogeneous moving target networks, in which all nodes change addresses, mask the critical points within the system, blending the mobile nodes with the critical, static nodes, and provide additional security for the static nodes. By applying a moving target defense to all nodes within a mobile-enabled system, the critical points can be masked and additional security can be provided.

B. J.Yackoski

In a decoy-based moving target defense (MTD), a computer network introduces a large number of virtual decoy nodes in order to prevent the adversary from locating and targeting real nodes. Since the decoys can eventually be identified and their Internet Protocol (IP) addresses blacklisted by the adversary, current MTD approaches suggest that the IP addresses of the real and decoy nodes should be randomly refreshed and reassigned over time. Refreshing and reassigning the IP addresses, however, disrupts services such as TCP/IP that rely on the IP address. To introduce an analytical approach to MTD and choosing the optimal randomization policy in order to minimize disruptions to system performance. Our approach consists of two components. First, the model get an interaction between the adversary and a virtual node as a sequential detection process, in which the adversary attempts to determine whether the node is real or a decoy in the minimum possible time.

To compute the optimal strategy for the adversary to decide whether the node is real or a decoy, and derive closed-form expressions for the expected time to identify the real node using this strategy. Second, to formulate the problem of deciding when to randomize the IP addresses based on a trade-off between reducing the probability of detecting the real node and minimizing the disruption to network services, as an optimal stopping problem. To derive the optimal randomization policy for the network and analyze the detection probability, expected number of connections lost due to IP randomization, and expected time between randomizations under the proposed policy. Their results are illustrated via a simulation study using real-world data from NMAP, a software tool used to identify decoy nodes. The simulation study indicates that our IP randomization policy reduces the probability of detection while minimizing the number of connections that are disrupted by the randomization.

C. A.Paulos

The need for a new command and control (C2) approach for the practical deployment of Moving Target Defenses (MTDs) enterprise networks. To describe some of the requirements and constraints associated with the combined use of multiple moving target defenses, and introduce a human-agent teamwork approach for the command and control of MTDs. To introduce and discuss some of the specific concepts and technologies that could play an important role in the development of this capability, and conclude by describing the implementation details of the human-agent teamwork C2 prototype, called MTC2.

Moving Target Defense (MTD) proposes a conceptual shift in this paradigm. The MTD concept proposes that the target itself does not need to be static, and that a dynamic (or moving) target design can be conceived such that it maintains functionality for legitimate users, while making it difficult for adversaries to identify and exploit system vulnerabilities. Conceptually, a moving target defense relies on sets of tools or mechanisms responsible for monitoring the state of the computer network, and a set of tools or mechanisms responsible for the mobility, or effectively changing the system.

Several kinds of MTD capabilities have been proposed. Defense monitoring capabilities include intrusion detection, server and firewall log analysis, and traffic pattern monitors. Mobility capabilities create dynamic changes in the target system, directly affecting its “mobility space.” Mobility capabilities focus on five different kinds of changes that can be made to the system. These changes may be associated with: a) the execution environment of services and applications; b) the computational platform (i.e., operating systems and architecture); c) the application or service itself; d) the data used by services and applications; or e) the network.

While early MTD results have been encouraging, questions about their general practicality and utility are still unresolved. Interdependencies between individual defense capabilities and the functionality of critical applications and services are poorly understood. Moreover, the study of the interactions among different configurations of individual tools, or among whole tool sets for different operational contexts, has been hampered by the dearth of applicable tools and techniques. A better understanding of these interactions is

essential for deployment of multiple moving MTDs, and even more so when adaptation to (or co-evolution with) the adversary is being considered. All these reasons motivate our interest in developing tools that address the MTD design requirements for C2, which is the focus of this paper.

One important difference from a classical feedback-loop approach in this formulation is that the sensing components can be configured and deployed at runtime, allowing the C2 to configure both the sensors and the actuators. This requirement drives the need for increased C2 sophistication, with the control of the mobility space being influenced by the monitoring feedback which, in turn, can be configured to operate within a desired context.

