Moving Target Defense Techniques

Subjects: Computer Science, Theory & Methods

Contributor: Rongbo Sun , Yuefei Zhu , Jinlong Fei , Xingyu Chen

Represented by reactive security defense mechanisms, cyber defense possesses a static, reactive, and deterministic nature, with overwhelmingly high costs to defend against ever-changing attackers. To change this situation, researchers have proposed moving target defense (MTD), which introduces the concept of an attack surface to define cyber defense in a brand-new manner, aiming to provide a dynamic, continuous, and proactive defense mechanism. With the increasing use of machine learning in networking, researchers have discovered that MTD techniques based on machine learning can provide omni-bearing defense capabilities and reduce defense costs at multiple levels.

moving target defense | cyber security | affordable defense | self-adaptive defense

1. Background

To have the principles of MTD thoroughly comprehended, it is essential to understand its background. The concept of MTD was first proposed in 2009 as a response to the shortcomings of reactive security defense mechanisms, which were primarily based on techniques such as authentication, access control, information encryption, intrusion detection, vulnerability scanning, and virus prevention. While these measures offered a degree of security, they proved inadequate due to the increasing automation and diversification of attacks. Furthermore, the complexity of modern networking environments places an overwhelming burden on network administrators, who may overlook even minor issues that could lead to serious security risks. In general, the following are key features that differentiate traditional cyber defense mechanisms from MTD:

- Traditional defenses aim to enhance the defense capabilities of static facilities and minimize their vulnerabilities' exposure. In contrast, MTD concentrates on dynamically shifting the attack surface [1] to increase resilience.
- Traditional defenses often focus on monitoring, detecting, preventing, and remediating attacks on static infrastructure. MTD emphasizes faster and more comprehensive attack detection and timely responses to mitigate potential damages.
- Traditional defenses rely on known attack patterns for defense and may be limited in addressing emerging or novel threats. MTD seeks to proactively address such unpredictable attacks through its dynamic nature.
- Unlike traditional defense mechanisms, which operate in a fixed dimension, MTD adapts and changes constantly to protect against attacks on ever-changing systems. This approach significantly limits attackers'

research time and ability to penetrate compromised systems.

While general defense mechanisms aim to improve system stability, their rigid nature makes it challenging to ensure long-term fortification against the rapidly evolving techniques employed by attackers. In contrast, MTD prioritizes affordable, service-oriented defense [1] to meet three core development points:

- Minimizing defense costs (e.g., system deployment overhead)
- Maximizing service availability for users
- Maintaining the required defense security levels

Although MTD is built on the architecture of general defense, it aims to minimize deployment overhead by adopting existing security mechanisms as its base. Introducing new security measures requires intensive analysis and patching efforts quintessentially, which can be time-consuming and impractical. MTD aims to preserve affordability in individual system deployments while maintaining its fundamental principle of providing cost-effective defense, i.e., *affordable defense*.

2. Design and Classification

The basic design principle of MTD centers around three key points.

2.1. What to Move

By dynamically shifting attack surfaces, MTD techniques confuse attackers who rely on fixed system configurations to execute an attack. As a collection of resource attributes (shown in **Table 1**) in a system that could be used by an attacker to execute an attack, the attack surface can be exploited to confuse the attacker by dynamically changing these configurations. To facilitate the enumeration of joint attack surfaces, they can be classified hierarchically based on their level of existence. This classification leads to the first way of classifying MTD techniques, which includes the network layer, platform layer, runtime environment layer, software layer, and data layer [1].

Table 1. Attack surfaces most often utilized.

The Attack Surfaces Often Utilized in Recent Years (Since '18)		
Network L.	❑IP address/Port [2][3][4][5][6][7][8][9][10][11][12][13][14]	❑Route/Network topology [15][16][17][18][19]
Platform L.	❑Virtual Machines [20][21][22][23][24]	❑Proxies [25]
Rt. Env. L.	❑Operation Systems [26][27][28]	
Software L.	❑Software [29][30][31][32][33]	

The Attack Surfaces Often Utilized in Recent Years (Since '18)		
Data L.	❑Instruction sets [34][35]	❑Codes [36][37]

various MTD techniques can disrupt the attacker's resource reconnaissance and vulnerability detection. By continuously shifting the attack surface, MTD techniques hinder an attackers' ability to locate and access target hosts, forcing them to continuously chase the target. This not only increases the attacker's cost but also eliminates their temporal advantage and information asymmetry advantage over defenders. The result is a more resilient defense mechanism that can adapt to ever-evolving threats.

