Hindawi
Security and Communication Networks
Volume 2020, Article ID 8882200, 15 pages
https://doi.org/10.1155/2020/8882200

Research Article

A Hybrid Cyber Defense Mechanism to Mitigate the Persistent Scan and Foothold Attack

Shuo Wang,[1,2] **Qingqi Pei**,[2,3] **Yuchen Zhang**,[1] **Xiaohu Liu**,[1] **and Guangming Tang**[1]

[1]*Information Science and Technology Institute, Zhengzhou 450001, China*
[2]*State Key Laboratory of Integrated Services Network, Xidian University, Xi'an 710071, China*
[3]*Shaanxi Key Laboratory of Blockchain and Secure Computing, Xidian University, Xi'an 710071, China*

Correspondence should be addressed to Qingqi Pei; qqpei@mail.xidian.edu.cn

Received 17 July 2020; Revised 1 September 2020; Accepted 26 September 2020; Published 21 October 2020

Academic Editor: Bela Genge

As the prerequisite for the attacker to invade the target network, Persistent Scan and Foothold Attack (PSFA) is becoming progressively more subtle and complex. Even worse, the static and predictable characteristics of traditional systems provide an asymmetric advantage for attackers in launching the PSFA. To reverse this asymmetric advantage and resist the PSFA, two new defense ideas, called moving target defense (MTD) and deception-based cyber defense (DCD), have been suggested to provide the proactive selectable measures to complement traditional defense. However, MTD is unable to defeat the sophisticated attacker with fingerprint tracking ability. Meanwhile, DCD is easy to be marked by the attacker, which will result in a great waste of defense resources and poor defense effectiveness. To address this shortcoming, we propose the hybrid cyber defense mechanism that combines the address mutation (belonging to MTD) and fingerprint camouflage (belonging to DCD) strategies. More specifically, we first introduce and formalize the attacker model of PSFA based on the cyber kill chain. Afterwards, the traffic direction technology is designed to realize the coordination between the strategy of address mutation and the strategy of fingerprint camouflage. Furthermore, we construct the fine-grained quantitative modeling of the attacker's behaviors through an in-depth observation of actual network confrontation. Based on this, a dynamic defense strategy generation algorithm is presented to maximize the effectiveness of our hybrid mechanism. Finally, the experimental results show that our hybrid mechanism can greatly improve the time required for a successful attack and achieve a better defense effect than the single strategy.

1. Introduction

Recent years have witnessed the fact that cyberattacks are gradually becoming a persistent, aggressive, and destructive threat that cannot be neglected [1]. Meanwhile, according to a recent report by Symantec [2], such attacks are getting gradually more sophisticated, which will make traditional cyber defense methods that focus on the reactive response after attacks ineffective.

According to cyber kill chain [3], the goal of the infection phase (including initial reconnaissance activities, attack weapon construction, and successful weapon delivery) is to establish a foothold in the target network, which is the prerequisite for the attacker to invade the target network and complete the attack. For illustration purposes, we call the series of attacks actions in the infection phase launched by the attacker the Scan and Foothold Attack (SFA for short). Obviously, any attacker who attempts to invade the target network and reach his target must first launch a successful SFA. Due to the existence of defense measures (such as firewall, intrusion detection system, intrusion prevention system, and so forth), attackers may not be able to launch the SFA successfully. However, in fact, if it fails, the subsequent attack cannot be carried out. As a result, attackers tend to launch SFA many times patiently, even if it will take them a lot of time. Particularly, advanced persistent threat (APT) attackers often lurk and repeatedly attack the target for a long period of time until they succeed. So based on the above considerations, in order to achieve a higher defense target, we assume that attackers will continue to launch SFA until successful and call this attack the Persistent Scan and Foothold Attack (PSFA for short).

In fact, traditional cyber defenses are useful in resisting PSFA. Firewalls can filter packets based on IP addresses or service ports to isolate attackers from the target network. However, smart attackers will use legitimate IP addresses to escape the limitation of firewalls. The intrusion detection system (IDS) and intrusion prevention system (IPS) can monitor the security status of the target network and interrupt, adjust, or isolate some abnormal behaviors. However, as passive defense technologies, IDS and IPS mainly focus on alarms generation after attacks, rather than defense in advance. Moreover, the missing alarms and the delay between attacks and alarms may cause the defender to miss the opportunity to stop the PSFA attacker. Therefore, the active defense measures that can provide additional selectable measures to complement traditional defense are urgently needed to resist PSFA.

Obviously, from the perspective of a defender, how to maximize the time required for a successful PSFA and delay its attack progress has become the top priority of cyber defense. In this paper, to better mitigate the PSFA, we develop the hybrid cyber defense mechanism that combines the address mutation and fingerprint camouflage strategies. More specifically, based on the cyber kill chain, we introduce and formalize the attacker model of PSFA in fine granularity. Then, our hybrid cyber defense mechanism is analyzed in detail. Furthermore, the quantitative modeling of attack analysis time is used to generate a dynamic defense strategy, which can maximize the time required for a successful attack. Finally, the experimental results confirm that the proposed hybrid mechanism can greatly improve the resistance of the system against the PSFA while keeping the system running reliably. The main contributions of this paper can be summarized as follows:

(1) To our knowledge, we are the first to formalize the attacker model of PSFA in fine granularity. According to the actual PSFA attack process, we describe it as a model with seven parameters, which will change with the progress of attack and defense.

(2) We propose the hybrid cyber defense mechanism that combines the address mutation and fingerprint camouflage strategies. The advantages of these two single defense mechanisms will be integrated to achieve better defense effect.

(3) As a proactive defense mechanism, our method can provide valuable time for traditional defense methods to resist PSFA. In addition, our method is easy to deploy and can coexist with traditional defense technologies.

2. Related Work

Apparently, gathering useful configuration parameters of the target network is a critical step towards launching a successful PSFA. However, the traditional cyber defense has two endogenous deficiencies: (i) the static nature of the conventional systems allows attackers enough time to probe the target network and gather information; (ii) conventional network defense mainly focuses on the reactive response after attacks have happened, rather than interfering with the attacker in the early stage of the cyber kill chain [4].

To overcome these two shortcomings, many proactive defense mechanisms have been widely adopted as alternative measures to disrupt and resist PSFA. Recent research on mainstream proactive defense mechanisms can be divided into two major categories: (i) moving target defense (MTD) [5–7] which aims at adding uncertainty and randomness in system configuration to ensure the information gathered by the attacker invalid; (ii) deception-based cyber defense (DCD) [8–10] which focuses on providing false information to confuse and deceive the attacker. For example, to enhance the network's resilience, Borbor et al. [11] developed an automated approach to diversifying network services under various cost constraints based on the extended resource graph model. In [12–14], the author presented an MTD mechanism called OpenFlow Random Host Mutation (OF-RHM) that can transparently mutate IP addresses with high unpredictability, while maintaining the normal work of the system. Moreover, there exist similar MTD technologies such as the shuffling of addresses, ports, and proxies [15–18].

Thus, although these single MTD mechanisms may result in some success in resisting automated worms and some low-level attackers, sophisticated attackers will make them invalid by combining multiple pieces of information (e.g., MAC address, operating system information, open ports, running services, and potential vulnerabilities) to identify these hosts whose single or limited system configuration parameters keep changing. To address this shortcoming, Connell et al. [19] presented a concurrent MTDs model that combines service reconfiguration and IP reconfiguration to improve defense effectiveness. Unfortunately, the two MTDs tend to interfere with each other, which will affect the normal operation of the system.

As for DCD, the author of [20] concentrated on generating a mix of true and false answers in response to scan requests from the attacker. However, there exist two noticeable drawbacks in their method. First of all, in fact, there is no guarantee that such mixed results generated through their method will not be distinguished by the sophisticated attacker. Second, when the system administrators perform normal network management tasks, these false answers may also confuse them. To improve the probability that the attacker will be deceived, Anwar et al. [21] designed a scalable algorithm to allocate honeypots based on the attack graph dynamically. On similar lines, Wang et al. [22] proposed an intelligent deployment strategy that can adaptively change the locations of honeypots according to the system security situation. Also, Tang and Sun [23] proposed a defensive mechanism that combines the IP randomization with decoy techniques to deceive the attacker. However, without the fingerprint camouflage mechanism, these above deception techniques may help in deceiving the attacker temporarily, but over a longer period of time, the sophisticated attacker will distinguish these tricks, thereby reducing the effectiveness of these defenses.

Moreover, unfortunately, relatively little attention has been paid to the effectiveness analysis of the above existing

works. Crouse et al. [24] proposed some probabilistic models to quantify the attack success rate. Hong and Kim [25] created a Hierarchical Attack Representation Model (HARM) to assess the effectiveness of MTD. However, these above models are only suitable to be used on simple attack scenarios, but not on complex PSFA scenario. In addition, game theory is widely used in quantifying the effectiveness of defense mechanisms [26]. For instance, Zhao et al. [27] described the interaction of the fingerprinting attack and its defense as a signal game model, whose equilibriums can be analyzed to select an optimal defense strategy. Feng et al. [28] demonstrated that MTD could be further improved when combined with information disclosure based on a Bayesian Stackelberg game model. Furthermore, Jajodia et al. [29] combined the reinforcement learning and Stackelberg game to create a Stackelberg honey-based adversarial reasoning engine. Wang et al. [30] proved that zero-determinant strategy would play a dominant role in the single-stage game. Also, Markov game theory has been extensively used by many scholars to address this problem [31–33]. The above works reveal that game theory is more suitable for describing simple scenarios where there exists a clear interaction between the defender and the attacker. However, intuitively, as a relatively complex scenario, PSFA is more often considered as the covert behaviors of the attacker, which leads to the fact that the game theory is unsuitable to describe the PSFA scenario.

