2015 International Conference on Information Processing (ICIP)
Vishwakarma Institute of Technology. Dec 16-19, 2015

Study of Dynamic Defense Technique to Overcome Drawbacks of Moving Target Defense

Sachin Kailas Bhopi
ME Student: Department of Information Technology
Ramrao Adik Institute of Technology
Nerul, Navi Mumbai, India
sach.703@gmail.com

Nilima M. Dongre
Assistant Professor: Department of Information Technology
Ramrao Adik Institute of Technology
Nerul, Navi Mumbai, India
nilimarj@gmail.com

***Abstract*— Attacker typically begin the attack by reconnaissance phase in which they monitor the network and probe it over a period of time. When an attack surface is static, an attacker can monitor the network, identify vulnerabilities and entry points and build efficient and targeted attacks. A Moving Target Defense is a way to disrupt the reconnaissance phase as it provides attack surface which constantly changes. An attacker then trying to probe and identifying vulnerabilities of false system which may required more resources as well as increase the risk of detection. Moving Target Defense technique either alters network configuration to limit the usefulness of an attacker reconnaissance or change computers appearance over time using TCP/IP fingerprint obfuscator but there is a new concept which leaves the defended system at rest and makes the Defense Dynamic. Dynamic Defense is a new defense technique that removes hacker ability to depend on previous information without introducing motion in the network infrastructure. This paper provides a comparative analysis of Moving Target Defense and Moving Defense Technique.**

Keywords—moving target; dynamic defense; changing configuration; network address randomization

I. INTRODUCTION

In the early days of computing, security threats mainly included viruses that doesn't causes any serious damage to the information or systems. Attacks with the potential harm to information hardly occur. Nowadays, attackers has ability to hack into security to gain an unauthorized access to impact negatively on profitability of business, confidence of customers, businesses reputation and overall economic growth. With few exceptions, traditional computer networks are designed to operate in relatively static environments. Most critical services and networks rely on well-planned structure and support capabilities that must be carefully configured for service provisioning. These supporting infrastructures range from physical device such as computers, routers and switches to higher level services such as domain name services, registration and authentication [1].

Software systems and their entire supporting infrastructure must then be maintained and protected against failures and attacks. Attackers usually get the information about the infrastructure and its potential vulnerabilities to achieve their goals. Attackers reconnoiter the network, plan their attack, and launch it on their timescale and defenders are left to react as best they can. In the best case, highly trained personnel monitor network activities, users and potential attackers to detect and respond to security events which are then used to update their defenses against future attacks. Unfortunately, this model tend to be much more costly to defenders than it is for attackers who can choose when and what to exploit, while defenders have to protect all assets from any potential attacks, all of the time.

One approach to prevent such exploits is to change one or more parameters of the attack surface over time. So that, the network ensures that attacks based on the previous parameter setting are ineffective against the updated parameter setting. Mechanism for changing the one or more parameter setting is classified as Moving Target Defense. Kewley et. al. [2] suggested that well resourced attacker spends approximately 45% of their time for performing reconnaissance. Therefore, avoiding this attack phase can be a successful defense strategy [3].

A Moving Target Defense is a one method to fail the reconnaissance phase of a attack. Moving Target techniques provide a defense strategy where the attack target frequently varies. It allows an attacker to probe the system and construct an exploit and then system will change its appearance so that the exploit will have slight or negligible impact. Also, an attacker acting on false information can spend more resources as well as increase the risk of detection. Moving Defense is a new technique which keeps the defended system at rest and makes the defense dynamic.

The remainder of this report is organized as follows. Section II presents Literature survey. Section III briefly addresses the issues in current systems and how it can be overcome. Section IV reports comparison of Moving target and moving defense system and analysis of it as well as implementation consideration, and Finally, Section V concludes the topic.

II. LITERATURE SURVEY

Literature involves techniques for providing security through moving target method which is actually solution to the static defense method as it will change the system appearance or network appearance after reconnaissance by the attacker.