Research on MTD has primarily focused on the network layer for several key reasons. Firstly, designing defense mechanisms at the network layer is more in line with MTD's pursuit of affordable defense due to its small size, low resource consumption, and ease of operation. Secondly, narrowing the focus to a specific layer, such as the network layer, allows for more targeted study and development.

Nevertheless, it is important to note that MTD has been in development for over a decade, and thus, the current top-heavy research situation does not fully represent the breadth and depth of MTD as a cyber defense mechanism.

2.2. How to Move

By seeking ways to shift attack surfaces to increase unpredictability and uncertainty, MTD techniques can lead to information failure for attackers. Cho et al. [38] classified the shifting of attack surfaces into shuffling, diversity, and redundancy (SDR), as well as hybrid techniques based on a mixture of these two or three, as shown in **Figure 1**.

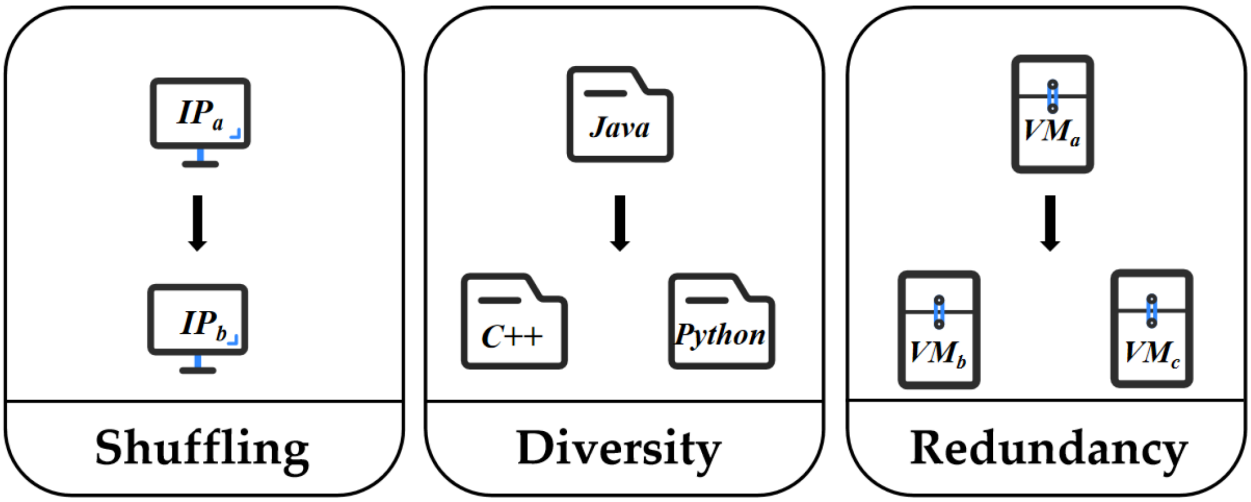

Figure 1. SDR examples.

- Shuffling

Shuffling involves randomizing or rearranging system configurations. IP hopping [2] is a common shuffling method that constantly changes the host's IP address to evade scanning by attackers. Shuffling does not require building

new security techniques. Instead, it builds on existing ones, and is, therefore, less burdensome in terms of development costs and resource consumption, is easy to operate, and is highly compatible. However, because shuffling relies on the quality of existing techniques, its effectiveness may be limited if those techniques are not sufficiently robust against attacks.

- Diversity

Diversity means alternating between different components that can achieve the same system functionality. For example, if a program is programmed in Python, the same functionality can be achieved in C++. Diversity builds on existing defense techniques and has similar advantages and disadvantages to shuffling. However, it also incurs additional defense costs due to the need to prepare extra systems or components.

