A Survey On Deceptive Technologies

Navyashree R[1], Guruprakash C D[2], M Siddappa[3]

[1]*Dept. of Computer Science and Engineering, Sri Siddhartha Institute of Technology, Karnataka, India.*

[2] *Dept. of Computer Science and Engineering, Sri Siddhartha Institute of Technology, Karnataka, India.*

[3] *Dept. of Computer Science and Engineering, Sri Siddhartha Institute of Technology, Karnataka, India.*

Abstract: **Cyber deception has lately gained popularity as a possible strategy for proactive cybersecurity. The goal of cyber deception tactics is to purposely insert misleading information into the early stages of attack reconnaissance and preparation in order to display the final assault action harmless as well as ineffectual. Deception methods are frequently regarded as game changers in cyber protection. Deception improves system as well as component security through denial, deception, disinformation, disguise, and misdirection. This study provides a comprehensive description of the deception technology ecosystem. This paper offers a formal perspective about cyber deception technologies.**

Key words: **Cyber defense, deception techniques, honeypots, honeytokens.**

I. Introduction

"All warfare is based on deceit," Sun Tzu reportedly said [1]. This was decades before the invention of first digital gadgets. Since then, 2500 years ago, deceit has been an important component of many industries, including the military. Deception has always been an important part of military tactics over the years. Stoll [2] and Cheswick [3] used the notion of deception for defensive applications in 1986 and 1991, respectively. Honeypots were the name given to these applications. Later, the concept was broadened to include Deception technologies. Cohen's Deception Toolkit would be the first publicly released deception software [4]. Deception approaches have grown in prominence in computer security during the last three decades. In the scenario of insider threats as well as social engineering, perimeter-based security solutions like as firewalls and authentication procedures does not ensure an adequate degree of security. Defense-in-depth methods, such like signature-based intrusion detection and prevention, are frequently plagued by a high rate of false detection's, leading to alarm fatigue within security information as well as event managing systems.

In past few years, researchers have seen an increase in the frequency and complexity of advanced cyber attacks [5]. This issue impacts both organizations as well as end-users, causing serious psychological, societal, and financial harm to those who fall prey to it [6]. Unfortunately, despite various attempts to increase awareness about cyber assaults, attackers continue to be able to penetrate their target machine by utilizing several attack vectors like zero-day vulnerabilities, weaknesses in software systems, access control regulations, or through social engineering their intended target into reinstalling or executing malicious software..

To counter this dangerous trend, the security experts has suggested and created a slew of solutions for improving information and network system security. These conventional security measures, while necessary in any contemporary security armament, could provide a full response to Internet dangers. As a result, complementary methods have lately been researched in order to become more proactive at predicting risks and perhaps warning against assaults in their initial phases. Deception tactics, in particularly, have sparked a great deal of interest with in scientific community.

Deception is too wide a subject to discuss inside a single article, since it emerges in many forms in practically all security disciplines. As a result, the remainder of this article will solely address strategies using it as a defense mechanism to fool an intruder when he is engaging with target network.

II. MODELS OF CYBER DECEPTION

This section examines models involving cyber deception. We begin by going through the three stages of one round of deception and summarizing common deception strategies and activities.

A. Model of One-Round Deception

Cyber deception techniques are defined as "planned measures meant to deceive and/or confound attackers, causing them to perform (or not undertake) particular behaviors that help computer security defenses." [7]. In practice, an attacker might continue to probe a target machine in order to uncover possible vulnerabilities to exploit, whereas a defender could opt to upgrade its system on a frequent basis in order to resist reconnaissance and possible exploits. The cyber deception defensive architecture may be characterized almost as a two-party interactive procedure. The interaction of attackers and defenders evolves throughout time.

Three phases of actions may be included in each round of cyber deception.

1) Phase I (planning).

Defenders could first describe the objective of the deception which might plausibly be expected to be achieved during planning process of deception, based on preliminary understanding of adversaries like as their objectives, interests, and abilities. A deception tactic would contain a strategy for dealing with the adversaries. The defense will carefully balance its specifics of the deception strategy in order to maximize the deception strategy's chances of success while minimizing the impact on routine operations.

