On Moving Target Techniques for Network Defense Security

Shouq Mohsen Alnemari, Sabah M Alzahrani

Abstract— The traditional technologies, tools and procedures of any network cannot be protected from attackers due to the unchanged services and configurations of the networks. To get rid of the asymmetrical feature, Moving Target Defense technique constantly changes the platform conformation which reduces success ratio of the cyberattack. Users are faced with realness with the increase of continual, progressive, and smart attacks. However, the defenders often follow the attackers in taking suitable action to frustrate expected attackers. The moving target defense idea appeared as a preemptive protect mechanism aimed at preventing attacks. This paper conducts a comprehensive study to cover the following aspects of moving target defense, characteristics of target attacks and its limitation, classifications of defense types, major methodologies, promising defense solutions, assessment methods and applications of defense. Finally, we conclude the study and the future concern proposals. The purpose of the study is to give general directions of research regarding critical features of defense techniques to scholars seeking to improve proactive and adaptive moving target defense mechanisms.

Keywords: Survey, moving target defense, network security, Cyber Security.

I. INTRODUCTION

In current years, since network security issues, leakage of sensitive data, breakdown of industrial schemes and disruption of finance services have become more danger, cyberspace destruction and penetration poses a serious warn to all sections of associations [1]. Handling the practical issues and potential threats that the current suffers in cyberspace; a moving target defense is one of the best-grown solutions that provide a new thought for improving cybersecurity [2]. Securing critical computer systems against cyber-attacks is an ongoing struggle for system administrators. Attackers often need to find only one vulnerability to compromise systems successfully. Even so, defenders face the technically challenging task of discovering and fixing every vulnerability in a complex system [3], which typically includes an operating system, device drivers, many software applications and hardware parts.

Inside cyberspace, this imbalance between a simple one-off attack tactic and a complex, multi-part defense strategy favors the attackers. While defensive applications have grown enormously in complication and magnitude over years' malware has still simple, effective, low computational relatively and still bypassing defensive applications [4]. Promising approaches have been applied to defense techniques that attempt to restore balance to the cyber landscape is a known is as moving target defense.

Moving target technologies are changing the static nature of computer systems to increase the cost, time and resources for rising attacks [5]. Put, these technologies switch systems into moving targets difficult for cyber scoundrels to hit. Advocates who use Moving Target Defense techniques strive to achieve any or all following goals: to make computer systems more dynamic by changing their properties over time, to make the internal parts of computer systems more random and indeterminate and to make computer systems more diverse [6]. To treat the fault of current defense tactics, Moving Target Defense has grown as a main success that gives advance protect versus adaptive opponents.

An objective of Moving Target Defense is to cycle continuously between several configurations in the cyber technique like altering network configuration, software and network ports [7]. These results in increasing the uncertainties for the attackers. In fact, it naturally diminishes the attacker's reconnaissance advantage over conventional defense mechanisms. The advantages of Moving Target Defense disappear if the transformation technique is acceptance as the attacker [8], with next periods on his side, ultimately be fit to portend this motion and planning attacks consequently. Hence, for Moving Target Defense to be efficient, they must have implicit changeability in them. So that Moving Target Defense should overcome based on what they are converting into, when they are transforming and how they are transforming [8].

The rest of this paper is prepared in the next:

In Section II, discuss some background knowledge about various moving target attack methods, then the characteristics for detection and defenses against malicious attacks present in section III.

Section IV surveys some promising solutions for moving target defense techniques based on machine learning (ML) techniques.

Section V discusses the evaluation metrics of moving target defense techniques and efficiency methods regarding scene of both attackers and defenders. Finally, section VI concludes the survey and propose future of moving target defense research.

Manuscript received on August 31, 2020.
Revised Manuscript received on January 08, 2021.
Manuscript published on January 30, 2021.
* Correspondence Author
Shouq Mohsen Alnemari*, Department of Cybersecurity, College of Computers and Information Technology, Taif University, Taif, Saudi Arabia. Email: shougalnemari@gmail.com
Sabah M Alzahrani, College of Computers and Information Technology, Taif University, Taif, Saudi Arabia. Email: sa.sabah@yu.edu.sa