Reconfigurable encryption architecture (REA) is suitable for securing the data on tactical network devices applying the MTD strategy. The REA supports the implementation of any

978-1-4673-7758-4/15/$31.00 ©2015 IEEE

user-defined symmetric encryption algorithm. The user can configure the contents of s-boxes, rotations at each round, and number of rounds in the encryption process. Besides, power consumption of block encryption algorithms is directly proportional to the number of rounds. Therefore, by appropriately choosing encryption parameters, lightweight and reconfigurable data security can be achieved for diverse tactical network devices [4].

Network Address Space Randomization is a method that allows the nodes of network to constantly update their IP addresses. Contrast to other network level detection methods, NASR does not provide packet level processing on network elements. Also contrast to host based detection, it does not require any modification to the system i.e. node [5].

Genetic Algorithm (GA) based Moving Target Defense is responsible for changing configuration of the actual host based on GA findings. It will select configuration among the most-fit in the chromosome pool and time during which a configuration is active should vary to counter possible attack. At the end of the interval, the configuration performance is reassessed. The fitness value of chromosome will revise and the pool will update. At one point, chromosome pool can't update after several iteration, which limits variety of the active configuration [6].

III. Moving To Dynamic Defense

Dynamic defense is a new enclave in the optimized security taxonomy as shown in figure 1.

A. *Changing Configuration (GA Based Defense)*

The basic concept is TCP/IP fingerprint obfuscator can portray different OS characteristics when probed by network scanner. If the OS identity over a network is changed after specific periods of time then we can provide moving target defense.

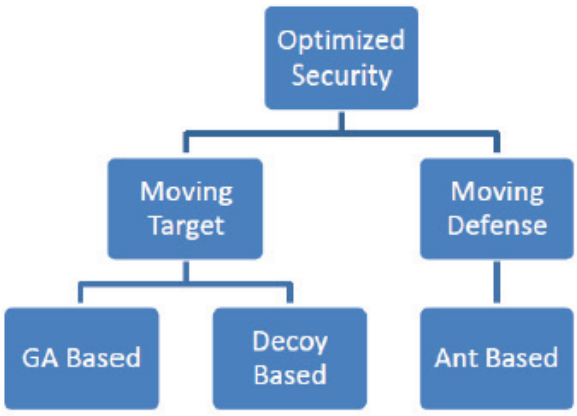

Fig. 1. Optimized security taxonomy

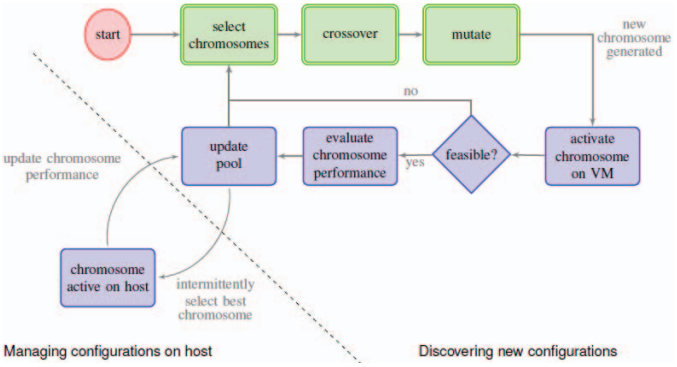

Fig. 2. Flow diagram of GA based moving target system [6].

The moving target part of the system is responsible for configuration setting changes according to genetic algorithm findings of the actual host. Intermittently, the MT process will select a configuration from among the most-fit in the chromosomes pool. In order to prevent possible attack the configuration changes according to selection from chromosome pool. At the end of the interval, the configuration performance is reassessed. Then revise fitness and update the pool accordingly. However, as number of iteration increased available chromosome in configuration pool will remain unchanged which leads to limited number of active configuration.