Motivated by the aforementioned goals and challenges, we go one step beyond and show that MTD can be further improved when combined with DCD. In this paper, we develop the hybrid cyber defense mechanism that combines the address mutation and fingerprint camouflage strategies. By modeling and quantifying attack strategy and defense strategy, our hybrid mechanism can greatly improve the resistance of the system against the PSFA while keeping the system running reliably.

3. Attacker Model of PSFA

According to the cyber kill chain, a successful PSFA consists of at least three stages. Note that the attacker conducts the PSFA from outside the target network, with the goal of establishing a foothold (normal host) in the target network. In the first stage, the attacker will scan the target network to obtain the target network information (active hosts, open ports, running software, vulnerabilities, etc.). In the second stage, he will analyze the information obtained and build effective attack weapons. In the third stage, the attacker will make the connection to a host and intrude into it by using the attack weapons that have been made in the second stage. Thus, in a static network, since the IP addresses of the hosts are not changing, the attacker can directly use the effective IP address of an active host obtained in the first stage to carry out the attack in the third stage. Although address mutation can prevent ordinary attackers from using IP addresses to track and identify the hosts, it has no effect on sophisticated attackers. In this paper, we assume that the sophisticated attacker has two capabilities: (i) the sophisticated attacker can track and identify these hosts by distinguishing their host fingerprints which are composed of its MAC address, operating system information, open ports, running services, potential vulnerabilities, and other multiple pieces of information; (ii) for any vulnerability in the target network, the sophisticated attacker can successfully exploit it after a period of analysis. It should be noted that, in the following, the attacker in our model refers to the sophisticated attacker. As a result, when the defender implements the address mutation strategy, the attacker has no choice but to scan the target network again for active hosts in the third stage. In addition, in this case, it is clear that only if the attacker scans at least the same host in the first and third stages can he launch a successful attack.

As analyzed above, when the defender does not implement any defense strategy (static network), it is easy for the attacker to attack the target network successfully. When the defender implements the defense strategy of address mutation (address-hopping network), the attack success probability is greatly reduced. Also, the defender can deploy some fingerprint camouflage hosts (e.g., honeypots), so that the attacker's attention is deviated to them in order to reduce the success probability of the attack. However, in fact, the PSFA attackers will continue to attack until they succeed. For this reason, no matter what defense strategies the defender adopts, the persistent attacker will attack successfully through multiple attacks. To better understand the persistent attacker and provide a decision-making basis for more effective defense strategies, we construct the attacker model of PSFA based on the real-world scenarios of attack and confrontation. Note that our model can be applied to various network environments, including address mutation and fingerprint camouflage. The whole process of PSFA is shown in Figure 1.

To better describe the whole process of PSFA, the definition of targeted host is firstly given.

Definition 1. (Targeted Host). From the perspective of an attacker, when he scans a host, he will spend some time analyzing its vulnerabilities and constructing the weapons that can be used to invade the host successfully. After that, we call that the host has become a targeted host that can be invaded successfully by the attacker when the attacker scans it again.

Then, the whole process of PSFA can be divided into the following steps:

Step 1: the attacker scans the target network to discover active hosts.

Step 2: the attacker analyzes the potential vulnerabilities of the hosts discovered in the previous step and constructs the attack weapons.

Step 3: the attacker scans the target network to discover the targeted hosts. If there are no targeted hosts, the attacker will go to Step 2. In contrast, if there is at least one targeted host, the attacker will launch attacks on all targeted hosts simultaneously.

Step 4: if the targeted hosts contain at least one normal host, the attack will succeed. In contrast, if the targeted hosts contain no normal hosts, in other words, all the

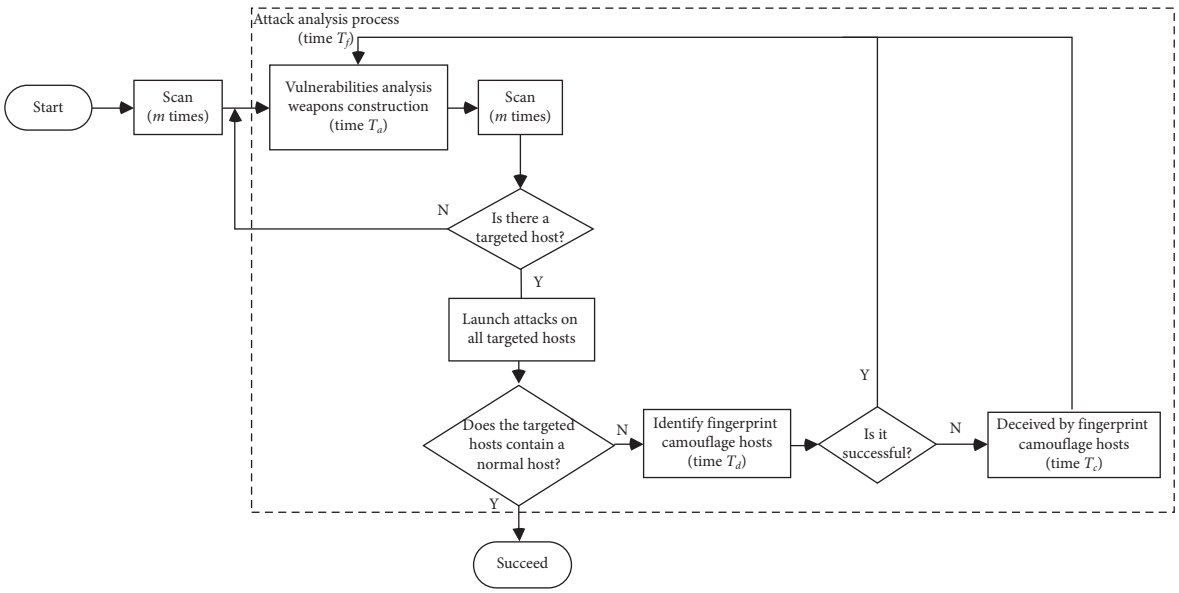

Figure 1: The whole process of PSFA.

targeted hosts belong to fingerprint camouflage hosts, as a result the attacker will spend some time identifying these fingerprint camouflage hosts.

Step 5: if the attacker does not identify these fingerprint camouflage hosts successfully, he will be deceived by them. In contrast, if the attacker identifies these fingerprint camouflage hosts successfully, he will go to Step 2.

As described above, the persistent attacker will continue to attack until he succeeds. Note that we call the series of actions of the attacker between any two scans an attack analysis process. To describe the PSFA more precisely, we give the definition of the attacker model of PSFA.

Definition 2. For the PSFA, the attacker model can be formalized as a six-tuple $attacker = (m, T_a, P_d, T_d, T_c, T_f)$, where

(1) m represents the maximum number of scanning times the attack can execute in any single scanning stage without being prevented by the defender. In other words, in the actual network confrontation, too many scans will reduce the concealment of the attack, so that the defender will more accurately identify and resist it by using more radical approaches (e.g., blocking its IP). In addition, it should be noted that, in order to ensure that the scanning process is hidden enough, sophisticated attackers will combine botnet and other scan tools (Nmap, Masscan, etc.) to accelerate the scanning process as much as possible. In addition, the process where the attacker uses these existing weapons to complete attacks is often very short [34]. Therefore, this paper assumes that the time spent in any scanning stage is ignored.

(2) T_a represents the spent time required for the attacker to complete vulnerabilities analysis and attack weapons construction after every scanning stage (vulnerability analysis time for short).

(3) P_d represents the probability that the attacker identifies the fingerprint camouflage host successfully. In fact, although the fingerprint of a fingerprint camouflage host is consistent with one of the normal hosts, the data and service activity in it cannot be completely the same as the normal host, so it is possible for high-level attackers to identify it successfully.

(4) T_d represents the time that the attacker spent identifying these fingerprint camouflage hosts.

(5) T_c represents the time to be deceived by fingerprint camouflage hosts if the attacker has not identified them successfully.

(6) T_f represents the time that the attacker will spend in an attack analysis process. Obviously, we can get

$$T_f = T_a + \sum T_d + \sum T_c. \quad (1)$$

The latter two items may or may not exist, which need to be determined according to the specific attack process.

4. Hybrid Cyber Defense Mechanism

According to Section 2, PSFA consists of several steps and will end with the attacker's success. Thus, the behaviors of both the attacker and defender can be regarded as a dynamic multistage process where the defender can adaptively adjust the defense strategy to balance the availability and security of the target network as well as to maximize the defense effectiveness. Note that although the PSFA attacker will end with success, the time required for a successful attack (from the start of the attack to the success of the attack) varies with

different defense strategies. As a result, the defender can quantify the effectiveness of a defense strategy by observing the time required for a successful attack when he implements this defense strategy.