II. CHARACTERISTICS OF MOVING TARGET ATTACK

Organizations use modern management of infrastructure tools and track the highest practices like patching programs, hardening and analyzing the technique registry to reduce the attack surface. However, skilled enemies penetrate network assets using zero-day attacks, custom malware, which are often hard to identify or block utilizing snooping detection techniques and antivirus tools. With regard the efficient preparation of smart cyber defenses, and it is essential together data about the attack process that the opponent is pursuing as shown in Fig. 1. An intelligence-based approach that focuses on studying specific threats from an attacker's perspective is essential to detect and mitigate complex attacks, which are defined as modern constant threats [9]. To realize the correlation, classification and collection of data on a cyberattack, in [10] called the Cyber Kill Chain or called (CKC). The knowledge based on evidence from their research can assist us understand and propagate defense metrics. The next part characterizes various stages of CKC, then a summarized description of Advanced Persistent Threat and how they examine over the CKC lens. This preparation will later help us understand how moving target defense can be more efficient in various stages of Advanced Persistent Threat.

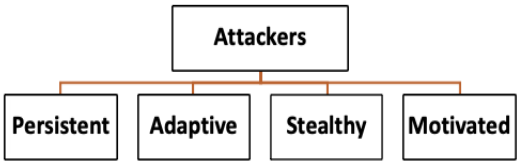

Fig. 1 A main characteristic of the advanced attackers.

In moving target attacks that investigate sides of characterizing and testing proactive attacks. Moving target defense technologies have been developed to handle smarter and continuing attacks and are equipped with more advanced tools.

- Persistent Attackers: In the current moving target defense action, we have detected that attackers are persistent, not executing a one-time attack [11]. This continual attack conduct is observed completely in multi-phase attacks that begin with examining attacks in the exploration phase prior to attacks that gain access to the external attackers and last to deliver the attack and utilization phase after they have been stormed.
- Adaptive attacker: is adapted to change dynamically the system cases and exterior environmental situations, taking to account materials and electronic accessibility. Also, the attackers have resources intelligence regarding as they carry out adaptive attacks [12] wisely supervise the limits of their resources and opportunistically desire to normalization a full system.
- Stealthy Attackers: do not exhibit recognizable attacking attitude every time. They carry out the attacks in a so secretive manner [13], even display the well-behaved characteristics of better citizens. Even so, while the attack counts to inflict serious damage or harm to the system, they exhibit offensive behaviors. But they remain invisible until it is right.
- Motivated Attackers: Moving Target Defense has been advanced to contact with intelligence attackers. In a special case, the attackers are smart enough to efficiently carry out attacks, so the attacks have a little damage but maximum results. Then, it can see the attacker to be a logical and critical agent of stimuli, such as a successful attack with minimal costs [14].

To protect against Advanced Persistent Threat, an intelligence-based defense paradigm is serious for defenders to mitigate the hazard and educability of the system. Authors in [15] improved a defense model based on intelligence called Cyber Kill Chain (CKC), based on several stages of a cyber-attack. The Cyber Kill Chain model includes:

- Describe the stages of intrusion.
- Determine the indexes of the opponent's killing chain of defense action paths.
- Identifying the pattern linking individual interventions to broader campaigns.
- Realizing of repeated intelligence collections.

Fig. 2 A Cyber Kill Chain model advanced attack stages.

The CKC model comprises the following stages [15] as shown in Fig. 2:

- Reconnaissance: Here the attacker collects data about the target's situation at this stage. For illustration, an attacker can achieve inactive monitoring utilizing automating tools like Nmap and trace-route and to conduct network investigations.
- Delivery: Sending of affected payload happens through this phase. For illustration, the attacker might drop a USB contaminated with malware on the prey's website or email the company's CFO. This measure needs the attacker to hedge the authentication, so the individual becomes a more crucial target through this stage. So, train manpower could assist reduce the attack region.
- A Weaponization: A data got in the intelligence phase. The attacker uses tools and techniques like phishing mails, which is a malware-infected document. To form a targeted attack payload versus the victims.

- Install: Once an attacker increases high advantages in the exploit phase, he may set up malware on the prey's machine or collect user data in the prey's data. applications that able to detect unusual activity like anti-malware applications, host-based intrusion defense systems. Get very critical in detecting the attack through this phase.
- Control and Command: Afterwards, the installing stage is performed, the attacker communicates to maintain remote control of the affected device. Materials like a network-based intrusion defense system and departed firewall concepts are very helpful in blocking and detecting harmful external communication messages.
- Exploitation: Offensive discharge happens through this phase. Such stage includes exploiting a vulnerability and gaining high privileges over the victim's resources using a specially designed payload that exploits a known vulnerability.
- Act on targets: through this stage, the attackers perform processes to obtain the targets of the attack, like data extraction and service disturbance. There are two different crucial activities often noticed in such attacks stage: are spin, where includes distinguishing related victim nodes which have then been exploited and sideways motion that affects recognizing alternative schemes that can be exploited.