III. SYSTEM ANALYSIS

Cybercrime is an evolving issue for global enterprises and individuals. Cybercriminals i.e., attackers are focusing more on valuable assets and critical infrastructures in a networked system e.g., enterprise systems and cyber-physical systems, which potentially has a high socioeconomic impact in an event of an attack. Security mechanism e.g., firewalls may produced the security, but the overall in-depth security of the networked system cannot be calculated without a security analysis e.g., cannot identify security flaws and potential threats. Moreover, attackers may explore an attack surface of the networked system to find vulnerabilities, and exploit them to penetrate through. More vulnerabilities can be modeled (with other privilege types), but they limited the number of vulnerabilities in our experiment due to the poor scalability. Used similar assumptions and settings for the simulation. There are no duplicated connections between nodes. For our example virtualized system, they assume there exists an attacker connected as a client, back-end server.

A. Moving Target Defense

In the arms race between cyber attackers and cyber defense methods, attackers now claim control. They employ sophisticated deception techniques designed to evade traditional and even "another generation" defense mechanisms, for example to hiding misuse behavior and disguising it as benign or unknown behavior. To outline these technologies, collectively known *as* Moving Target Attacks (MTA), in our existing blog post. But there is a cyber defense strategy that cuts the attack-patch cycle. *Moving Target Defense* (MTD) uses counter-deception techniques that constantly change the target surface so that attackers can't get a foothold.

There are two main categories of MTD:

- **Network level MTD**: Changing the network topology, including IP-hopping, random port numbers, extra open or closed ports, fake listening hosts, and obfuscated port traffic as well as fake information about the host and OS type and version.
- **Host-level MTD**: Changing the host and OS level resources, naming, and configuration. To outline these technologies, collectively known as Moving Target Attacks *(*MTA), in our existing blog post.

B. Proposed Method Harm

The system can be regarded as a small sized example of the Cloud Band model, and we create a larger model for our simulation. More vulnerabilities can be modeled (with other privilege types), but they limited the number of vulnerabilities in our experiment due to the poor scalability. They used the similar assumptions and settings for the simulation as in (i.e., a randomly generated networked system with a given density value that specifies the average number of connections a node has). There are no duplicated connections between nodes. For our example virtualized system, to assume there exists an attacker connected to a client, back-end server. To the best of our knowledge, this is the first work to evaluate the effectiveness of MTD techniques via a formal security model for a comparative security analysis and measuring changes in performance. Our contributions are: Incorporating and analyzing the effectiveness of the MTD techniques (Shuffle, Diversity, and Redundancy) using the HARM Take into account complex Diversity deployment strategy; Conduct comprehensive experiments for MTD techniques and consider changes in performance and security.

C.Importance Measures

To use importance measures IMs to further improve the scalability. They can analyze the scalability and compare the changes in the performance and security when deploying MTD techniques using simulations. The performance of the IMs is compared against an Exhaustive Search ES method, where the ES method for deploying the MTD techniques computes all possible deployment scenarios of the given MTD technique to find the best deployment strategy. In contrast, using the IMs to deploy the MTD technique computes important system components based on the IMs, where the MTD techniques are deployed onto an important server is selected for a redundancy.

D. Mtd Implementation

MTD techniques can be deployed in various layers of the networked system as shown in Table 4, and they can improve the MTD framework. To enlist the some of the most recent MTD techniques, where their effectiveness could be measured using our idea in this paper. Shuffle: System settings in various layers are rearranged when the Shuffle technique is deployed. At the TCP/IP layer. Showed changing the IP addresses in a software-defined network (SDN), with their major goal of maximizing the unpredictability and the mutation rate. Shuffled IP addresses, with a specified object to harden networks against Hit list Worms. At the infrastructure layer, in private clouds with focuses on the integrity of the software prior to the considered a VM-LM in clouds with focuses on practicability considering the availability and duration of the VM-LM. At the application layer randomized. HTML elements to mitigate web bots showed the secure

service access for clients by relocating secret proxies and shuffling client-to-proxy assignments.

Diversity is the equivalent functionalities are maintained, but the implementations vary in various layers when the Diversity technique is deployed. At the topology layer, formalized family of metrics for path diversity (e.g., reliability and resilience) and proposed path diversification selection algorithm.

The use of an abstracted Cloud Band model. The example networked system can be regarded as a small sized example of the Cloud Band model, and to create a larger model for our simulation. A proportion of important VMs for security analysis, and choosing different percentages of important nodes are analyzed in the next experiment. They can assume there are two vulnerabilities for each VM, and the attacker can exploit any of the two vulnerabilities to compromise that VM.