Let the hopping interval of the defense strategy of address mutation be T_1. Upon further analysis, if the hopping interval is smaller than attack analysis time, that is, $T_1 < T_f$, the IP addresses of all hosts in the target network will change, which will lead to the IP addresses of active hosts discovered in the previous scan stage being invalid. Hence, any two scans in two scan steps can be regarded as two independent events; that is, the attacker's scanning strategy in the current scan step will be random scanning. In contrast, if $T_1 > T_f$, the IP addresses of the hosts may not have changed after time T_f, which will allow the attacker to combine repeated scanning and random scanning strategies. Note that repeated scanning strategy refers to the fact that the attacker scans the effective IP addresses (discovered in the previous scan step) in the current scan step again.

Furthermore, through the approximate probability calculation, it can be easily inferred that the attacker can greatly improve the scanning success probability by using the repeated scanning strategy, which will greatly reduce the time required for a successful attack. Therefore, it is important for the defender to make the hopping interval less than the attack analysis time as much as possible, which will lead to the IP addresses of active hosts discovered by the attacker in the previous scan stage being invalid and further increase the time required for a successful attack.

From the perspective of the defender, if the hopping interval of the defense strategy of address mutation is too small, the target network may not work well to provide its business function. Thus, we assume the minimum hopping interval is T_{need}, which can ensure the normal operation of the target network. In other words, when the defender implements the defense strategy of address mutation, he should ensure that the hopping interval is greater than the minimum hopping interval, that is, $T_1 > T_{\text{need}}$. In this case, when the attack analysis time is shorter than T_{need}, the attacker will use the repeated scanning strategy to reduce the effectiveness of the defense strategy of address mutation.

To overcome this limitation, this paper proposes an active fingerprint camouflage strategy by using traffic redirection technology, as shown in Figure 2.

As shown in Figure 2, when the attacker scans some IP addresses (including IP_1) and discovers a normal host $Host_1$ in Step 1, after the attack analysis time T_f that is shorter than T_{need}, according to the strategy of address mutation, the IP address of $Host_1$ will not change and remain IP_1. To prevent the attacker from using IP_1 to scan and locate $Host_1$ again in the next scan step, the defender can use the traffic redirection technology to redirect the source and destination addresses of the attacker's connections. Specifically, the defender rewrites the destination IP address of the connection (from the attacker to $Host_1$) to IP_{101} and the source IP address of the connection (from $Honeypot_1$ to the attacker) to IP_1, respectively. After that, the connection from the attacker to $Host_1$ will be redirected to $Honeypot_1$. In particular, it should be noted that the defender needs to ensure that the fingerprint of $Host_1$ is the same as that of $Honeypot_1$ in this traffic redirection process. As a special host designed by the defender to deceive the attacker, the fingerprint camouflage host contains the images of all normal hosts in the target network, so that the defender can disguise it as any normal host by converting its fingerprint into that of the normal host. Note that fingerprint camouflage hosts can be constructed by a virtual cloud platform or high-performance physical machine to ensure that the delay of fingerprint conversion process can be ignored. As a result, due to the consistency of fingerprints, the attacker will believe that the normal host $Host_1$ is connected in the two scan steps, which will make the attacker fall into a scam. Thus, it can be seen that the traffic redirection technology can make the attacker's repeated scanning strategy invalid without changing the normal host IP addresses, so as to ensure the normal operation of the target network. However, in fact, although the active fingerprint camouflage strategy can effectively compensate for the flaws and shortcomings of address mutation strategy, the sophisticated attacker may identify traffic redirection process through some abnormal characteristics (just like the round-trip time difference of network flows), which will improve the attacker's ability to identify the fingerprint camouflage hosts and reduce the defense effectiveness of fingerprint camouflage strategy to a certain extent.

Further analysis reveals that in order to effectively resist the attacker's repeated scanning strategy, when the attack analysis time is greater than T_{need}, the defender can implement the defense strategy of address mutation or active fingerprint camouflage; in contrast, when the attack analysis time is shorter than T_{need}, the defender cannot choose but implement the active fingerprint camouflage strategy.

However, in the real-world network confrontation, it is likely for some sophisticated attackers to identify this scam when the defender uses traffic redirection technology many times. In this case, the attacker can camouflage the source IP address of connections to avoid being identified by the defender, which will lead to the failure of the active fingerprint camouflage strategy. Therefore, in order to use traffic redirection technology as little as possible, we assume that the defender will implement the defense strategy of address mutation when the attack analysis time is greater than T_{need}.

As discussed above, to resist the PSFA, the fingerprint camouflage strategy can be divided into passive and active. The passive fingerprint camouflage strategy will be implemented in the following two situations:

(1) When the attacker discovers a normal host (marked as $Host_1$) in one scan step, and then he discovers a fingerprint camouflage host $Honeypot_3$ in the next scan step, the defender will disguise the $Honeypot_3$ as $Host_1$ by converting its fingerprint to ensure their fingerprints are consistent. Then, the attacker will mistake $Honeypot_3$ as $Host_1$ and attack it.

(2) When the active fingerprint defense strategy is implemented, the defender also needs to convert the fingerprint of the fingerprint camouflage host to that of the normal host discovered by the attacker in the

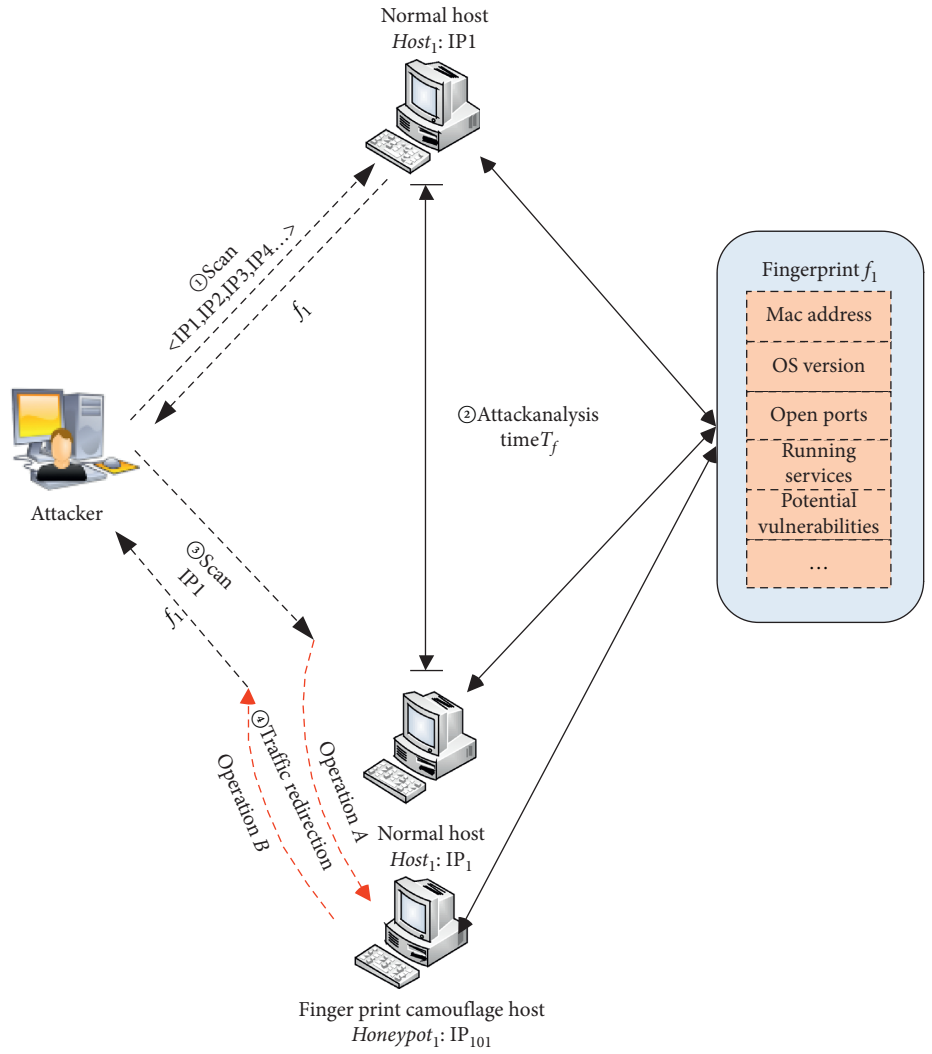

Figure 2: The active fingerprint camouflage strategy by using traffic redirection technology.

previous scan step in advance. For example, as shown in Figure 2, the fingerprint of $Honeypot_3$ will be converted to the fingerprint of the $Host_1$ before implementing the traffic redirection.

Thus, the passive fingerprint camouflage strategy can be regarded as the auxiliary strategy of the address mutation and active fingerprint camouflage strategies. In other words, when the address mutation and active fingerprint camouflage strategies are implemented, the passive fingerprint camouflage strategy will also be adjusted naturally. Hence, this paper focuses on how to dynamically coordinate address mutation and active fingerprint camouflage strategy to maximize defense effectiveness.