However, there is a limitation of the advanced, persistent threat attacks. It gets very close to the attackers in a reconnaissance phase once the attackers are external attackers. Nevertheless, most times, sneaky and undiscovered insider attackers are more than dangerous to the scheme when they are not handled decently, such as being detected by an intrusion defense system. But given the large scale of false detection, moving target defense can aid offside spotting by collect other layers of defense versus interior attackers.

III. CLASSIFICATION OF MOVING TARGET DEFENSE

MTD is the idea of control any modification across several shapes of a system to enhance the doubt and increase the complexity for attackers, also decrease their chance and gain the costs of their examination and attack attempts. Moving Target Defense modifies anyone to make, analyze, test, and spread various techniques and schemes that change constantly extra time to gain complexness and outgoing to attackers, reduce the burden to vulnerabilities and attack opportunities and raising scheming resilience. Moving Target Defense approaches are designed under different categorizations with various criteria. Moving target defense methods have been discussed with different categorizations with various standards. The next part discusses the classification of moving target defense techniques. Then we differentiate the concepts of moving target defense from concepts of cheat and cover generalities and differences between them.

There is a classification of moving target defense methods based on its activity criteria to find movement [16]. We describe three kinds of moving target defense techniques as follows:

A. Shuffling process

This technology reorganizes or nestles scheming configurations, like changing IP addresses in the TCP / IP layer for VM devices. The main target of MTD based mixing approaches is to raise the uncertainty and confusion of the attackers by doing the data gathered by the attackers outdated or by cachexia the attacker's resources in gathering useless data. Finally, a mixing-based moving target defense can block or retard attackers from reaching the target scheme. As the scheme gains additional time to display attack action, intrusion defense system defense mechanisms can prepare smarter strategies for handling the attack based on specific attacks.

shuffling technology randomizes network configurations. The shuffling based moving target defense technologies use IP shuffling in various networks domains. A paper [17] proposed IP shuffling, target defense triggering using the concept of IP decoding in a Software Defined Networking environment. A proposal in [18] suggestion of a host IP address mutation is used to defend a wide area network by using a Software Defined Networking controller that controls DNS interactions. Authors in [19] proposed a random IP technique to thwart malicious worm attacks, with the goal of avoiding malware that collects data about victims' goal in a networked scheme and makes it difficult for attackers to recognize additional weak targets. An implemented-on IP shuffle technique by shifting IP addresses unexpectedly while reducing the above of moving target defense processes. The authors used a Software Defined Networking based on OpenFlow protocols, which frequently delegates realistic IP addresses interpreted from to the IP address of a proper host.

B. Diversity process

This technology uses the preparation of model parts to various applications that add the same functionality. Examples include utilize of a various routing or platform change paths that consist of implementing different software components or migrating between different platforms. Diversity based moving target defense techniques aim to improve system resiliency by rising responsibility tolerance as the scheme can supply normal works in the being of attackers in the scheme.

A different moving target defense technology have been introduced to raise network flexibility and service supplies [20, 21]. They have deployed a diversification method for virtual servers such as operating systems, virtualization elements, application software, and network servers. They assessed the considered variation process in relation to the likelihood of the attack being successful.

In this paper [22] an emphasis has placed on moving target defense technology based on various programming applications to avoid code attacks and programming injections. This paper suggested that moving target defense technology be used in various layers of applications to shift the executing communication of the web applications without disrupting or affecting the system's practicality.