- Redundancy

Redundancy refers to the preparation of multiple copies of a system or network component to ensure that the new copy can be replaced at any time if the original system or component is attacked, disabling the original attack process. It is worth noting that redundancy requires higher service availability for users than the previous two techniques. Therefore, quality measurement of redundancy is usually accomplished by evaluating the system's Quality of Service (QoS). In addition, if redundancy is not performed correctly, it provides a more significant opportunity for an attacker to execute an attack on a larger attack surface (e.g., another server to attack or another path to the target) than a system that does not use redundancy.

- Hybrid

Hybrid combines two or three of the above methods. While enhancing security, the benefits of each of the three methods can be taken into account, such as improving QoS while keeping the overhead low, but what cannot be overlooked is that hybrid presents a larger attack surface than individual methods and requires an additional overhead when combining multiple methods into a single solution.

2.3. When to Move

MTD techniques need to determine when to update the current state of the MTD system to maximize the invalidation of the relevant resource information obtained by an attacker. The conditions for triggering updates can be divided into fixed-time triggering [39] and ad hoc event triggering.

- Fixed-time triggering: MTD techniques periodically shift the attack surface at fixed intervals. Setting the triggering interval requires a technique-specific analysis, but for each technique, researchers need to find the right triggering point. If the interval is too long, attackers have enough time to penetrate the system and launch an attack. If it is too short, the MTD mechanism is triggered frequently, leading to wasted resources and degraded performance. Additionally, frequent triggering of MTD can significantly degrade the QoS and users' experience.

As a result, self-adaptive MTD techniques based on ad hoc event triggering are becoming increasingly favored. These techniques can effectively avoid the problems associated with selecting fixed intervals. By adapting to changes in the system or network environment, self-adaptive MTD techniques can ensure optimal defense mechanisms that minimize the likelihood of successful attacks while maintaining high QoS and user usage satisfaction.

- Ad hoc event triggering: MTD shifts the attack surface when the system detects an attacker's access or a precursor to an attack. Self-adaptive MTD adopts this approach, and its main challenge is accurately predicting attacks that can trigger MTD effectively.

Machine learning can be a helpful tool in addressing this challenge by assisting in the achievement of the self-adaptive triggering of MTD. By analyzing patterns in system behavior, machine learning algorithms can identify potential threats and predict future attacks more accurately than traditional rule-based systems.

3. Development Trends and Challenges for Existing MTD Techniques

3.1. Systematic Development

As mentioned above, MTD techniques are classified into two categories based on *what to move* and *how to move*, but these techniques are generally independently proposed by different researchers and have not yet formed a complete system. Therefore, it is urgent and significant in the future that work is conducted to analyze the system or network attributes affected by various MTD techniques, evaluate whether different MTD techniques can be utilized integrally, and establish a complete and available MTD system.

3.2. Integration with Existing Security Defense Mechanisms

MTD defends attackers by shifting the attack surface, but by its nature, this defense mechanism cannot cover the vulnerability of the system itself. For instance, software randomization [29][30][31] (classified as Shuffling/Software layer), a common MTD technique, does not eliminate the existence of vulnerabilities in software. Attackers are still capable of performing vulnerability attacks on specific targets through exploiting mining, buffer overflow, and other methods.

Another example is instruction set randomization [34][35] (classified as Shuffling/Data layer). Although it can prevent attackers from inserting binary instructions into the target program to execute an attack successfully, the vulnerability of the target program is also not eliminated, and well-designed worms and viruses can still break through the defense of instruction set randomization.

Existing network security defenses such as firewalls, intrusion detection systems, and anti-virus systems have been deployed in the network with network topology and a configuration that is relatively fixed, while introducing MTD into them changes the existing network configuration, thus potentially leading to increased resource

consumption, reduced network availability, and possible mutual interference with existing network security defense techniques.

MTD must be implemented appropriately without affecting existing network operations and must adapt to existing network infrastructure, network services, and network protocols. The development trend of MTD needs to integrate better with existing network security protection technology and be embedded better into the existing network.

3.3. Combination with New Techniques

How to maintain the vitality of MTD is our concern, and we believe that as a defense framework concept rather than a defense mechanism that needs to be built from scratch, MTD can be very compatible with emerging techniques.