Note that the usefulness of our hybrid defense mechanism is to improve the time required for a successful PSFA and delay the attacker's attack process. In fact, our method and traditional defense methods can be complementary. First, traditional defense methods such as IDS and IPS tend to generate alarms and take some measures after the attack. However, the missing alarms and the delay between attacks and alarms may cause the defender to miss the opportunity to stop the PSFA attacker. In this case, our method can delay the attacker and provide valuable time for traditional defense methods to resist PSFA. Second, in our method, the condition for the successful implementation of the fingerprint camouflage strategy is the perception of the attacker's behavior, which can be achieved by the IDS and IPS. Moreover, in our attacker model of PSFA, m represents the maximum number of scanning times the attack can execute in any single scanning stage without being prevented by the defender. Obviously, the value of m depends on the performance of the IDS and IPS. Specifically, the better the performance of IDS and IPS, the smaller the value of m, and the attacker will spend more time launching a successful

PSFA. From the above analysis, we can see that our hybrid cyber defense mechanism can coexist well with traditional defense technologies.

5. Quantitative Modeling of Attack Analysis Time

As analyzed above, this paper quantifies the effectiveness of a defense strategy by observing the time required for a successful attack when the defender implements this strategy. To meet the needs of effectiveness quantification, we further construct the fine-grained quantitative modeling of attack analysis time through an in-depth observation of actual network confrontation:

(1) Note that the vulnerability analysis time T_a is related to the hosts that need to be analyzed by the attacker. Let V represent the set of hosts in the target network. Let Scan_i represent the set of hosts discovered by the attacker in the ith scan step. Obviously, $\text{Scan}_i \subseteq V$. Let $T_a\ (i+1)$ represent the vulnerability analysis time that the attacker will spend in the next attack analysis process. Then, we can get

$$T_a(i+1) = \begin{cases} f(\text{Scan}_i), & i = 1, \\ f\left((\text{Scan}_i) \backslash \left(\cup_{j=1}^{j=i-2} \text{Scan}_j\right) \cap \text{Scan}_i\right), & i \in \{3, 5, \ldots\}, \end{cases} \tag{2}$$

where $((\text{Scan}_i) \backslash ((\cup_{j=1}^{j=i-2} \text{Scan}_j) \cap \text{Scan}_i))$ represents the set of hosts that need to be analyzed by the attacker in the next attack analysis process. Obviously, hosts that the attacker has analyzed before the ith step no longer need to be analyzed. f represents the function from the set of hosts that need to be analyzed to the vulnerability analysis time, which is generally related to the attacker's ability, the number of vulnerabilities, and their complexities.

(2) Since the probability P_d is related to the fidelity of the fingerprint camouflage host, the attacker's ability, and the strategy of the defender, we can write it as

$$P_d(n) = 1 - \eta + \beta \cdot (n-1) + p_l \cdot \sigma_i, \tag{3}$$

where n represents the nth fingerprint camouflage host identified by the attacker, $\eta \in [0, 1]$ represents the fidelity of the fingerprint camouflage host, and β represents the influence of attacker's learning ability on P_d, which is described by the linear model. Generally speaking, the high-level attackers will continue to learn and accumulate experience in the attack process; that is, the more fingerprint camouflage hosts the attacker has identified, the higher his recognition ability. In addition, p_l represents the increased value of P_d when the defender implements the traffic redirection technology in the previous step. Accordingly, $\sigma_i = 0$ represents that the defender has implemented traffic redirection technology, and $\sigma_i = 1$ represents that the defender has not implemented the traffic redirection technology.

(3) Similarly, the time T_d is related to the fidelity of the fingerprint camouflage host, the attacker's ability, and the strategy of the defender. Then, we can write it as

$$T_d(n) = t_1 \cdot \eta - \delta_1 \cdot (n-1) - t_l \cdot \sigma_i, \tag{4}$$

where n represents the nth fingerprint camouflage host identified by the attacker, $\eta \in [0, 1]$ represents the fidelity of the fingerprint camouflage host, t_1 represents the influence of the attacker's initial ability on T_d, δ_1 represents the influence of attacker's learning ability on T_d, and t_l represents the decreased value of T_d when the defender implements the traffic redirection technology in the previous step.

(4) The time T_c is related to the fidelity of the fingerprint camouflage host and the attacker's ability, which can be written as

$$T_c(n_c) = t_2 \cdot \eta - \delta_2 \cdot (n_c - 1), \tag{5}$$

where n_c represents the n_cth fingerprint camouflage host mistakenly identified by the attacker, $\eta \in [0, 1]$ represents the fidelity of the fingerprint camouflage host, t_2 represents the influence of the attacker's initial ability on T_c, and δ_2 represents the influence of attacker's learning ability on T_c.

6. Dynamic Defense Strategy Generation

6.1. Dynamic Defense Strategy. As discussed above, it is important for the defender to correctly predict the attack analysis time of each attack analysis process. Let $D^P = \{D_i \mid i = 0, 1, 3, 5, \ldots\}$ represent the set of defense strategies for each step of PSFA, where D_i represents the defense strategy for the ith step. Let P_1 and P_2 represent the defense strategies of address mutation and active fingerprint camouflage, respectively. Then, D_i can be written as

$$D_i = \begin{cases} P_1\colon T^{P_1}(i) \geq T_{\text{need}}, & i = 0, \\ P_1\colon T^{P_1}(i) \approx \widetilde{T}_f(i+1), & \text{if } \widetilde{T}_f(i+1) > T_{\text{need}}, i = 1, 3, \ldots, \\ P_2, & \text{if } \widetilde{T}_f(i+1) \leq T_{\text{need}}, i = 1, 3, \ldots, \end{cases} \tag{6}$$

where $T^{P_1}(i)$ represents the hopping interval of P_1 which is implemented by the defender in the ith step. $\widetilde{T}_f(i+1)$ represents the attack analysis time of next step predicted by the defender in the ith step. Particularly, when $i = 0$ which indicates that there is no attack in the target network, the defender will implement address mutation strategy, and the hopping interval can be set according to the actual network situation, as long as it is greater than T_{need}. $P_1\colon T^{P_1}(i) \approx \widetilde{T}_f(i+1)$ means that the defender will

implement address mutation strategy in the ith step, and the hopping interval can be set slightly smaller than $\widetilde{T}_f(i+1)$. Hence, accurate prediction of $\widetilde{T}_f(i+1)$ becomes the key to defense strategy implementation. The specific prediction method is as follows.

6.2. Prediction of Vulnerability Analysis Time T_a. Let the set of hosts in the target network be $H = \{h_x \mid x = 1, 2, \ldots, v+p\}$, where v and p represent the number of normal hosts and fingerprint camouflage hosts, respectively. Let $NH = \{h_x \mid x = 1, 2, \ldots, v\}$ and $HH = \{h_y \mid y = v+1, v+2, \ldots, v+p\}$ represent the set of normal hosts and fingerprint camouflage hosts, respectively. Then, we can get $H = NH \cup HH$.

Furthermore, let Vul_x represent the set of vulnerabilities of host h_x. Accordingly, let Vul_Y represent the set of vulnerabilities of all hosts belonging to the host set Y.

According to Common Vulnerability Scoring System (CVSS), each vulnerability is identified by its common vulnerability enumeration identifier (CVE-ID), and each vulnerability can be divided into low-complexity vulnerability, medium-complexity vulnerability, and high-complexity vulnerability. Based on this, a row vector $C_{Vul_Y} = [L_{\text{num}}^{Vul_Y}, M_{\text{num}}^{Vul_Y}, H_{\text{num}}^{Vul_Y}]$ is created to represent the number of low-complexity vulnerability, medium-complexity vulnerability, and high-complexity vulnerability of the vulnerability set Vul_Y. Then, we can get

$$T_a(i+1) = \begin{cases} f(\text{Scan}_i) = g\left(\mathbf{C}_{Vul_{\text{Scan}_i}}\right), & i = 1, \\ f\left(\text{Scan}_i \setminus \left(\left(\cup_{j=1}^{j=i-2} \text{Scan}_j\right) \cap \text{Scan}_i\right)\right) = g\left(\mathbf{C}_{\left(Vul_{\text{Scan}_i}\right) \setminus \left(Vul_{\cup_{j=1}^{j=i-2} \text{Scan}_j}\right)}\right), & i \in \{3, 5, 7, \ldots\}, \end{cases} \tag{7}$$

where g represents the function from the set of vulnerabilities to the vulnerability analysis time. Then, we assume that

$$g\left(\mathbf{C}_{Vul_Y}\right) = t_L \cdot L_{\text{num}}^{Vul_Y} + t_M \cdot M_{\text{num}}^{Vul_Y} + t_H \cdot H_{\text{num}}^{Vul_Y}, \tag{8}$$

where t_L, t_M, and t_H represent the average time taken by the attacker to analyze a low-complexity vulnerability, medium-complexity vulnerability, and high-complexity vulnerability, respectively. Obviously, the values of these three parameters depend on the attacker's ability.

We assume that the defender knows the expression model of g but does not know the values of these three parameters (t_L, t_M, and t_H). However, the defender can infer the vulnerability analysis time of the next step based on historical attack data and then provide the basis for dynamic adjustment of defense strategy. For illustration purposes, let $\mathbf{C}_i = [L_{\text{num}}^i, M_{\text{num}}^i, H_{\text{num}}^i]$, $(i \in \{1, 3, 5, 7, \ldots\})$ represent the number of low-complexity vulnerability, medium-complexity vulnerability, and high-complexity vulnerability of the vulnerability set that needs to be analyzed by the attacker in the ith step. Then, we can get

$$T_a(i+1) = g(\mathbf{C}_i) = t_L \cdot L_{\text{num}}^i + t_M \cdot M_{\text{num}}^i + t_H \cdot H_{\text{num}}^i. \tag{9}$$

Therefore, the defender can use the multiple linear regression model to predict the vulnerability analysis time of the next step based on the historical attack data of previous steps. Let $\widetilde{T}_a(i+1)$ represent the prediction value of $T_a(i+1)$.