C. Redundancy process

This technology supplies several replications of scheme elements, like several ways between connections in the system layer or double software elements that provide the same functionality in the application layer. The main goal of redundancies of moving target defense is to gain system dependability by supplying iterative conditions to provide similar services once certain network connections or scheme elements are agreed upon. Here, redundancy lends to acceleration the resiliency of a system in the being of internal dangers. This technology can often be mixed with diverseness-based moving target defense, such as excess services are accessible where the attacker is necessary to recognize supplemental credentials or intelligence service to utilize other alternate elements. The authors in [23] presented a proposal of a novel mechanism called a traffic morphing by following the conception of moving target defense in the status of redundancy for environments called A cyber-physical system. The suggested paper designs a traffic morphing algorithm to defend cyber-physical system terms by keeping several repeated network terms in which delay spreads between packets are indistinguishable from those observed in normal network terms. Cyber-physical system messages could be posted with one of these sittings to cope with a limited period. In the procedure of dynamic modification of the transformation procedure, this paper displayed the low-level of the complexness of the presented paper and rise adaptation to the mechanics of cyber-physical systematization. This paper [24] suggested alternative method for redundancy for web servers to block poisonous code offensive by injection on a web server by growing a self-protection mechanism, considering mitigation and detection of architectural threats. They utilized what is called understanding-based increase that supplies replication of software elements at runtime. Nevertheless, this paper did not verify the powerfulness of the presented moving target defense system.

IV. MOVING TARGET DEFENSES BASED ON MACHINE LEARNING

Moving target defense has been suggesting utilizing different forms of modeling techniques and solutions. Here, we discuss modeling techniques and key solutions for moving target defense based on machine learning techniques. Machine learning (ML) uses optimization techniques and statistics to quickly and with high accuracy analyses a complex situation [25]. Based on this, the combination of ML and control theory can perform the complex system control improvement difficulty efficiently. For the complicated and distributed features of moving target defense deployment, machine learning control ensures accurate moving target defense strategy selection. This study [26] proposed a diversity shifting approach settled on control theory. The security state assessment algorithms were initially adopted to examine the network security authorities. Consequently, it finds the runtime. Meanwhile, the cost of defense is assessed in various defense strategies by determining execution overheads. Therefore, it chooses a defensive strategy by ensuring defensive effectiveness and low overhead. The authors [27] presented a predictive moving target defense technique using machine learning to apologize for the opponent's skill to recognize the defensive performance. In this paper, the authors hypothesized attacker could study and take advantage of a rearward engineering manner to expect defensive schemes. They tested their formula by cybersecurity databases to demo the efficacy and strength of their algorithm. The paper used another method to batch with the same difficulty in [28]. They made use of defensive moving target defense and method based on machine learning, using the co-biological process relation between the attackers and defenders to deduce an ideal defensive scheme difficult to the inverse. In [29] the authors made a comparison between the open-and-close loops of defense schemes. It checks the correction characteristic of the close loop scheme can shorten the input intervention. In addition, it displays that multi-component doubt will be formed complexity growing following the law of variation. Using reinforcement learning [30] the authors designed two repetitive reinforcement learning techniques to determine an idealistic defense scheme versus cyberattack, especially when the data about the attackers is unfamiliar. They utilized stochastic stability and Markov chains in the technique by presenting the adaptive, strong reinforcement learning ability. They explained their scheme can give the near-optimal solution of the strategy of the defensive. In this study [31] the authors proposed a moving target defense framework based on deep neural networks that raise the safety and strength of deep neural network against hostile attacks. In MTDeep, the entered photo is categorized by choosing a grid from a group of grids based on a strategy created via the theoretical reasoning of the game randomly. The interaction between the images classification system is designed using MTDeep and its users in recurring Bayesian games. A defender designs space is a group of deep neural networks that have been made for the same mission, but it not influenced by the aforesaid attack. Another approach provides the game with MTDeep's optimal shifting strategy to reduce misclassification on the photo changed by opponents with advanced rating quality for valid individuals of the scheme. Authors in this paper [32] designed a moving target defense technique-based approach to embed deep optical sensing systems against antagonistic examples to generate convolutional neural network (CNN) models that can be utilized collaboratively to notice and crosspiece hostile examples. Adversarial neural networks are neural network entries that lead to false classification results. Deep models are dynamically created by the conception of moving target defense after scheme deployment. Post-distribution of models varies across schemes. This coming nullifies and disables the attackers as a fundamental foundation for building effective hostile models. Likewise, Authors in [33] proposed a strategic approach to selecting ML to defend against adversarial ML technique. In this paper, the authors recommended that attacks versus learning can be decreased through the cautious scheme of the strategic choice of learning attributes and methods. Defenders perform several learners by calculating their strategical stimulation utilizing the game theory path.