Undoubtedly, the future of MTD is not just about machine learning. MTD has been combined with many other types of emerging techniques to achieve better active defense effects, such as:

- SDN-based MTD

MTD tends to change the existing network configuration and, therefore, usually causes the degradation of network service availability. For example, while IP address hopping can interfere with attackers' scanning and intrusion to some extent, it may cause the failure of the entire network communication, whereas a software-defined network (SDN) can fundamentally change the network structure, giving the central controller the ability to regulate the entire network globally [40]. Therefore, IP address hopping in SDN [41] could minimize the impact of moving target defense techniques on the entire network.

- MTD-applied cloud computing

Cloud computing has been widely adopted to process massive traffic data. Many large data centers have utilized cloud computing to provide convenient services due to highly centralized data and services, which is precisely the reason why cloud services are in demand of high-level defense mechanisms to protect these highly centralized data and services. Favorably, the combination of MTD with cloud computing outstandingly improves the proactive defense capability of cloud servers [42] and ensures the security of cloud services [43].

3.4. Challenges for Existing MTD Techniques

Several issues that require improvement in some existing MTD techniques, including:

- Large resource consumption and high defense costs.

- For example, in the face of the attacker's scanning, the existing MTD's countermeasure is to perform IP hopping when scanning behavior is detected, and their representative techniques include but are not limited to

OF-RHM [2], SEHT [3], DDS [4], and NATD [5]. Their common problem is a lack of accuracy and efficiency in identifying attack manners, the waste of resources caused by untargeted hops, and a lack of integration with the affordable defense pursued by MTD.

- They have an incapability of balancing multi-constraints (e.g., costs, security performance, and service availability).

- For instance, routing randomization has been proven to be an effective method against eavesdropping attacks. Currently, representative routing randomization techniques include but are not limited to: RRM [44], AE-RRM [41], AT-RRM [45], and SSO-RM [46]. However, RRM and AE-RRM implement random transformations only on the routes of data transmission between nodes, without considering different attack behaviors and protecting network QoS under such circumstances. As for AT-RRM and SSO-RM, they can dynamically adjust transformation strategies to some extent, but their protection effectiveness for QoS is still unsatisfactory, and they fail to consider the varying demands of different applications for latency and bandwidth. Besides, all of their packets' granularity is too coarse, making it easy for attackers to intercept continuous data packets and render the defense ineffective.

- Relatively fixed defense strategies (easy to be reconnoitered and recognized by attackers).

An example is the ASLR [47] deployed in Unix systems. It performs well in defending against buffer overflow vulnerabilities by randomly selecting the base address of the stack at runtime. This means that the location of each variable in memory is uncertain, making it difficult for attackers to exploit these vulnerabilities. However, ASLR is vulnerable to BROP attacks [48], which can exploit the fact that the parent process retains the same address space layout when forking a child's process. This example illustrates that fixed defense strategies are vulnerable to countermeasures applied by attackers. Therefore, there is no easy way for MTD to achieve long-term defense success.

Although MTD is confronted with many challenges, its idea that transitioning from passiveness to activeness and affordable defense is the future trend of cyber security means it has broad application prospects in many fields. With the help of machine learning, MTD research has met a brave new world.

References

1. Okhravi, H.; Rabe, M.; Leonard, W.; Hobson, T.; Bigelow; Streilein, W. Survey of Cyber Moving Targets; Technical Report, 1166; MIT Lincoln Laboratory: Lexington, MA, USA, 2013.
2. Jafarian, J.H.; Al-Shaer, E.; Duan, Q. 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, New York, NY, USA, 13 August 2012; pp. 127–132.