Drawback of this technique is when fitness score of the chromosomes do not change over time and pool can become stagnate and Always using same chromosomes pool will potentially limit the new configuration that would be discovered in subsequent GA iteration. Solution can be first, Increase mutation rate so GA to operate more as a random search a large portion of the parameter is just randomly changed. But, As a result some settings from prior good chromosome will lose in the genetic algorithm process and further solutions can't base on earlier active solution. Second, Increase pool size to have many good chromosomes and many variations. But, selection phase uses the best two solutions hence larger pool size can't affect the performance of the system.

B. *Network or IP address randomization (Decoy Based Defense)*

The basic concept is periodically remapping the network addresses so particular IP address won't always represent the same computer. But overhead associated with ensuring the network remains usable for legitimate users can be significant.

In this area current research is Effectiveness of IP address randomization in Decoy-Based MTD which focuses on a technique that uses large number of decoys that are virtual machines with valid IP address and implement common network protocol and hence appears to an attackers as a valid system. By monitoring communication of virtual machine and attacker we can get attackers information. The attacker can differentiate between real and decoy nodes in following ways: First, Due to resource constraints: A decoy network protocols are simplified and thus behaves different from those used by the real nodes. Second, Slow response: Decoys has few

computational resources which takes more time to respond to request [7].

Drawback of the system is TCP use static addresses, and IP randomization will disturb service provisioning to the legitimate user but, Solution can be import extra decoy which keeps more busy to attacker before reaching to the real node. In this case, even if attacker scan at high scanning rate hypervisor can wait until the number of connection to the real node goes to zero but improvement in availability to outside nodes must be balanced with the resource cost in the CPU and memory required to maintain a large number of decoys.

C. Ant Based Cyber Defense (Dynamic Defense)

Moving Defense is a new technique which leaves the defended system at rest and makes the defense dynamic. To overcome the drawback of MTD without requiring additional cost for CPU and memory resources as well as without introducing the additional complexity in an available infrastructure researchers moving towards the new evolution in a security that is Moving Defense.

In this area current research is Defense of Move: Ant based Cyber Defense. It removes hacker capability to trust on earlier experience without introducing motion in the infrastructure [8]. As shown in the figure 3, ABCD hierarchy contains human supervisor at top of the hierarchy, then Sergeants which inform human about anomalies and set policies for lower level agents, then Sentinels tracks security reports about the machine over time and ant like sensors which roam from machine to machine. Ant like sensors visits the sentinels through any path to check anomalies. If anomalies detected then sentinels inform the digital ant to drop pheromones which is an indication for another ants which contain different set of malicious definitions to visit at that particular node to verify it has their known types of anomalies or not. If multiple pheromones are drop at one node then sentinels forms the swarm which is recorded at the sergeants which take an action if it can't handle by sergeants then inform human supervisor to take corrective action.

Advantages of Moving Defense Technique are; First, Improved security: Signature database quickly become too large to search thoroughly each time because each ant carries only single indicator and search rate is regulated by ant-arrival rate. Second, Increase cost of attack: All malware signatures are distributed to all ant sensors which travel through different path and no two sensors compare the same quantities according to the same expected distributions. This unpredictability reduces the utility of adversary reconnaissance and makes it difficult for attackers to choose the time and strategy of attack. Third, Discover new threat signature: Each sensors path to a given location differs every time; each sensors experience will be different. This gives each sensor different historical reading and unpredictable detection threshold which leads to new threat signature. Forth, No Alteration in protected infrastructure: This system removes attacker ability to rely on prior experience without changing any infrastructure properties unlike moving target defense.