A moving target defense based on machine learning allows the scheme to catch sophisticated attack forms with advanced applicability. Even so, since machine learning performance frequently needs a great number of datasets to train to ensure a definite level of forecast efficiency when data deficits are underperforming even with high overheads and complexity. Moreover, the model needs to ensure an adequate plane of procedure powerfulness available in a situation where moving target defenses spread because some assets-limited situations can't tolerate machine learning-based moving target defense.

V. MOVING TARGET DEFENSE EVALUATION METHODS

Although researchers recognize that moving target defense evaluation is the key to determine the quality of defense provided, measurable measures around these analysis positions are necessary for effective assessment. For illustration, switching the percentage of (A) number of host's results in a decrease of B percentage in the attack's likelihood of being successful and an increase of z percentage in quality of service for the average input.

There is a classification of the evaluation moving target defense techniques based on their quantity. We describe two types of metrics of moving target defense techniques as follows:

A. secure metrics.

An important aspect of network defense is visualizing system attacks. Enterprise systems have become bigger and compounder with various network overlays and underlying applications. The old saying that cannot be measured cannot be managed is appropriately applied here. Secure metrics cover attack quantification using the Common Vulnerability Scoring Services metric evaluations such as CIA metric:

It measures many types of attack processes such as

- Attack Graphs and Attack Trees.
- Attack Representation Methods.

1) Confidentiality, Integrity and Availability (CIA) Metrics.

CIA is used as quantitative measures to measure the effect of the system under attack. In this paper [34] considering the availability is an essential measured for examining the effect of moving target defense countermeasure. The scheming configuration rate alpha is modeled as a purpose of system assets using Continuous Time Markov Chain models. It considers the analysis of the effect of reconfiguration on the availableness for fine-tuning moving target defense option. In [35] a framework uses Intrusion Detection System alerts and vulnerability score Common Vulnerability Scoring Services metric calculated based on CIA metric values to identify critical services in the network.

2) Attack Graph and Attack Tree.

It is a Common Vulnerability Scoring Services instant single a part of quantitative data on the dangers such as complexness of acting network attacks, affect confidentiality or honesty of the scheme if the attack is booming. This data lonely is not enough for taking moving target defense decisions. The Attack model approaches such as the Attack Graph method [36] and the Attack Tree [37] solve this part by the potential attack paths and the paths of the attackers take. A software Defined Networking based scalable moving target defense solution [38] prepares utilization of based on offensive graph approach to execute the security appraisal of large-scale networks. According to the security authority of the cloud networks, moving target defense counter metrics are selected.

3) Risk Metrics.

Moving target defense systems have associated risks once the organization considers deploying the moving target defense technology in whole or in part. Based on the NIST institute, there are various attacks, service interruptions and faults inception by the humans or devices that may break important goodness and qualities at the enterprise or domestic level. Risk appraisal is an important metric, and there are numerous ways to spread it and utilize it. This part highlights the work that was embraced and picked into account the dangers connected with positioning a moving target defense solution. In [39], the authors provide metrics for evaluating moving target defense and hazard analysis. For danger measures, they schemed statistical measures to think about the impact of the way an attacker can rapidly and successfully execute and win in an opponent's attacks. They assumed that the scheme would always have work in operation that could be evaluated. They studied the validity of the metrics through an Advanced Persistent Threat attack scenario simulation, in which they assumed that Advanced Persistent Threat would usually have many kinds of elevated that could be measured and detected. Finally, performing the proposed metrics was also evaluated by checking the designed system usage.

Authors in [40] give a comprehensive assessment of optimum measure selection on a group of weak attack tracks in the attack graph. Using assessing the degree of Common Vulnerability Scoring Services vulnerabilities, the authors made the choice of selecting a measure, considering the return on investment (ROI) share. The measure choice that provides the least return on investment is the optimum one. The performance of the NICE system has been shown to be effective in the status of system time lag, device usage and passage load.

4) Policy conflict analysis.

Moving target defense countermeasures such as network address switching can introduce new traffic or new flow rules quickly and dynamically. In [41] the authors explain how various countermeasures for moving target defense techniques like the change of load balancing, network address, and intrusion disclosure can reason safety policy infractions. Moving target defense based on the Software Defined Networking, but the conflict's policy can reason security breaches [42], loops and black holes in the network as discussed by the authors in [43] the variables and security policy violations should be analyzed at the network level before deploying the moving target defense countermeasure.

B. Usability metrics.

This type analyzes moving target defense research work on aspects such as Quality of Service, network capacity and delay, the impact on current mission metrics and cost of moving target defense deployment.