3. Lei, C.; Zhang, H.; Ma, D.; Yang, Y. Network Moving Target Defense Technique Based on Self-Adaptive End-Point Hopping. Arab. J. Sci. Eng. 2017, 42, 3249–3262.
4. Miao, L.; Hu, H.; Cheng, G. The Design and Implementation of a Dynamic IP Defense System Accelerated by Vector Packet Processing. In Proceedings of the International Conference on Industrial Control Network and System Engineering Research, New York, NY, USA, 15–16 March 2019; pp. 64–69.
5. Smith, R.J.; Zincir-Heywood, A.N.; Heywood, M.I.; Jacobs, J.T. Initiating a Moving Target Cyber Defense with a Real-Time Neuro-Evolutionary Detector. In Proceedings of the 2016 on Genetic and Evolutionary Computation Conference Companion, New York, NY, USA, 20–24 July 2016; pp. 1095–1102.
6. Al-Shaer, E.; Duan, Q.; Jafarian, J.H. Random host mutation for moving target defense. In Security and Privacy in Communication Networks, 8th International ICST Conference, SecureComm 2012, Padua, Italy, 3–5 September 2012; Springer: Berlin/Heidelberg, Germany, 2012; Volume 106.
7. Antonatos, S.; Akritidis, P.; Markatos, E.P.; Anagnostakis, K.G. Defending against Hitlist Worms Using Network Address Space Randomization. In Proceedings of the 2005 ACM Workshop on Rapid Malcode, Computer Networks, New York, NY, USA, 11 November 2005; pp. 3471–3490.
8. Kewley, D.; Fink, R.; Lowry, J.; Dean, M. Dynamic Approaches to Thwart Adversary Intelligence Gathering. In Proceedings of the DARPA Information Survivability Conference and exposition II (DISCEX), Anaheim, CA, USA, 12–14 June 2001; Volume 1, pp. 176–185.
9. Sharma, D.P.; Kim, D.S.; Yoon, S.; Lim, H.; Cho, J.; Moore, T.J. FRVM: Flexible Random Virtual IP Multiplexing in Software-Defined Networks. In Proceedings of the IEEE TrustCom, New York, NY, USA, 1–3 August 2018; pp. 579–587.
10. Xu, X.; Hu, H.; Liu, Y.; Zhang, H.; Chang, D. An Adaptive IP Hopping Approach for Moving Target Defense Using a Light-Weight CNN Detector. Secur. Commun. Netw. 2021, 2021, 8848473.
11. Luo, Y.B.; Wang, B.S.; Wang, X.F.; Hu, X.F.; Cai, G.L.; Sun, H. RPAH: Random Port and Address Hopping for Thwarting Internal and External Adversaries. In Proceedings of the 2015 IEEE Trustcom/BigDataSE/ISPA, Helsinki, Finland, 20–22 August 2015; pp. 263–270.
12. Carroll, T.E.; Crouse, M.; Fulp, E.W.; Berenhaut, K.S. Analysis of Network Address Shuffling as a Moving Target Defense. In Proceedings of the IEEE International Conference on Communications (ICC), Sydney, NSW, Australia, 10–14 June 2014; pp. 701–706.
13. MacFarland, D.C.; Shue, C.A. The SDN shuffle: Creating a Moving-Target Defense Using Host-Based Software-Defined Networking. In Proceedings of the 2nd ACM Workshop on Moving Target Defense (MTD), Denver, CO, USA, 12 October 2015; pp. 37–41.