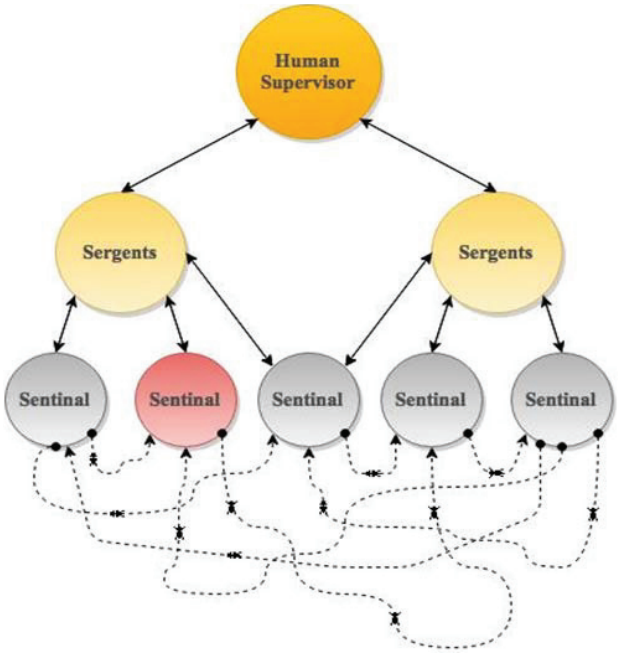

Fig. 3. Dynamic defense framework

Issues of Moving Defense Technique are; first, Spawning and self terminating feature of ants: It leaves them open to the possibility of an attack in which all the ants or all ants of specific kind are destroyed and no more remain to spawn but it has solution of Lonely sentinels: if a sentinel hasn't seen any of a particular type of sensor for long time, it will spawn an ant, favoring types that have proven effective in the past and those that haven't been seen recently. Second, Attackers attempt to bring down a node to subverting ABCD: Attacker could attempt to attract many ants to a system to conduct a resource exhaustion attack on the affected node, the end result will only be a swarm that will attract attention to the attackers position but it has a solution of Population dynamics: It ensures that the ant density i.e. mean number of ants visiting each node per unit time will remain approximately constant over the entire enclave regardless of an attackers attempts to bring down a node.

Application: Energy Sector: Energy sector devices often have long, stable deployment life cycles on resource-constrained platforms, which limits the ability to conduct a traditional MTD that could change part of the system on which that legacy hardware or software depends. ABCD was designed to operate in resource constrained environments such as those found in the energy sector without disrupting legacy features.

IV. Comparative Analysis

Comparison of moving defense using Ant based cyber defense with moving target defense using GA based cyber defense as well as Decoy based cyber defense against various parameters is shown in Table I.

A. Comparison

TABLE I. COMPARISON OF GA BASED, DECOY BASED AND ANT BASED CYBER DEFENSE

Parameter	GA based cyber defense	Decoy based defense	Ant based cyber defense
Mode of defense	Moving Target	Moving Target	Moving Defense
Basic idea	Changing system configuration	Changing IP address	Use of Digital Ants
Alters system or network properties	Yes	Yes	No
System Performance	Changing Configuration can affect some application behavior	Changing IP address can limit availability to legitimate user.	Does not affect system performance as it does not altered system properties.
Discover new threat	No	No	Yes
Cost of attack	High	High	High
Cost of defense	Lower than Decoy based but higher than Ant based	High and will increase as number of decoy used.	Lower than other two due to population dynamics features.
Drawback	After sometime chromosome pool become stagnate so new exploit can affect the system.	Disturb and degrade performance of real node to avoid it additional cost required to deploy more decoys.	At some level, this system is susceptible to single node denial-of-service attack.
Application	Suitable for small organization with approx 100 PC.	Suitable for small organization with approx 100 PC.	Suitable for embedded system (LEC 2010 microprocessor) to critical infrastructure such as energy sector.

B. Analysis

Above discussed methods in Table I shows the current evolution in the area of Moving target defense and even beyond that with the help of Moving defense technique. Here we have seen moving target is actually a best approach to increase cost of attack over the cost of defense unlike static defense but it compensate with the alteration to the actual system properties which sometimes adversely affect the performance of the system. So there is a need to make a system which takes the benefit form Static Defense as well as Moving Target Defense which leads to introduction of new technique that is Moving Defense. Moving Defense technique has capability to provide security more than that of Moving Target Defense and even without altering any system properties. It comes with the additional benefits such as this technique has capability to find previously unknown attacks and uses Decentralize security approach, which will breathe new life into defenses that can work effectively with the huge sizes of today and tomorrows networks.