- A cost measures

Security versus the DDOS offensive is an important priority of many electronic systems. A paper [44] offers a cost-effective MTD solution versus Protection against DDOS and hidden transmission attacks. With adapting moving target defense, their work aims to solve the cost of adaptation and the cost to a defender if the attacker successfully exploited a particular weakness? This solution does not rely on the alerts generated by the Intrusion Detection System during the adaptation procedure. Adaptation cost involves any outgoing accompanied to buy the needed software or hardware that aids in the alteration process.

- QoS metrics

Moving target defense can lead to some performance cost on existing system resources. In [45] a paper identified virtual IP mutation, range allocation and range allocation restrictions to reduce the QoS impact that VIP collisions can have and maintain an optimal level of unpredictability. Probabilistic performance analysis of moving target defense survey defenses was performed by authors in [46]. The research work analyzes quantifiable moving target defense metrics such as survey, spoofing performance and probability of success of the attack versus the probability of connection interruption and the likelihood of attacker success under various conditions such as network size and number of computers at risk. Authors [47] performed a statistical analysis of static versus dynamic attacks against different moving target defense-based strategies:

- Standardized
- Randomized
- Diversity
- Evolution

The research consequences on execution versus flexibility show that a diversity-based moving target defense is the optimal scheme with most attacking scenes. They, too, display that uncertainties around the adversary:

1) A slow adverse or a rapidly developing adversary.
2) Can adversely affect the effectiveness of target defense.

VI. CONCLUSION

In this survey, we proposed an efficient survey of moving target defense techniques, their main taxonomies, major purpose dimensions, common attack behaviors dealt with by current moving target defense approaches and application areas that were considered in the moving target defense literature. For future research direction, cover other moving target defense classifications should be performed. And apply more useful evaluation metrics needed to protect to service availability for users.