To incorporate the MTD techniques for security modeling and analysis uses the HARM. To analyze the security of Shuffle, Diversity, and Redundancy, and performed security analyzes to measure their effectiveness, which is comparable using the same metrics. In addition, they proposed to use the IMs to deploy MTD techniques in an efficient way. To show that the security analysis and deploying MTD techniques using the IMs and the ES method were equivalent, but the performance was dramatically improved using the IMs.

E. System architecture

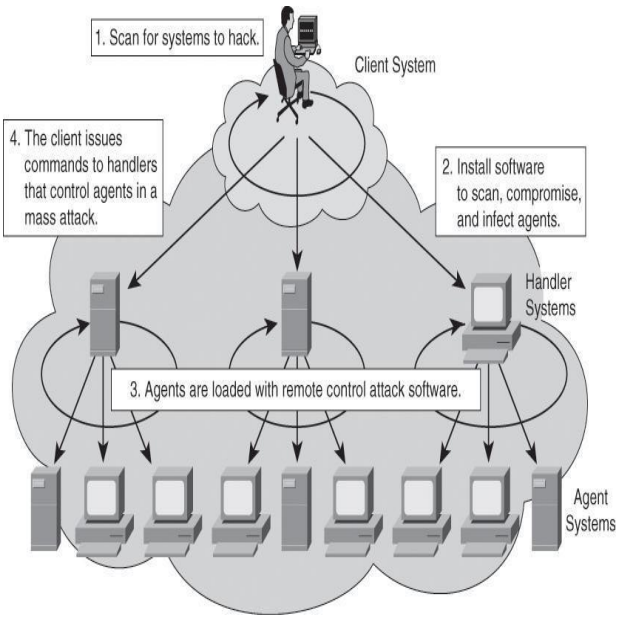

FIGURE E. SYSTEM ARCHITECTURE

IV. MODULES

A.Modules Description

- ***Attack Graph***

Moving Target Defense MTD can continuously change the attack surface of the networked system , and these techniques can be used in various application domains dynamic networks , wireless sensor networks , and adaptive execution environment in a virtualized system. However, existing studies do not rely on any formal security models (also known as attack representation models ARMs, such as Attack Graphs AG sor Attack Trees. Consequently, it is difficult to measure and compare the effectiveness of MTD techniques which MTD technique minimizes the system risk. In this project, the term effectiveness of the MTD techniques describes the ability to enhance the 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 to maximize the attack cost. To address this problem, they propose to incorporate MTD techniques into ARMs and assess the effectiveness of them.

- ***Attack Tree***

A simple example based on the virtualized system is shown in Figure 3.To assume that is unavailable, the attacker has compromised, and targets are and steal information from different asset nodes. To apply an OS diversity technique in the example as specified in Section, where a dotted box represents the VM with OS diversity applied. On the other hand, Figure shows that the OS diversity is applied to that satisfies the security goal with only a single implementation of OS diversity. If they can assume the implementation of the OS diversity has an associated cost, then minimizing the number of nodes OS diversity only on is more cost effective.

- ***Importance Measures***

To use importance measures IMs to further improve the scalability. They can analyze the scalability and compare the changes in the performance and security when deploying MTD techniques using simulations. The performance of the IMs is compared against an Exhaustive Search ES method, where the ES method for deploying the MTD techniques computes all possible deployment scenarios of the given MTD technique to find the best deployment strategy. In contrast, using the IMs to deploy the MTD technique computes important system components based on the IMs, where the MTD techniques are deployed onto an important server is selected for a redundancy.

- ***Moving Target Defense***

Also, we used the IMs to select highly important network components hosts and vulnerabilities to deploy the MTD techniques, and a significant improvement using the IMs in terms of scalability is shown in comparison to the ES method in our experiments. Moreover, our experimental results showed that we can assess the effectiveness of the MTD techniques as well as the changes in the performance the ECC, reliability and availability and security the system risk and

attack cost to observe the trade-offs between those metrics prior to deploying the MTD techniques.

- ***Security Analysis And Model***

To the best of our knowledge, this is the first work to evaluate the effectiveness of MTD techniques via a formal security model for a comparative security analysis and measuring changes in performance. Our contributions are: Incorporating and analyzing the effectiveness of the MTD techniques (Shuffle, Diversity and Redundancy) using the HARM Take into account complex Diversity deployment strategy; Conduct comprehensive experiments for MTD techniques and consider changes in performance and security.