C. Implementation Consideration

The Digital ant framework should be written in a language which has fast development cycle, strong library support, flexible, and ability to run multiple architecture and operating systems preferably Python. The framework implements Sergeants, Sentinels and Sensors. The Sergeant is responsible for creating the network of Sentinels, creating and dispatching Sensors to the network and as a central logging location. The Sentinel is responsible for managing an interface to data sources for Sensors to read, as well as receiving and executing Sensors. Communication between the Sergeants and Sentinels can be done with TCP/IP sockets, using plain-text messages. Each Sentinel would be identifying by an IP address and a port number. A configuration file exists that the Sergeant uses to contact each Sentinel to join it to the Sergeant's enclave. In addition the Sergeant informs each Sentinel of its neighbors, which are also specified in the configuration file.. The Sentinel also packages and transmits (migrates) Sensors to its neighbors. Each Sensor contains a reference to the Sentinel instance that it is currently visiting. This reference is managed by the Sentinel when a Sensor is received and unpackaged. The Sensor uses this reference to communicate with the Sentinel, e.g., to move to a new Sentinel or to query a data source.

The Sensor is network packet which contains fields such as id: unique identifier for the ant, sensor_type: to tell sentinel what sensor function to execute, state: foraging, dropping, idle etc., age: how long the ant has been travelling, direction: to determine next node when the ant is not following a pheromone trail, prior node: used to direct ants along pheromone trail, where_found: location where evidence found.

V. CONCLUSION

This paper compared the various techniques, methods and results. Moving Defense technique is a new evolution in cyber defense which combines the benefits from both; static defense as well as moving target defense. We have studied the issues of static defense techniques in literature and also benefits of moving target defense but due to moving target approach we faces a new issues which reduces the performance as well as availability to legitimate user. This introduces a concept of

moving defense instead of moving target which actually help us to increase the cost of attack like MTD as well as doesn't affect the availability to legitimate user like static defense.

References

[1] Marco Carvalho and Richard Ford, "Moving Target Defenses for Computer Networks," 1540-7993/14/$31.00 (c) 2014 IEEE, Pages 73-76, March/April 2014.

[2] D. Kewley, R. Fink, J. Lowry, and M. Dean, "Dynamic approaches to thwart adversary intelligence gathering," Proceeding of the DARPA Information Survivability Conference & Exposition II(DISCEX '01), volume 1, Pages 176-185, 2001.

[3] J.F. Dunnigan and A.A. Nofi, "Victory and Deceit: Deception and Trickery at war", Second Edition, Writers Club Press,2001.

[4] M.I. Husain, K. Courtright, R. Sridhar, "Lightweight Reconfigutable Encryption Architecture for Moving Target Defense," IEEE Military Communications Conference, Pages 214-219, 2013.

[5] S. Antonatos, P. Akritidis, E. P. Markatos, and K. G. Anagnostakis, "Defending against hitlist worms using network address space randomization," Computer Networks, volume 51, number 12, pages 3471–3490, 2007.

[6] M.B. Crouse, E.W. Fulp, and D. Canas, "Improving the Diversity Defense of Genetic Algorithm Based Moving Target Approaches," Proceeding of the Nat'l Symp. Moving Target Research, 2012.

[7] Andrew Clark, Kun Sun and Radha Poovendran, "Effectiveness of IP Address Randomization in Decoy-Based Moving Target Defense," 52nd IEEE Conference on Decision and Control, Pages 678-685, 10-13 December 2013.

[8] Gleen A. Fink, Jereme N. Haack and David McKinnon, Errin W. Flup, "Defence on the Move: Ant-Based Cyber Defence," 1540-7993/14/$31.00 (c) 2014 IEEE, Pages 36-43, March/April 2014.