REFERENCES

1. Weimann, G. (2005). Cyberterrorism: The sum of all fears? Studies in Conflict & Terrorism, 28(2), 129-149.
2. Craigen, D., Diakun-Thibault, N., & Purse, R. (2014). Defining cybersecurity. Technology Innovation Management Review, 4(10).
3. Nespoli, P., Papamartzivanos, D., Mármol, F. G., & Kambourakis, G. (2017). Optimal countermeasures selection against cyber-attacks: A comprehensive survey on reaction frameworks. IEEE Communications Surveys & Tutorials, 20(2), 1361-1396.
4. Jasper, S. (2017). Strategic cyber deterrence: The active cyber defense option. Rowman & Littlefield.
5. Zhuang, R., DeLoach, S. A., & Ou, X. (2014, November). Towards a theory of moving target defense. In Proceedings of the First ACM Workshop on Moving Target Defense (pp. 31-40).
6. Gollmann, D. (2010). Computer security. Wiley Interdisciplinary Reviews: Computational Statistics, 2(5), 544-554.
7. Cai, G., Wang, B., Luo, Y., Li, S., & Wang, X. (2016, January). Characterizing the running patterns of moving target defense mechanisms. In 2016 18th International Conference on Advanced Communication Technology (ICACT) (pp. 191-196). IEEE.
8. Lei, C., Zhang, H. Q., Tan, J. L., Zhang, Y. C., & Liu, X. H. (2018). Moving target defense techniques: A survey. Security and Communication Networks, 2018.
9. Tankard, C. (2011). Advanced persistent threats and how to monitor and deter them. Network security, 2011(8), 16-19.
10. Garba, F. A. (2019). The anatomy of a cyber attack: dissecting the cyber kill chain (ckc). Scientific and Practical Cyber Security Journal, 3(1).
11. Ben-Asher, N., Morris-King, J., Thompson, B., & Glodek, W. J. (2016). Attacker skill defender strategies and the effectiveness of migration-based moving target defense in cyber systems. In 11th International Conference on Cyber Warfare and Security: ICCWS2016 (p. 21).
12. Jia, Q., Wang, H., Fleck, D., Li, F., Stavrou, A., & Powell, W. (2014, June). Catch me if you can: A cloud-enabled DDoS defense. In 2014 44th Annual IEEE/IFIP International Conference on Dependable Systems and Networks (pp. 264-275). IEEE.
13. Jafarian, J. H., Al-Shaer, E., & Duan, Q. (2012, August). Openflow random host mutation: transparent moving target defense using software defined networking. In Proceedings of the first workshop on Hot topics in software defined networks(pp. 127-132).
14. Feng, X., Zheng, Z., Cansever, D., Swami, A., & Mohapatra, P. (2017, May). A signaling game model for moving target defense. In IEEE INFOCOM 2017-IEEE conference on computer communications (pp. 1-9). IEEE.
15. Hutchins, E. M., Cloppert, M. J., & Amin, R. M. (2011). Intelligence-driven computer network defense informed by analysis of adversary campaigns and intrusion kill chains. Leading Issues in Information Warfare & Security Research, 1(1), 80.
16. Hong, J. B., & Kim, D. S. (2015). Assessing the effectiveness of moving target defenses using security models. IEEE Transactions on Dependable and Secure Computing, 13(2), 163-177.
17. Sharma, D. P., Kim, D. S., Yoon, S., Lim, H., Cho, J. H., & Moore, T. J. (2018, August). FRVM: Flexible random virtual IP multiplexing in software-defined networks. In 2018 17th IEEE International Conference On Trust, Security And Privacy In Computing And Communications/12th IEEE International Conference On Big Data Science And Engineering (TrustCom/BigDataSE) (pp. 579-587). IEEE.
18. MacFarland, D. C., & Shue, C. A. (2015, October). The SDN shuffle: creating a moving-target defense using host-based software-defined networking. In Proceedings of the Second ACM Workshop on Moving Target Defense (pp. 37-41).
19. Anderson, N., Mitchell, R., & Chen, R. (2016, November). Parameterizing moving target defenses. In 2016 8th IFIP International Conference on New Technologies, Mobility and Security (NTMS) (pp. 1-6). IEEE.
20. Huang, Y., & Ghosh, A. K. (2011). Introducing diversity and uncertainty to create moving attack surfaces for web services. In Moving target defense (pp. 131-151). Springer, New York, NY.
21. Huang, Y., Ghosh, A. K., Bracewell, T., & Mastropietro, B. (2010, June). A security evaluation of a novel resilient web serving architecture: Lessons learned through industry/academia collaboration. In 2010 International Conference on Dependable Systems and Networks Workshops (DSN-W) (pp. 188-193). IEEE.
22. Taguinod, M., Doupé, A., Zhao, Z., & Ahn, G. J. (2015, August). Toward a moving target defense for web applications. In 2015 IEEE International Conference on Information Reuse and Integration (pp. 510-517). IEEE.
23. Li, Y., Dai, R., & Zhang, J. (2014, June). Morphing communications of cyber-physical systems towards moving-target defense. In 2014 IEEE International Conference on Communications (ICC) (pp. 592-598). IEEE.
24. Yuan, E., Malek, S., Schmerl, B., Garlan, D., & Gennari, J. (2013, June). Architecture-based self-protecting software systems. In Proceedings of the 9th international ACM Sigsoft conference on Quality of software architectures (pp. 33-42).