14. Kampanakis, P.; Perros, H.; Beyene, T. SDN-Based Solutions for Moving Target Defense Network Protection. In Proceedings of the IEEE International Symposium on a World of Wireless, Mobile and Multimedia Networks (WoWMoM), Sydney, NSW, Australia, 19 June 2014; pp. 1–6.
15. Achleitner, S.; Porta, T.L.; McDaniel, P.; Sugrim, S.; Krishnamurthy, S.V.; Chadha, R. Deceiving network reconnaissance using SDN-based virtual topologies. IEEE Trans. Netw. Serv. Manag. 2017, 14, 1098–1112.
16. Achleitner, S.; La Porta, T.; McDaniel, P.; Sugrim, S.; Krishnamurthy, S.V.; Chadha, R. Cyber Deception: Virtual Networks to Defend Insider Reconnaissance. In Proceedings of the 8th ACM CCS International Workshop on Managing Insider Security Threats, New York, NY, USA, 28 October 2016; pp. 57–68.
17. Hong, J.B.; Yoon, S.; Lim, H.; Kim, D.S. Optimized Network Reconfiguration for Software Defined Networks Using Shuffle-Based Online MTD. In Proceedings of the IEEE Symposium on Reliable Distributed Systems (SRDS), Hong Kong, China, 26–29 September 2017.
18. Xu, X.; Hu, H.; Liu, Y.; Tan, J.; Zhang, H.; Song, H. Moving target defense of routing randomization with deep reinforcement learning against eavesdropping attack. Digit. Commun. Netw. 2022, 8, 373–387.
19. Trassare, S.T.; Beverly, R.; Alderson, D. A Technique for Network Topology Deception. In Proceedings of the MILCOM 2013—2013 IEEE Military Communications Conference, San Diego, CA, USA, 18–20 November 2013; pp. 1795–1800.
20. Hong, J.B.; Enoch, S.Y.; Kim, D.S.; Nhlabatsi, A.; Fetais, N.; Khan, K.M. Dynamic security metrics for measuring the effectiveness of moving target defense techniques. Comput. Secur. 2018, 79, 33–52.
21. Danev, B.; Masti, R.; Karame, G.; Capkun, S. Enabling Secure VM-vTPM Migration in Private Clouds. In Proceedings of the 27th Annual Computer Security Applications Conference (ACSAC), New York, NY, USA, 5–9 December 2011; pp. 187–196.
22. Zhang, Y.; Li, M.; Bai, K.; Yu, M.; Zang, W. Incentive Compatible Moving Target Defense against VM-Colocation Attacks in Clouds. In Proceedings of the IFIP International Information Security Conference, Heraklion, Greece, 4–6 June 2012; pp. 388–399.
23. Penner, T.; Guirguis, M. Combating the Bandits in the Cloud: A Moving Target Defense Approach. In Proceedings of the 17th IEEE/ACM International Symposium on Cluster, Cloud and Grid Computing, Madrid, Spain, 14–17 May 2017; pp. 411–420.
24. Peng, W.; Li, F.; Huang, C.-T.; Zou, X. A Moving Target Defense Strategy for Cloud-Based Services with Heterogeneous and Dynamic Attack Surfaces. In Proceedings of the IEEE International Conference on Communications (ICC), Sydney, NSW, Australia, 10–14 June 2014; pp. 804–809.

25. Jia, Q.; Sun, K.; Stavrou, A. Motag: Moving Target Defense against Internet Denial of Service Attacks. In Proceedings of the 22nd International Conference on Computer Communications and Networks (ICCCN), Nassau, Bahamas, 30 July–2 August 2013; pp. 1–9.
26. Thompson, M.; Evans, N.; Kisekka, V. Multiple OS Rotational Environment an Implemented Moving Target Defense. In Proceedings of the 2014 7th International Symposium on Resilient Control Systems (ISRCS), Denver, CO, USA, 19–21 August 2014; pp. 1–6.
27. Colbaugh, R.; Glass, K. Predictability-Oriented Defense against Adaptive Adversaries. In Proceedings of the 2012 IEEE International Conference on Systems, Man, and Cybernetics (SMC), Seoul, Republic of Korea, 14–17 October 2012; pp. 2721–2727.
28. Huang, Y.; Ghosh, A.K.; Bracewell, T.; Mastropietro, B. A Security Evaluation of a Novel Resilient Web Serving Architecture: Lessons Learned Through Industry/Academia Collaboration. In Proceedings of the IEEE/IFIP International Conference on Dependable Systems and Networks Workshops (DSN-W), Chicago, IL, USA, 28 June–1 July 2010; pp. 188–193.
29. Jackson, T.; Salamat, B.; Homescu, A.; Manivannan, K.; Wagner, G.; Gal, A.; Brunthaler, S.; Wimmer, C.; Franz, M. Compiler-generated software diversity. In Moving Target Defense; Springer: Berlin/Heidelberg, Germany, 2011; pp. 77–98.
30. Vikram, S.; Yang, C.; Gu, G. Nomad: Towards Nonintrusive Moving-Target Defense against Web Bots. In Proceedings of the IEEE Conference on Communications and Network Security (CNS), National Harbor, MD, USA, 14–16 October 2013; pp. 55–63.
31. Casola, V.; Benedictis, A.D.; Albanese, M. A Moving Target Defense Approach for Protecting Resource-Constrained Distributed Devices. In Proceedings of the IEEE 14th International Conference on Information Reuse Integration (IRI), San Francisco, CA, USA, 14–16 August 2013; pp. 22–29.
32. Yuan, E.; Malek, S.; Schmerl, B.; Garlan, D.; Gennari, J. Architecture-Based Self-Protecting Software Systems. In Proceedings of the 9th International ACM SIGSOFT Conference on Quality of Software Architectures, New York, NY, USA, 17–21 June 2013; pp. 33–42.
33. Larsen, P.; Homescu, A.; Brunthaler, S.; Franz, M. SoK: Automated Software Diversity. In Proceedings of the IEEE Symposium on Security and Privacy, Berkeley, CA, USA, 18–21 May 2014; pp. 276–291.
34. Kc, G.S.; Keromytis, A.D.; Prevelakis, V. Countering Code-Injection Attacks with Instruction-Set Randomization. In Proceedings of the 10th ACM Conference on Computer and Communications Security (CCS), New York, NY, USA, 27–30 October 2003; pp. 272–280.
35. Portokalidis, G.; Keromytis, A.D. Global ISR: Toward a Comprehensive Defense against Unauthorized Code Execution. In Moving Target Defense: Creating Asymmetric Uncertainty for Cyber Threats; Springer: New York, NY, USA, 2011; pp. 49–76.