2) Phase II (implementing and deploying).

The deception strategy is put into action during this phase. Deception components may include devices (hosts or servers), data on devices, and connectivity among devices, depending on the deception strategy.

3) Phase III (monitoring and evaluating outcome)

It is the finale of one round of deceit. Because deception-based defense relies on influencing the attacker, it is critical to maintain track of the assailant's conduct and observe the attacker's response once deception is implemented.

B. Deception Schemes and Common Actions

Information simulation and dissimulation are the two major types of activities used in deception-based cyber defense. To conceal data, information dissimulation is widely utilized. Masking, repackaging, and dazzling are all common techniques [8].

1) Masking: Masking is an attempt to conceal or remove critical knowledge from target in hopes of avoiding exposure. Data masking methods such as substitution, encryption, and shuffling are frequently used to safeguard sensitive content like as personal identifying information.

2) Repackaging: The modification of essential aspects of the subject so that they appear unimportant or dissimilar from the original, with the hope that the attack's focus would be diverted away from the subject, is referred to as repackaging. IP address hopping [9] is a modern repackaging method in which computers on a network frequently have various IP addresses hence network flows are difficult for attackers to monitor.

3) Dazzling: Dazzling distorts or conceals important characteristics of the target without eliminating them, causing the target to be confused with unrelated things. Software obfuscation, for instance, conceals important areas of either of the source or running code.

Information simulation entails tactics such as mimicking, inventing, and decoying [10]. The goal of simulation would be to generate and disseminate false information in order to divert and confuse adversaries.

4) Mimicking: Creating a false entity by imitating crucial characteristics or the identity of some other genuine entity. It is one of the most prevalent simulation approaches. A honeypot [11], for example, can imitate a legitimate web site.

5) Inventing: Conjuring up non-existent entities with essential aspects and key qualities that appear genuine. There are important distinctions among mimicking as well as inventing. While the major criterion of mimicking is to build a counterfeit entity that seems to be the genuine thing, invention generates a novel entity that appears to be realistic.

6) Decoying: Among all simulation approaches, decoying has been the most commonly employed. A decoy is often an object that just seems or behaves like a genuine one. It is employed to divert attention away from the true target. In this part, we will go through deception strategies. These strategies are classified depending on their intended defensive surface.

III. Overview of Deception Techniques:

In this part, we will go through deception strategies. These strategies are classified depending on their intended defensive surface.

A. ***Host-based Techniques:***

In-host-system deception it typically allows an attacker to penetrate a target machine in a controlled approach. The target system's deception setting can be used to not only mislead the attacker, but also to assist defenders in gathering vital information about the attacker who has entered the system.

1) Honeywords [12], a recent work of in-host-system deception, generates extra hashed fake passwords for each user's account in a system. Even if a file holding hashed passwords is hacked and the hash value can be reversed, an adversary cannot distinguish a genuine password even from a similar-looking honeyword. When the attacker tries using the cracked albeit incorrect password, the program immediately detects the password hacking action.

Rauti et al. [13] examine entities that may be used to lure attackers into honeypots, including files, specified data content, databases, specific database records, data in RAM, file system metadata, user accounts, registry data, and operating system interfaces (e.g., system call numbering).

2) Honey Patches [14]: The purpose of a honey patch was to have a patched server respond to an attacker in the same way that a non-patched server might. This prevents information leakage by displaying an error message stating that the machine is no more vulnerable to a certain attack. It then generates a container that looks to be a compromised machine but contains censored information which the adversary cannot see.

A typical instance is honey patching, which reformulates regular security patches into honey-patches that might mislead adversaries by making it very difficult for any of them to assess whether or not a possible breach was successful. When a system recognizes an effort to attack, the honey patch directs the adversary to an unpatched decoy, where the assault is permitted to proceed. Meanwhile, the decoy setting allows the defense to acquire information about the assault and maybe discover previously hidden malware. Furthermore, employing a decoy, deception may be delivered to the intruder in the form of faked data or settings.