25. Dunlop, M., Groat, S., Urbanski, W., Marchany, R., & Tront, J. (2011, November). Mt6d: A moving target ipv6 defense. In 2011-MILCOM 2011 Military Communications Conference (pp. 1321-1326). IEEE.
26. Le Goues, C., Nguyen-Tuong, A., Chen, H., Davidson, J. W., Forrest, S., Hiser, J. D., ... & Van Gundy, M. (2013). Moving target defenses in the helix self-regenerative architecture. In Moving target defense II (pp. 117-149). Springer, New York, NY.
27. Colbaugh, R., & Glass, K. (2012, October). Predictability-oriented defense against adaptive adversaries. In 2012 IEEE international conference on systems, man, and cybernetics (SMC) (pp. 2721-2727). IEEE.
28. Colbaugh, R., & Glass, K. (2013, June). Moving target defense for adaptive adversaries. In 2013 IEEE International Conference on Intelligence and Security Informatics (pp. 50-55). IEEE.
29. Farchi, E., Shehory, O., & Barash, G. (2019). Defending via strategic ML selection. arXiv preprint arXiv:1904.00737.
30. Zhu, M., Hu, Z., & Liu, P. (2014, November). Reinforcement learning algorithms for adaptive cyber defense against Heartbleed. In Proceedings of the First ACM Workshop on Moving Target Defense (pp. 51-58).
31. Sengupta, S., Chakraborti, T., & Kambhampati, S. (2019, October). Mtdeep: boosting the security of deep neural nets against adversarial attacks with moving target defense. In International Conference on Decision and Game Theory for Security (pp. 479-491). Springer, Cham.
32. Song, Q., Yan, Z., & Tan, R. (2019). Moving target defense for deep visual sensing against adversarial examples. arXiv preprint arXiv:1905.13148.
33. Farchi, E., Shehory, O., & Barash, G. (2019). Defending via strategic ML selection. arXiv preprint arXiv:1904.00737.
34. Paruchuri, P., Kraus, S., Pearce, J. P., Marecki, J., Tambe, M., & Ordonez, F. (2008). Playing games for security: An efficient exact algorithm for solving Bayesian Stackelberg games.
35. Kil, C., Jun, J., Bookholt, C., Xu, J., & Ning, P. (2006, December). Address space layout permutation (ASLP): Towards fine-grained randomization of commodity software. In 2006 22nd Annual Computer Security Applications Conference (ACSAC'06)(pp. 339-348). IEEE.
36. Dunlop, M., Groat, S., Urbanski, W., Marchany, R., & Tront, J. (2011, November). Mt6d: A moving target ipv6 defense. In 2011-MILCOM 2011 Military Communications Conference (pp. 1321-1326). IEEE.
37. Compton, K., & Hauck, S. (2002). Reconfigurable computing: a survey of systems and software. ACM Computing Surveys (csuR), 34(2), 171-210.
38. Ge, L., Yu, W., Shen, D., Chen, G., Pham, K., Blasch, E., & Lu, C. (2014, June). Toward effectiveness and agility of network security situational awareness using moving target defense (MTD). In Sensors and Systems for Space Applications VII (Vol. 9085, p. 90850Q). International Society for Optics and Photonics.
39. Zeitz, K., Cantrell, M., Marchany, R., & Tront, J. (2017, April). Designing a micro-moving target IPv6 defense for the Internet of Things. In 2017 IEEE/ACM Second International Conference on Internet-of-Things Design and Implementation (IoTDI) (pp. 179-184). IEEE.
40. Kewley, D., Fink, R., Lowry, J., & Dean, M. (2001, June). Dynamic approaches to thwart adversary intelligence gathering. In Proceedings DARPA Information Survivability Conference and Exposition II. DISCEX'01 (Vol. 1, pp. 176-185). IEEE.
41. Ward, B. C., Gomez, S. R., Skowyra, R., Bigelow, D., Martin, J., Landry, J., & Okhravi, H. (2018). Survey of Cyber Moving Targets Second Edition (No. TR-1228). MIT Lincoln Laboratory Lexington United States.
42. Yuan, E., Malek, S., Schmerl, B., Garlan, D., & Gennari, J. (2013, June). Architecture-based self-protecting software systems. In Proceedings of the 9th international ACM Sigsoft conference on Quality of software architectures (pp. 33-42).
43. Yusuf, S. E., Ge, M., Hong, J. B., Kim, H. K., Kim, P., & Kim, D. S. (2016, December). Security modelling and analysis of dynamic enterprise networks. In 2016 IEEE International Conference on Computer and Information Technology (CIT) (pp. 249-256). IEEE.
44. Vikram, S., Yang, C., & Gu, G. (2013, October). Nomad: Towards non-intrusive moving-target defense against web bots. In 2013 IEEE Conference on Communications and Network Security (CNS) (pp. 55-63). IEEE.
45. Cho, J. H., Sharma, D. P., Alavizadeh, H., Yoon, S., Ben-Asher, N., Moore, T. J., ... & Nelson, F. F. (2020). Toward proactive, adaptive defense: A survey on moving target defense. IEEE Communications Surveys & Tutorials, 22(1), 709-745.
46. Venkatesan, S., Albanese, M., Cybenko, G., & Jajodia, S. (2016, October). A moving target defense approach to disrupting stealthy botnets. In Proceedings of the 2016 ACM Workshop on Moving Target Defense (pp. 37-46).
47. Hong, J., & Kim, D. S. (2012). Harms: Hierarchical attack representation models for network security analysis.

AUTHORS PROFILE

Shouq Mohsen Alnemari received the bachelor's degree in Computer Science from Taif University, Saudi Arabia in 2019. Currently, she is pursuing her master's degree in Cyber Security at Taif University.

Sabah M Alzahrani Vice Chair of Computer Engineering Department, Taif University, matster and Ph.D in Computer and Information System Engineering from Tennessee State University 2018.