6.3. Prediction of the Probability That the Attacker Identifies the Fingerprint Camouflage Host Successfully. According to equation (3), the probability P_d is related to the fidelity of the fingerprint camouflage host, the attacker's ability, and the strategy of the defender.

In theory, the defender can estimate the parameters of equation (3) based on the historical data of identification fingerprint camouflage hosts, and the more historical data, the higher the accuracy of estimation. However, in the actual network attack and defense process, the historical data is scarce because the times when the attacker identifies the fingerprint camouflage host are often small, which will result in a low-precision estimation result. Moreover, equation (6) supports the conclusion that the smaller prediction value of $\widetilde{T}_f$ (compared to the actual vale T_f) will resist the stronger attacker. Hence, P_d can be predicted in the following formula:

$$\widetilde{P}_d(n) = \begin{cases} 1, & n = 1, \\ 0.5, & \forall dp_j = 0\,(1 \le j \le n-1, n \ge 2), \\ 1, & \exists dp_j = 1\,(1 \le j \le n-1, n \ge 2), \end{cases} \tag{10}$$

where $\widetilde{P}_d(n)$ represents the prediction value of P_d. $dp_j = 0\,(0 \le j \le n-1)$ indicates that the jth fingerprint camouflage host is incorrectly identified by the attacker. In contrast, $dp_j = 1\,(0 \le j \le n-1)$ indicates that the j th fingerprint camouflage host is correctly identified by the attacker.

The case of $n = 1$ in equation (10) shows that when the attacker identifies the fingerprint camouflage host for the

first time, the defender cannot predict the attacker's ability without the historical data and will assume that the attacker's ability is at the highest level; that is, the attacker will identify the fingerprint camouflage host correctly. In other cases, when the attacker correctly identifies the fingerprint camouflage host at a certain time, due to the accumulation of attacker's experience, it is reasonable to believe that the attacker will also correctly identify the fingerprint camouflage host later; when the attacker has not been able to correctly identify the fingerprint camouflage host before, we set $P_d = 0.5$.

6.4. Prediction of the Time That the Attacker Spent Identifying These Fingerprint Camouflage Hosts. According to equation (4), the time T_d is related to the fidelity of the fingerprint camouflage host, the attacker's ability, and the strategy of the defender. By similar reasoning, the defender can use the multiple linear regression model to predict T_d. Let $\widetilde{T}_d$ represent the prediction value of T_d.

6.5. Prediction of the Time to Be Deceived by Fingerprint Camouflage Hosts If the Attacker Has Not Identified Them Successfully. According to equation (5), the time T_c is related to the fidelity of the fingerprint camouflage host and the attacker's ability. Similarly, the defender can use the multiple linear regression model to predict T_c. Let $\widetilde{T}_c$ represent the prediction value of T_c.

6.6. Dynamic Defense Strategy Generation Algorithm. Based on the above analysis, the defender can generate the dynamic defense strategy, as shown in Algorithm 1.

7. Implementation and Analysis

In order to verify the effectiveness of our method, we conducted our experiments using Mininet to build the network topology and setting Ryu as the central controller based on Software Defined Networks (SDN). On this basis, learning from the currently popular idea of address mutation [12], we realize the target network with address hopping function. The topology of the experimental network is shown in Figure 3. Specifically, the central controller network consists of four servers: security awareness (SA) server, hopping control (HC) server, fingerprint camouflage (FC) server, and DNS server.

SA server integrates traditional defense technologies (e.g., FWs, IDS, IPS) to monitor the security status of the whole target network and provide the decision-making information as a basis for the HC server and FC server. The HC server can adaptively adjust the hopping interval and implement the hopping strategy according to the current network security status. The FC server manages all the fingerprint camouflage hosts and dynamically converts them according to the defense strategy. DNS server generates a unique and virtual domain name for each host in the target network. Before normal communication between different hosts, the source host will have to obtain the mapping relationship between a domain name and virtual IP address of the destination host by accessing the DNS server. Note that these hosts communicate via virtual IP address, and the central controller realizes address mutation by periodically transforming the mapping relationships between domain names and virtual IP addresses. In order to improve the security of the system, the central controller can use the domain name generator to periodically generate complex and irregular domain names, which can avoid attackers using virtual domain names to break through the address mutation network. Note that the number of normal hosts and fingerprint camouflage hosts in the target network can be dynamically adjusted according to the specific needs.

As mentioned above, although the PSFA attacker will end with success, the time required for a successful attack (form the start of the attack to the success of the attack) varies with different defense strategies. As a result, we can quantify the effectiveness of a defense strategy by observing the time required for a successful attack when he implements this defense strategy. According to our hybrid cyber defense, the behaviors of both the attacker and defender can be regarded as a dynamic multistage process where the defender can adaptively adjust the defense strategy to balance the availability and security of the target network as well as to maximize the defense effectiveness.

As a note, in our simulation experiments, let the size of address hopping space be 1000, the number of normal hosts be 50, and the number of scans implemented by the attacker in each scan step be 50. In addition, let the total times of attacks launched by the attacker be 100, and each attack is independent. Then, we take the average time required for 100 attacks as the time required for a successful attack. In addition, we also analyze the time taken by the attacker to be deceived (including T_d and T_c) in every attack. Similarly, we take the average time to be deceived for 100 attacks as the time taken by the attacker to be deceived. Furthermore, we select 100 different vulnerabilities (including 20 low-complexity vulnerabilities, 20 high-complexity vulnerabilities, and 60 medium-complexity vulnerabilities) from the National Vulnerability Database (NVD) as our vulnerability set *Vul*. And then, each host is deployed with three different vulnerabilities that are randomly selected from *Vul*. Also, according to the attack's ability, the attacker can be divided into three types: low-level attacker, medium-level attacker, and high-level attacker. The corresponding capability parameters of three different types of attackers are shown in Table 1.

As discussed above, the minimum hopping interval T_{need} is also a key factor to be considered in our hybrid defense strategy. Generally speaking, the value of T_{need} is closely related to the service type of the target network. Specifically, for domain name resolution, real-time simulation of combat, automatic driving, data synchronization, video conference, and other business types that require high network connectivity, T_{need} can be set larger. For general network services, T_{need} can be set smaller. In addition, too small T_{need} will increase the size of the flow table and then increase the pressure of the controller, which will affect the performance of the whole network. Although in the process of communication, once the addresses change, the host can resolve

Input: the number of normal hosts v, the number of fingerprint camouflage host p, the vulnerability set of each host $\{Vul_x \mid x = 1, 2, \ldots, v + p\}$, the fidelity of the fingerprint camouflage host η, the minimum hopping interval T_{need}, the size of address hopping space u, and the attacker model of PSFA *Attacker* (m, t_L, t_M, t_H, α, β, p_l, t_1, t_2, δ_1, δ_2, t_l).
Output: the defense strategy for each step $\{D_i \mid i = 0, 1, 3, 5, \ldots\}$
(01) Initialization of target network configuration and attacker model
(02) **for** $i = 0, 1, 3, 5, \ldots$
(03) $\text{Scan}_i = \text{Scan}(m)$
(04) **if** $i = 0$
(05) $(D_i \longmapsto P_1 \colon T^{P_1}(i) \geq T_{\text{need}})$
(06) **end if** (04)
(07) **if** $i = 1$
(08) $(D_i \mapsto P_2 \cup P_1 \colon T^{P_1}(i) = T_{\text{need}})$
(09) **end if** (07)
(10) **if** $i \geq 1$
(11) **if** $(\exists h_x (1 \leq x \leq v) \in ((\cup_{j=1}^{j=i-2} \text{Scan}_j) \cap \text{Scan}_i))$
(12) **break**
(13) **end if** (11)
(14) **if** $((\cup_{j=1}^{j=i-2} \text{Scan}_j) \cap \text{Scan}_i = \varnothing)$
(15) $(\tilde{T}_f(i+1) = \tilde{T}_a(i+1))$
(16) **end if** (14)
(17) **if** $(\exists h_x (1 \leq x \leq v) \in ((\cup_{j=1}^{j=i-2} \text{Scan}_j) \cap \text{Scan}_i)$ and $(\cup_{j=1}^{j=i-2} \text{Scan}_j) \cap \text{Scan}_i \neq \varnothing)$
(18) $(\tilde{T}_f(i+1) = 0)$
(19) **for each** $(h_y (v+1 \leq x \leq v+p) \in ((\cup_{j=1}^{j=i-2} \text{Scan}_j) \cap \text{Scan}_i))$
(20) $(\tilde{T}_f(i+1) = \tilde{T}_f(i+1) + \tilde{T}_d(h_y^n) + ((1 - \tilde{P}_d(h_y^n) \cdot \tilde{T}_c(h_y^{n_c})))$
(21) **end for** (19)
(22) $(\tilde{T}_f(i+1) = \tilde{T}_f(i+1) + \tilde{T}_a(i+1))$
(23) **end if** (17)
(24) **if** $(\tilde{T}_f(i+1) > T_{\text{need}})$
(25) $(D_i \mapsto P_1 \colon T^{P_1}(i) \approx \tilde{T}_f(i+1))$
(26) **end if** (24)
(27) **if** $(\tilde{T}_f(i+1) \leq T_{\text{need}})$
(28) $D_i \mapsto P_2$
(29) **end if** (27)
(30) **end if** (10)
(31) **Wait time** $T_f(i+1)$
(32) **end for** (02)
(33) **Return** $\{D_i \mid i = 0, 1, 3, 5, \ldots\}$

Algorithm 1: Dynamic defense strategy generation algorithm.

the new IP address of the destination host by visiting the DNS server. However, in fact, this process often causes high delays and affects the normal network service.