Unfortunately, due to the complexity of developing patches that simultaneously repair a vulnerability and offer signs to an attacker that it is still susceptible, this approach is exceedingly difficult to apply. Dazzling is used by honey patches to make it harder to differentiate between susceptible and non-vulnerable systems and to develop novel containers as honeypots

.

3) Ghost Patches: The authors [15] employ a similar strategy, generating software patches that include both genuine and fake vulnerability fixes. They make use of a common strategy used by attackers to discover vulnerabilities: reverse-engineering software patches. The purpose of their strategy is to waste an attacker's time by inserting "fake fixes" in updates that point to vulnerabilities which are not present.

This strategy is quite simple to implement. Their ghost patches include dazzling methods to distract from genuine patched vulnerabilities, as well as imitating and decoying strategies to trick an attacker into thinking they successfully exploited vulnerability.

4) System Compromise: Wang et al. [16] proposed using deception methods to improve detection of system breach attempts by developing multi-layer decoy architecture with decoys for user profiles, files, servers, and network / system activities. These decoys were designed to mask an organization's true assets and shield them from coordinated strikes. Rrushi [17] advocated using a fake Network Interface Controller (NIC) for Windows operating systems in a similar manner. This fake interface was purposefully built up to entice and identify malicious software which may be operating on the system.

Rowe et al. [18] implemented a proactive deception strategy to thwart system breach attempts. They proposed the use of counterfeit honeypots, which make ordinary but vital systems appear to be actual honeypots, thus confusing an attacker and diverting them away from compromised system. Similarly, Urias et al. [19] proposed to clone and move infected computers and position them in a false environment where system and network parameters are copied to imitate the genuine network environment.

5) Insiders: Kaghazgaran and Takabi [20] proposed extending role-based access control techniques with honey permissions to identify and prevent insider attacks. These are false permissions in the notion that they grant unauthorized access to only counterfeit versions of sensitive resources. The authors would discover insiders who prompted these malicious operations by tracking actions to access or alter such false assets.

B. Network-based Techniques:

A typical network assault scenario involves an adversary attempting to acquire control (or disable) of a valued target in network initially by scanning the network and then breaching into a susceptible system to obtain access to further devices in the network from the originally compromised device. To thwart the adversary from successfully breaching the network, the defender must interact with the assailant by inspecting incoming packets and attempting to identify the assailant's intent and capacity, and then respond by denying entry to systems and orchestrating inaccurate information to misguide attackers.

Several kinds of network-level data might possibly be modified or fabricated to fulfill a deceitful purpose,

1) Network topology information: The work in [21] proposes utilizing a changed network topology response to fool an opponent's traceroute probe, in which attacker frequently employs as the initial step in determining forward route of data packets.

2 Network host information: A movable honeypot system for industrial control systems was presented in [22]. This device may be installed in a variety of network locations to give an extra layer of security against attacker reconnaissance efforts. Furthermore, the system can alert the defense to oncoming assaults as soon as they occur.

Network tarpits [23] are often used in defensive cyber deception to disguise as many false hosts as feasible in order to trick or confound network scanners.

3) Network traffic information [24] offered an adaptive strategy to deceiving an attacker by actively collecting traffic data in an effort to get system fingerprints and discover a prospective target. The suggested misleading defensive strategy manipulates outgoing traffic to look like it was originated by a host with different system characteristics (e.g., operating system and service).

In their paper, Bringer et al. [25] explore numerous network-based approaches. Monitoring routing protocol assaults (e.g., RIP, OSPF) and hierarchical honeypots with low-fidelity wide-scoped introspection that pass "interesting" opponents to systems with higher-fidelity introspection depending on traffic patterns were among the papers reviewed. Rauti et al. [26] examine the entities that might be forged in order to lure enemies into honeypots.

4) Covert Authentication: The authors of [27] offer a unique method of employing concealed messages through two-factor authentication. Their method makes use of a mobile phone app that scans a QR code created by a server. The application then provides the user with various messages to transmit to the server secretly, and those two values are used to construct a response to the server. The server could then offer the user accordingly, potentially routing the client to a honeypot or blocking write-access.

This strategy is quite easy to implement. Current two-factor authentication techniques already employ mobile phones, so implementation is as trivial as an application update.