Second, we simulated the performance with respect to the different proportion of important VMs selected, which is shown in Figure 9. It shows that as the proportion of important VMs decreases (i.e., the number of selected important VMs decreases), the performance of security analysis increases. It also shows that taking into account all VMs using the IMs (i.e., equivalent to the ES method) performs worse than the ES method due to the overhead of computing the IMs.

B Security Analysis and Model

To the best of our knowledge, this is the first work to evaluate the effectiveness of MTD techniques via a formal security model for a comparative security analysis and measuring changes in performance. Our contributions are: Incorporating and analyzing the effectiveness of the MTD techniques (Shuffle, Diversity, and Redundancy) using the HARM Take into account complex Diversity deployment strategy; Conduct comprehensive experiments for MTD techniques and consider changes in performance and security.

Second, we simulated the performance with respect to the different proportion of important VMs selected. It shows that as the proportion of important VMs decreases the performance of security analysis increases. It also shows that taking into account all VMs using the IMs (i.e., equivalent to the ES method) performs worse than the ES method due to the overhead of computing the IMs. However, this overhead is almost negligible, as the complexity of computing the IMs is in a polynomial complexity, whereas evaluating security with the AG or the HARM is in an exponential complexity.

V.CONCLUSION

Moving Target Defense (MTD) is a network defense strategy that continuously changes the attack surface to prevent cyber crimes and thwart attacks. By doing so, they can minimize the potential socio-economic impact on enterprises and individuals, as well as protect important assets and critical infrastructures. A major problem of adopting the MTD techniques is the inability to guarantee that the security is enhanced by changing the attack surface. Therefore, they must assess the change in security prior to deploying any MTD techniques. However, the effectiveness of implementing the various MTD techniques cannot be compared to one another, because they did not consider using a formal security model to investigate them. Also, it is difficult to decide how to deploy the MTD techniques efficiently. To address the aforementioned problems by incorporating the MTD techniques Shuffle, Diversity and Redundancy into the HARM, and assessed the security of them. They showed a formal security analysis of the MTD techniques using various performance and security metrics, which are used to compare their effectiveness.

VI. FUTURE ENHANCEMENT

A formal security analysis of the MTD techniques using various performance and security metrics, which are used to compare their effectiveness. Also, it is used the IMs to select highly important network components (e.g., hosts and vulnerabilities) to deploy the MTD techniques, and a significant improvement using the IMs (in terms of scalability) is shown in comparison to the ES method in this experiments. Moreover, the experimental results showed that can assess the effectiveness of the MTD techniques as well as the changes in the performance (e.g., the ECC, reliability and availability) and security (e.g., the system risk and attack cost) to observe the trade-offs between those metrics prior to deploying the MTD techniques.

REFERENCES

[1] Casola.V, De Benedictis.A, And Albanese .M.. (2015), Assessing the Effectiveness of Moving Target Defenses using Security Models", In Proc. Of The Ieee 14th International Conference On Information Reuse And integration, Pp. 22–29.

[2] Crouse. M And Fulp.E. (2014), Target Defenses To Network Security" In Proc. Of The 4th Symposium On Configuration Analytics And Automation.

[3] Evans.d,Nguyen-Tuong.a, and knight.j. (2014), "a command and control framework for moving target defense cyber resilience, effectiveness OF MOVING target defenses," in moving target defense, ser. Advances in information security, jajodia.s, Ghosh.a Swarup.v, wang.c, eds.springer new york, vol. 54, pp. 29–48.

[4] Manadhata.P. (2013), "Effectiveness Of Ip Address Randomization In Decoy- Based Moving Target Defense," In Moving Target Defense Ii, Ser. Advances in Information Security, Jajodia.S, Ghosh.A, Subrahmanian.V New York, Vol. 100 Pp. 1–13.

[5] Manadhata.P And Wing. J. (2013), "Optimizing A Network Layer Moving Target defense For Specific System Architectures," Ieee Transactions On Software Engineering, Vol. 37, No. 3, Pp. 371–386.

[6] Paulos.A, Pal.P, Schantz.R, And Benyo.B. (2013),"Analysis Of Network Address Shuffling As A Moving Target Defense" In Proc. Of The 8th Annual Cyber Security And Information Intelligence Research Workshop (Csiirw 2013). New York, NY, USA: Acm, Pp. 62:1–62:4.