Therefore, we simulate the normal network service of the target network: within 4 hours, two different hosts communicate with each other every 10 minutes, and each connection is maintained for a certain period of time (connect time, CT). Through simulations, the relationship between the connection success rate and hopping interval under different conditions is shown in Figure 4.

As shown in Figure 4, the connection success rate increases with the increase of the hopping interval for different values of CT and will remain at a high level when the hopping interval reaches a certain value. Note that the connection success rate cannot reach 100%, and there exists certain randomness in it, which is affected by the specific communication environment of the target network. In addition, the longer the CT, the longer the hopping interval that meets the established requirements of the connection success rate. For this reason, this paper sets $CT = 60$ s and $T_{\text{need}} = 500$ s. Based on this, our experiments simulate the process of PSFA in which the hybrid cyber defense mechanism is implemented by the defender. First, we assume that the fidelity of the fingerprint camouflage host is 0.5 and study the effect of the number of fingerprint camouflage hosts on the effectiveness of our defense strategy, as shown in Figure 5.

Note that three different indicators are used to quantify the effectiveness of our defense strategy. They are the time required for a successful attack, the time to be deceived, and the ratio of the two. As shown in Figure 5, when the number of the fingerprint camouflage hosts is zero, it means that the defender only adopts the address mutation strategy and ignores the fingerprint camouflage strategy. In this case, the time required for a successful attack is short. When the number of the fingerprint camouflage hosts reaches 5, the values of these three indicators are greatly increased, which indicates that the fingerprint camouflage strategy improves the defense effect. However, when the number of the fingerprint camouflage hosts is more than 5, the values of these

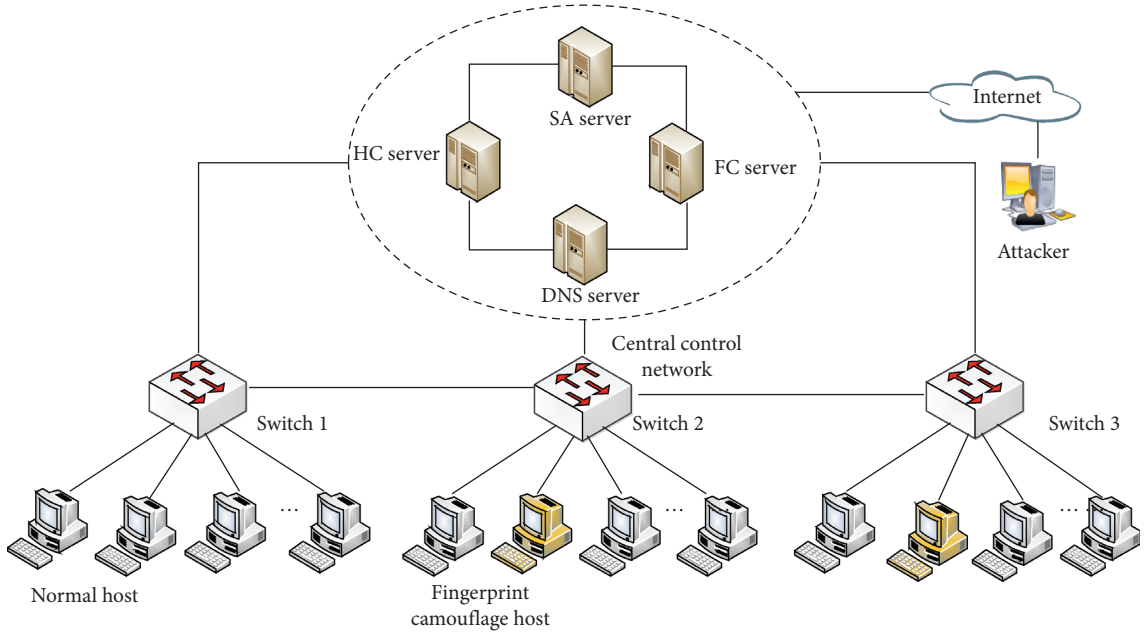

Figure 3: The topology of the experimental network.

Table 1: The corresponding capability parameters of three different types of attackers.

Types of attackers	$[t_L, t_M, t_H]$ (s)	β	p_l	t_1 (s)	δ_1	t_l (s)	t_2 (s)	δ_2
Low-level attacker	[120, 240, 400]	0.025	0.05	400	2.5	5	1600	10
Medium-level attacker	[60, 120, 200]	0.05	0.1	200	5	10	800	20
High-level attacker	[30, 60, 100]	0.1	0.2	100	10	20	400	40

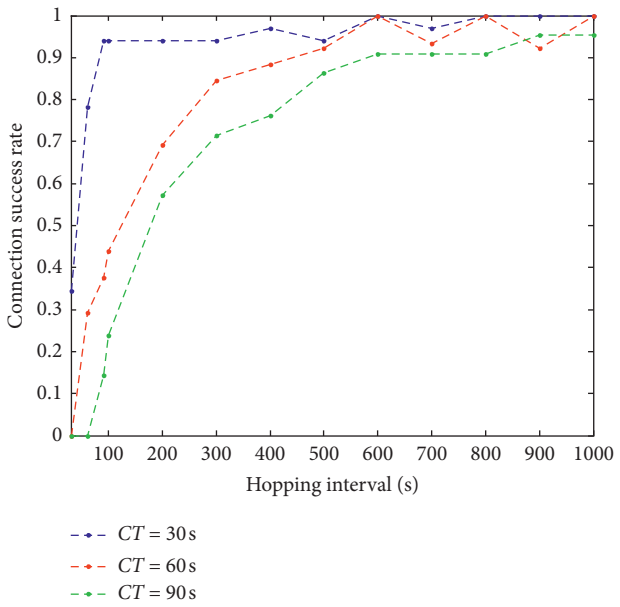

Figure 4: The relationship between the connection success rate and hopping interval under different conditions.

three indicators increase slowly with the increase of the number of fingerprint camouflage hosts.

Further analysis shows that the active fingerprint camouflage strategy can achieve a high defense effect as long as the number of fingerprint camouflage hosts in the target network meets the condition of implementing the traffic redirection traction technology, which means that the number of fingerprint camouflage hosts should be slightly larger than the expected number of the normal hosts discovered by the attacker in each scan step. In other words, our hybrid strategy can achieve a high defense effect without deploying too many fingerprint camouflage hosts, thus improving the utilization of defense resources. As mentioned above, the size of the address hopping space is 1000, the number of normal hosts is 50, and the number of scans implemented by the attacker in each scan step is 50. By calculating, we can see that the expected number of the normal hosts discovered by the attacker in each scan step is three. For this reason, in our hybrid strategy, we let the number of fingerprint camouflage hosts be five and further study the effect of the fidelity of fingerprint camouflage host on the effectiveness of our defense strategy, as shown in Figure 6.

As shown in Figure 6, the values of these three indicators increase approximately linearly with the increase of the fidelity of the fingerprint camouflage hosts. Therefore, improving the fidelity of the fingerprint camouflage host plays an important role in improving the defense effect, which is consistent with the actual practice of network attack and defense. Moreover, the experimental results show that, without any defense strategy, the time required for a successful attack of the low-level attacker, medium-level