5) Dynamic Networking: Kewley et al. [28] originated the concept of infusing dynamic changes into a network in 2001. They disguised host addresses by building a network address translation (NAT) layer that modifies outward-facing identification information such as IP addresses and TCP/UDP port numbers on a regular basis. This method leverages dazzling tactics on certain systems by simulating fake or temporary network topologies.

.

C. Hybrid Techniques:

Hybrid deception approaches use a combination of host-based and network-based approaches to deceive adversaries. Sandia is still working on strategies that explicitly merge host-based and network-based deception. Their High-Fidelity Adaptive Deception & Emulation System (HADES) [29] replicates current network architecture and forks linked endpoint virtual computers to entrap intruders, analyze destructive activity, and secure production systems.

To maximize the efficiency of the deception, the hybridization of network and host deception incorporates a wide range of deceptive components such as masking, dazzling, mimicking, and decoying.

D. Cryptography based Techniques:

Honey encryption, a novel cryptographic primitive, was recently created to aid improve system resistance against brute force assaults [30]. A honey-encrypted ciphertext has the distinct quality that an attacker may use the incorrect key to produce a valid-looking output, however the attacker would be unable to tell if it is the right plaintext or otherwise. The honey encryption strategy allows the defense to thwart brute-force attackers that try to predict keys at arbitrary.

Honey encryption is based on a very precise distribution transforming encoder (DTE) across the message space. Unfortunately, the usage of DTE has a significant influence on the feasibility of honey encryption, owing to its inapplicability to increasingly complex structured data.

IV. Conclusions

The current state of the art in deception technology and related topics is provided in this paper. It was mentioned that deception technology is a useful enhancement to standard security. In this research, we described how to tackle cyber deception using technology. As a result, this paper conducted a quick study of a substantial body of work on deception strategies. The methods were classified as host-based, network-based, or hybrid.

Honeypot-based approaches are commonly used in host-based deception by enticing attackers into sandbox settings with monitoring capabilities. Modern advances in host-based deception investigate additional unique entities that can be faked. Furthermore, current strategies try to enhance software patches by incorporating honeypots in to the patches and concealing the weaknesses that patches address. Network-based deception strategies seek to conceal assets while capitalizing on developments in dynamic networking. Many of these approaches are used in hybrid systems to generate comprehensive deception capabilities, such as directing enemies to cloned networks generated on demand.

More exploration could be done to find ways to use deception at the data level (e.g., within a production machine, having fake data created when an attack is taking place), masking (making the truth inaccessible), or repackaging (making the truth appear to be something else). In terms of hybrid solutions, when deceptive layers are integrated to create deception systems, additional analysis on the effect of such deceptions may be conducted.

In the field of cyber security, cyber deception has a lot of potential since the technologies that provide host and network dynamism may be exploited as means to maneuver and fool the attacker. However, much more study is needed to move deceptions from basic, single-point approaches to successful system-based solutions.

References

[1] Wu Sun. *The Art of War*. Mens sana. Knaur, München, 2001

[2] Clifford Stoll. *The Cuckoo's Egg: Tracking a Spy Through the Maze of Computer Espionage* 1989 .

[3] Bill Cheswick. An evening with berferd in which a cracker is lured, endured, and studied.1991

[4] Fred Cohen. The deception toolkit home page and mailing list.1995

[5] Internet Security Threat Report . https://www.symantec.com/content/dam/symantec/docs/reports/istr-21-2016-en.pdf.

[6]Trend Micro. 2015. Understanding Targeted Attacks: The Impact of Targeted Attacks. https://www.trendmicro.com/vinfo/us/security/news/cyber-attacks/the-impact-of-targeted-attack.

[7] J. J. Yuill, *Defensive computer-security deception operations: Processes, principles and techniques*. ProQuest, 2006

[8] S. Grazioli and S. L. Jarvenpaa, "Deceived: under target online,"*Communications of the ACM*, vol. 46, no. 12, pp. 196–205, 2003.

[9] E. Al-Shaer, "Toward network configuration randomization for moving target defense," in *Moving Target Defense*. Springer, 2011, pp. 153–159.