36. Azab, M.; Hassan, R.; Eltoweissy, M. Chameleonsoft: A Moving Target Defense System. In Proceedings of the 7th International Conference on Collaborative Computing: Networking, Applications and Worksharing (CollaborateCom), Orlando, FL, USA, 15–18 October 2011; pp. 241–250.
37. Kohli, T. An Efficient Threat Detection Framework for Docker Containers using AppArmor Profile and Clair Vulnerability Scanning Tool. Master's Thesis, National College of Ireland, Dublin, Ireland, 2022.
38. Cho, J.-H.; Yoon, S.; Kim, D.S. Toward Proactive, Adaptive Defense: A Survey on Moving Target Defense. IEEE Commun. Surv. Tutor. 2020, 22, 709–745.
39. Lei, C.; Zhang, H.-Q.; Tan, J.-L.; Zhang, Y.-C.; Liu, X.-H. Moving target defense techniques: A survey. Secur. Commun. Netw. 2018, 3759626.
40. Debroy, S.; Calyam, P.; Nguyen, M.; Neupane, R.L.; Mukherjee, B.; Eeralla, A.K.; Salah, K. Frequency-minimal utility-maximal moving target defense against DDoS in SDN-based systems. IEEE Trans. Netw. Serv. Manag. 2020, 17, 890–903.
41. Aseeri, A.; Netjinda, N.; Hewett, R. Alleviating Eavesdropping Attacks in Software-Defined Networking Data Plane. In Proceedings of the 12th Annual Conference on Cyber and Information Security Research, New York, NY, USA, 4–6 April 2017; pp. 1–8.
42. Li, Y.; Dai, R.; Zhang, J. Morphing Communications of Cyber-Physical Systems Towards Moving-Target Defense. In Proceedings of the 2014 IEEE International Conference on Communications (ICC), Sydney, NSW, Australia, 10–14 June 2014; pp. 592–598.
43. Torquato, M.; Vieira, M. Moving target defense in cloud computing: A systematic mapping study. Comput. Secur. 2020, 92, 101742.
44. Duan, Q.; Al-Shaer, E.; Jafarian, H. Efficient Random Route Mutation Considering Flow and Network Constraints. In Proceedings of the IEEE Conference on Communications and Network Security (CNS), National Harbor, MD, USA, 14–16 October 2013; pp. 260–268.
45. Liu, J.; Zhang, H.; Guo, Z. A defense mechanism of random routing mutation in SDN. IEICE Trans. Inf. Syst. 2017, 100, 1046–1054.
46. Zhou, Z.; Xu, C.; Kuang, X. An Efficient and Agile Spatio-Temporal Route Mutation Moving Target Defense Mechanism. In Proceedings of the IEEE International Conference on Communications (ICC), Shanghai, China, 20–24 May 2019; pp. 1–6.
47. Ganz, J.; Peisert, S. ASLR: How Robust Is the Randomness? In Proceedings of the 2017 IEEE Cybersecurity Development (SecDev), Cambridge, MA, USA, 24–26 September 2017; pp. 34–41.
48. Bittau, A.; Belay, A.; Mashtizadeh, A.; Mazières, D.; Boneh, D. Hacking Blind. In Proceedings of the 2014 IEEE Symposium on Security and Privacy, Berkeley, CA, USA, 18–21 May 2014; pp.

227–242.