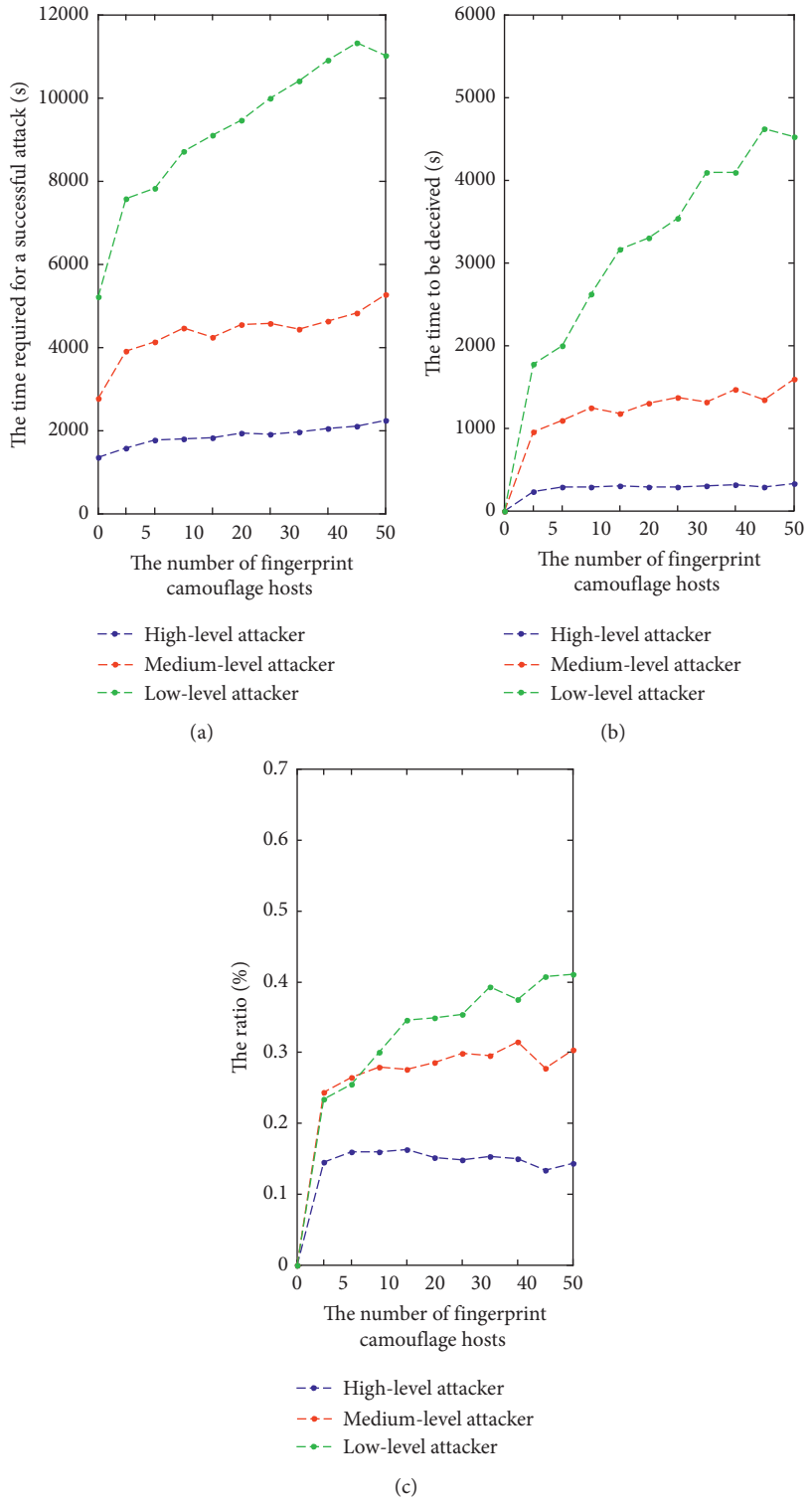

Figure 5: The effect of the number of fingerprint camouflage hosts on the effectiveness of our defense strategy.

attacker, and high-level attacker is 688 s, 349 s, and 163 s, respectively. On the other hand, in the actual network attack and defense, under the situation that the defender only implements the fingerprint camouflage strategy but not the address mutation strategy, the fingerprint camouflage hosts are easy to be marked by the PSFA attacker, which will result in a great waste of defense resources and poor defense effect.

Furthermore, we present a comparison with similar research on preventing attacks in the infection phase. The comparison results are summarized in Table 2. For a clearer

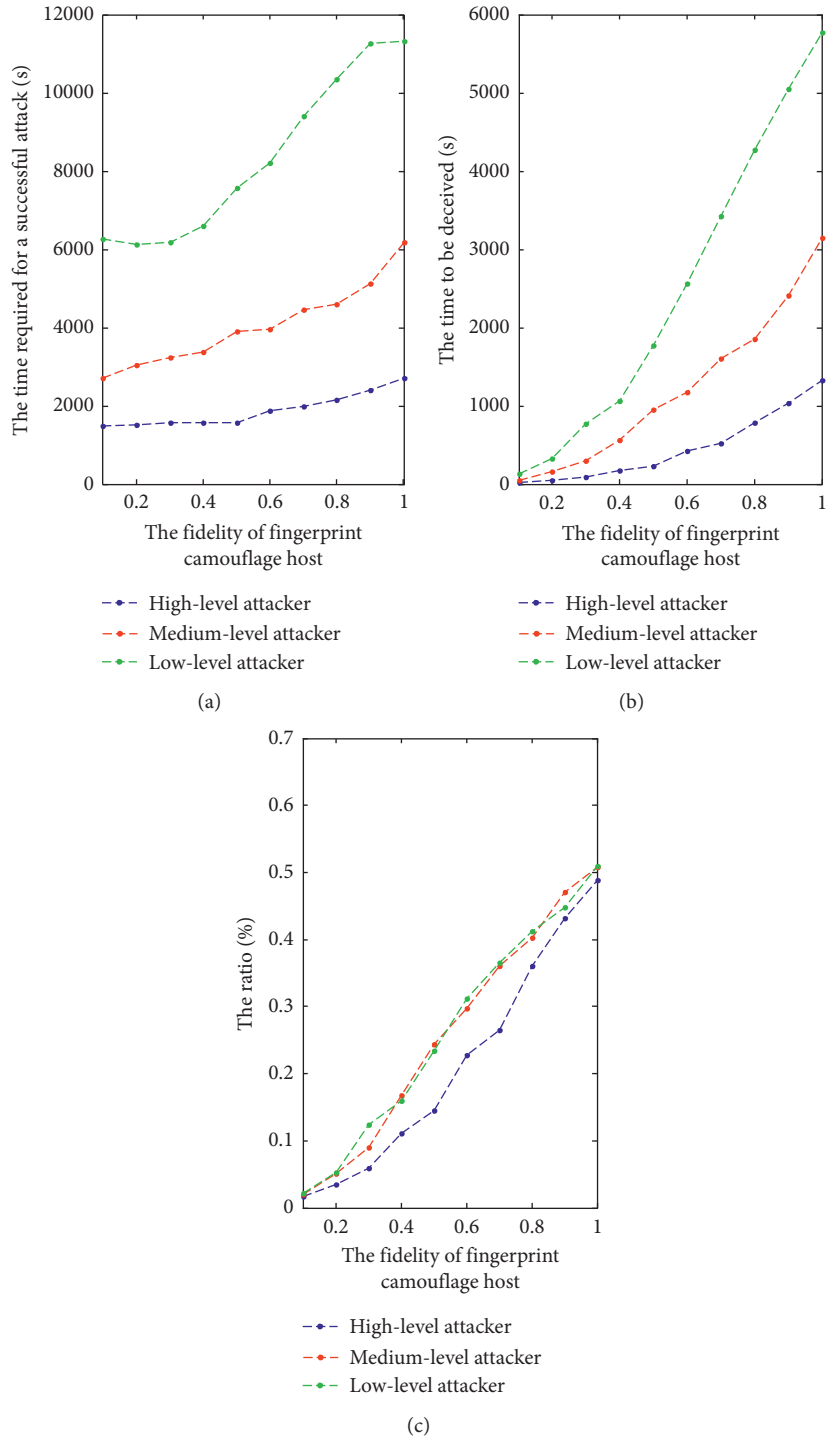

Figure 6: The effect of the fidelity of fingerprint camouflage host on the effectiveness of our defense strategy.

Table 2: Comparison summary.

Method	Detailed attacker model	Multistage attack	Hybrid mechanism	Dynamic strategy	Easy deployment
Ref. [14]	No	No	No	No	Yes
Ref. [20]	No	No	No	Yes	No
Ref. [24]	No	Yes	Yes	No	Yes
Ref. [35]	No	No	Yes	Yes	No
This study	Yes	Yes	Yes	Yes	Yes

comparison, we carefully selected five different indicators: detailed attacker model, multistage attack, hybrid mechanism, dynamic strategy, and easy deployment. First, the method with a detailed attacker model is convincing and valuable. Second, multistage attack accords with the reality of network confrontation. Third, the hybrid strategy is more effective than the single strategy. Then, the static policy is easy to be detected and identified by the attacker, so support dynamic strategy is significant. Finally, only if these methods are easy-to-deploy can they be widely used.

In [14], only the address mutation mechanism is designed to resist scan attack. In addition, the attack process is simplified by the hypothesis. In [20], generating mixed information is a difficult problem, which will make their method not easy-to-deploy. In [24], the attacker model is simple, and the defender only implements the static strategy, which makes it unable to resist complex PSFA. In [35], they integrate too many defense mechanisms, making it hard to deploy.

From the above comparisons, we can conclude that our method is the only one that has the detailed attacker model and support the dynamic strategy. In fact, to our knowledge, we are the first to formalize the attacker model of PSFA in fine granularity. To sum up, our hybrid cyber defense mechanism that combines the address mutation and fingerprint camouflage strategies can realize the dynamic adaptive evolution of the defense strategy, greatly improve the time required for a successful attack, and delay or even interrupt the attack progress, which could win sufficient time for the global network security defense and lay the foundation for ultimately defeating the PSFA attacker.

8. Conclusion

PSFA is the prerequisite and key foundation for the attacker to penetrate the target network. Meanwhile, attacks are getting gradually more sophisticated, making it difficult for the defender to mitigate PSFA. As a result, how to improve the effectiveness of defense against PSFA has become a key problem to be solved. Even worse, to our best knowledge, this attacker model of PSFA has never been analyzed and described in detail before. Therefore, this paper formalizes the attacker model of PSFA based on the cyber kill chain and processes a hybrid cyber defense mechanism to mitigate PSFA. Specifically, this paper designs three different defense strategies: address mutation, passive fingerprint camouflage, and active fingerprint camouflage. Furthermore, we develop the dynamic defense strategy generation algorithm to achieve the adaptive coordination of these three strategies. By rigorous theoretical analysis and actual simulation results, we confirm that our hybrid cyber defense mechanism can effectively mitigate PSFA. A possible goal for our future work would focus on the integration of more strategies and their effectiveness assessment.