[10] J. B. Bell and B. Whaley, *Cheating and deception*. Transaction Publishers, 1991.

[11] L. Spitzner, "Honeypots: Sticking it to hackers," *Network Magazine*,vol. 18, no. 4, 2003

[12] A. Juels and R. L. Rivest, "Honeywords: Making password-cracking detectable," in *Proc. of ACM CCS*, 2013.

[13] S. Rauti and V. Lepp¨anen, "A survey on fake entities as a method to detect and monitor malicious activity," in Parallel, Distributed and Networkbased Processing (PDP), 2017 25th Euromicro International Conference on. IEEE, 2017, pp. 386390.

[14] F. Araujo, K. W. Hamlen, S. Biedermann, and S. Katzenbeisser, "From patches to honey-patches: Lightweight attacker misdirection, deception, and disinformation," in Proceedings of the 2014 ACM SIGSAC conference on computer and communications security. ACM, 2014, pp. 942953.

[15] J. Avery and E. H. Spafford, "Ghost patches: Fake patches for fake vulnerabilities," in IFIP International Conference on ICT Systems Security and Privacy Protection. Springer, 2017, pp. 399412.

[16]Wei Wang, Jeffrey Bickford, Ilona Murynets, Ramesh Subbaraman, Andrea G. Forte, and Gokul Singaraju. 2013. Detecting Targeted Attacks By Multilayer Deception. Journal of Cyber Security and Mobility (2013).

[17] Julian L Rrushi. 2016. NIC displays to thwart malware attacks mounted from within the OS. Computers & Security (2016).

[18] Neil C Rowe. 2006. Measuring the effectiveness of honeypot counter-counterdeception. In IEEE Annual Hawaii International Conference on System Sciences (HICSS).

[19] Vincent E Urias, William MS Stout, and HanWLin. 2016. Gathering threat intelligence through computer network deception. In IEEE Symposium on Technologies for Homeland Security (HST).

[20] Parisa Kaghazgaran and Hassan Takabi. 2015. Toward an Insider Threat Detection Framework Using Honey Permissions. Journal of Internet Services and Information Security (JISIS) (2015).

[21] S. T. Trassare, R. Beverly, and D. Alderson, "A technique for network topology deception," in *Proc. of IEEE MILCOM*, 2013.

[22] E. Vasilomanolakis, S. Srinivasa, and M. Muhlhauser, "Did you really hack a nuclear power plant? an industrial control mobile honeypot," in *Proc. of IEEE CNS*, 2015.

[23] Wikipedia, "Tarpit (networking)," https://en.wikipedia.org/wiki/Tarpit%28networking%29.

[24]M. Albanese, E. Battista, and S. Jajodia, "A deception based approach for defeating OS and service fingerprinting," in *Proc. of IEEE CNS*, 2015.

[25]M. L. Bringer, C. A. Chelmecki, and H. Fujinoki, "A survey: Recent advances and future trends in honeypot research," International Journal of Computer Network and Information Security, vol. 4, no. 10, p. 63, 2012.

[26] S. Rauti and V. Lepp¨anen, "A survey on fake entities as a method to detect and monitor malicious activity," in Parallel, Distributed and Networkbased Processing (PDP), 2017 25th Euromicro International Conference on. IEEE, 2017, pp. 386390.

[27] M. H. Almeshekah, M. J. Atallah, and E. H. Spafford, "Enhancing passwords security using deceptive covert communication," in IFIP International Information Security Conference. Springer, 2015, pp. 159173.

[28] D. Kewley, R. Fink, J. Lowry, and M. Dean, "Dynamic approaches to thwart adversary intelligence gathering," in DARPA Information Survivability Conference & Exposition II, 2001. DISCEX01. Proceedings, vol.1. IEEE, 2001, pp. 176185.

[29] Sandia National Laboratories, High-Fidelity Adaptive Deception & Emulation System (HADES), https://ip.sandia.gov/technology.do/techID=187

[30] A. Juels and T. Ristenpart, "Honey encryption: Encryption beyond the brute-force barrier," *IEEE Security Privacy*, vol. 12, no. 4, 2014.