Data Availability

The data used to support the findings of this study are available from the corresponding author upon request.

Conflicts of Interest

The authors declare that there are no conflicts of interest regarding the publication of this paper.

Acknowledgments

This work was supported by the National Key Research and Development Program of China (No. 2018YFE0126000), the Key Program of NSFC-Tongyong Union Foundation (No. U1636209), the National Natural Science Foundation of China (61902292), the Key Research and Development Programs of Shaanxi (Nos. 2019ZDLGY13-04 and 2019ZDLGY13-07), and the Fundamental Research Funds for the Central Universities (No. XJS201502).

References

[1] T. Alladi, V. Chamola, and S. Zeadally, "Industrial control systems: cyberattack trends and countermeasures," *Computer Communications*, vol. 155, no. 4, pp. 1–8, 2020.

[2] A. Alshamrani, S. Myneni, A. Chowdhary, and D. Huang, "A survey on advanced persistent threats: techniques, solutions, challenges, and research opportunities," *IEEE Communications Surveys & Tutorials*, vol. 21, no. 2, pp. 1851–1877, 2019.

[3] L. Martin, "Cyber kill chain (ckc)," 2017, https://www.lockheedmartin.com/en-us/capabilities/cyber/cyber-kill-chain.html.

[4] C. Wang and Z. Lu, "Cyber deception: overview and the road ahead," *IEEE Security & Privacy*, vol. 16, no. 2, pp. 80–85, 2018.

[5] R. Zhuang, S. Zhang, A. Bardas et al., "Investigating the application of moving target defenses to network security," in *Proceedings of the 2013 6th International Symposium on Resilient Control Systems (ISRCS)*, pp. 162–169, San Francisco, CA, USA, August 2013.

[6] C. Lei, H.-Q. Zhang, J.-L. Tan, Y.-C. Zhang, and X.-H. Liu, "Moving target defense techniques: a survey," *Security and Communication Networks*, vol. 2018, Article ID 3759626, 25 pages, 2018.

[7] S. Zhang, A. Chowdhary, A. Sabur et al., "A survey of moving target defenses for network security," *IEEE Communications Surveys & Tutorials*, vol. 22, 2020.

[8] K. E. Heckman, F. J. Stech, and B. S. Schmoker, "Denial and deception in cyber defense," *Computer*, vol. 48, no. 4, pp. 36–44, 2015.

[9] S. Thomas, *Cyber Deception: Building the Scientific Foundation*, Springer, Berlin, Germany, 2016.

[10] X. Han, N. Kheir, and D. Balzarotti, "Deception techniques in computer security: a research perspective," *ACM Computing Surveys*, vol. 51, no. 4, pp. 1–36, 2018.

[11] D. Borbor, L. Wang, S. Jajodia, and A. Singhal, "Optimizing the network diversity to improve the resilience of networks against unknown attacks," *Computer Communications*, vol. 145, pp. 96–112, 2019.

[12] J. H. Jafarian, E. Al-shaer, and Q. Duan, "OpenFlow random host mutation: transparent moving target defense using software defined networking," in *Proccedings of 2012 the first workshop on Hot topics in software defined networks*, pp. 127–132, Helsinki, Finland, August 2012.

[13] J. H. Jafarian, E. Al-shaer, and Q. Duan, "Adversary-aware IP address randomization for proactive agility against sophisticated attackers," in *Proccedings of 2015 IEEE*

conference on computer communication, pp. 738–746, Hong Kong, April 2014.

[14] J. H. Jafarian, E. Al-shaer, and Q. Duan, "An effective address mutation approach for disrupting reconnaissance attacks," *IEEE Transactions on Information Forensics and Security*, vol. 10, no. 12, pp. 2562–2577, 2015.

[15] M. M. Islam, Q. Duan, and E. Al-shaer, "Specification-driven moving target defense synthesis," in *Proccedings of 2019 ACM Workshop on Moving Target Defense*, pp. 13–24, London, UK, November 2019.

[16] S.-Y. Chang, Y. Park, and B. B. Ashok Babu, "Fast IP hopping randomization to secure hop-by-hop access in SDN," *IEEE Transactions on Network and Service Management*, vol. 16, no. 1, pp. 308–320, 2019.

[17] Q. Jia, K. Sun, and A. Stavrou, "MOTAG: moving target defense against internet denial of service attacks," in *Proceedings of 2013 22nd International Conference on Computer Communication and Networks (ICCCN)*, pp. 1–9, Nassau, Bahamas, July 2013.

[18] J. B. Hong, S. Yoon, H. Lim, and D. S. Kim, "Optimal network reconfiguration for software defined networks using shuffle-based online MTD," in *Proccedings of 2017 IEEE 36th Symposium on Reliable Distributed Systems (SRDS)*, pp. 234–243, Hong Kong, September 2017.

[19] W. Connell, L. H. Pham, and S. Philip, "Analysis of concurrent moving target defenses," in *Proccedings of 2018 ACM Workshop on Moving Target Defense*, pp. 21–30, New York, NY, USA, October 2018.

[20] S. Jajodia, N. Park, F. Pierazzi et al., "A probabilistic logic of cyber deception," *IEEE Transactions on Information Forensics and Security*, vol. 12, no. 11, pp. 2532–2544, 2017.

[21] A. H. Anwar, C. Kamhoua, and N. Leslie, "Honeypot allocation over attack graphs in cyber deception games," in *Proccedings of 2020 International Conference on Computing, Networking and Communications (ICNC)*, pp. 502–506, Big Island, HI, USA, March 2020.

[22] J. Sun, Q. Pei, J. Wang, Y. Zhang, and X. Liu, "An intelligent deployment policy for deception resources based on reinforcement learning," *IEEE Access*, vol. 8, pp. 35792–35804, 2020.

[23] J. Tang and K. Sun, "DESIR: decoy-enhanced seamless IP randomization," in *Proccedings of 2016 Annual IEEE International Conference on Computer Communications (INFOCOM)*, pp. 1–9, San Francisco, CA, USA, April 2016.

[24] M. Crouse, B. Prosser, and E. W. Fulp, "Probabilistic performance analysis of moving target and deception reconnaissance defenses," in *Proccedings of the second ACM Workshop on Moving Target Defense*, pp. 21–29, Denver Colorado, CO, USA, October 2015.

[25] J. B. Hong and D. S. Kim, "Assessing the effectiveness of moving target defenses using security models," *IEEE Transactions on Dependable and Secure Computing*, vol. 13, no. 2, pp. 163–177, 2016.

[26] J. Pawlick, E. Colbert, and Q. Zhu, "A game-theoretic taxonomy and survey of defensive deception for cybersecurity and privacy," *ACM Computing Surveys*, vol. 52, no. 4, pp. 1–28, 2019.

[27] Z. Zhao, D. Gong, and F. Liu, "An SDN-based fingerprint hopping method to prevent fingerprinting attacks," *Security and Communication Networks*, vol. 2017, Article ID 1560594, 12 pages, 2017.

[28] X. T. Feng, Z. Z. Zheng, D. Cansever et al., "A signal game model for moving target defense," in *Proceedings of IEEE Conference on Computer Communications (INFOCOM)*, pp. 1–9, Atlanta, GA, USA, May 2017.

[29] S. Jajodia, N. Park, and E. Serra, "SHARE: a stackelberg honey-based adversarial reasoning engine," *ACM Transactions on Internet Technology*, vol. 18, no. 3, pp. 1–41, 2018.

[30] S. Wang, H. Shi, Q. Hu, B. Lin, and X. Cheng, "Moving target defense for internet of things based on the zero-determinant theory," *IEEE Internet of Things Journal*, vol. 7, no. 1, pp. 661–668, 2020.

[31] C. Lei, H.-Q. Zhang, L.-M. Wan, and D.-h. Ma, "Incomplete information markov game theoretic approach to strategy generation for moving target defense," *Computer Communications*, vol. 116, pp. 184–199, 2018.

[32] A. Liu, S. Sengupta, D. Huang, and S. Kambhampati, "Markov game modeling of moving target defense for strategic detection of threats in cloud networks," in *Proccedings of AAAI Workshop on Artificial Intelligence for Cyber Security (AICS)*, pp. 1–9, Honolulu, HI, USA, January 2019.

[33] A. Chowdhary, S. Sengupta, A. Alshamrani, D. Huang, and A. Sabur, "Adaptive MTD security using Markov game modeling," in *Proceedings of 2019 International Conference on Computing, Networking and Communications (ICNC)*, pp. 577–581, Honolulu, HI, USA, February 2019.

[34] J. H. Jafarian and K. Das, "A novel permutational sampling technique for cooperative network scanning," in *Proccedings of 2019 International Conference on Privacy, Security and Trust (PST)*, pp. 1–6, Fredericton, Canada, August 2019.

[35] Q. Duan, E. Al-Shaer, and M. Islam, "CONCEAL: a strategy composition for resilient cyber deception: framework, metrics, and deployment," in *Autonomous Cyber Deception*, E. Al-Shaer, J. Wei, K. Hamlen, and C. Wang, Eds., pp. 101–123, Springer, Berlin, Germany, 2019.