WWW.IJRPR.COM

International Journal of Research Publication and Reviews

Journal homepage: www.ijrpr.com ISSN 2582-7421

IoT Sentinel: Safeguarding IOT devices through Dynamic Honeypot Security Strategies

[1]Deepak Verma, [2]Aryan Gupta, [3]Mr. Mahesh Kumar Tiwari

[1 2]Student, scholar, Department of Computer Science, National PG College, Lucknow
[3]Assistant Professor, Department of Computer Science, National PG College Lucknow

ABSTRACT

The proliferation of Internet of Things (IoT) devices has brought numerous benefits to various industries, but it has also introduced significant security challenges. In response to the evolving threat landscape, the concept of honeypots has emerged as a valuable tool for detecting, analyzing, and mitigating attacks targeting IoT ecosystems. This research paper presents IoT Guard, a comprehensive honeypot security framework designed to enhance the security posture of IoT environments. Through the deployment of deceptive IoT devices and services, IoT Guard aims to lure attackers, gather threat intelligence, and strengthen defensive measures. This paper explores the architecture, components, deployment strategies, use cases, and real-world examples of IoT Guard, demonstrating its effectiveness in safeguarding IoT deployments against emerging cyber threats.

Introduction

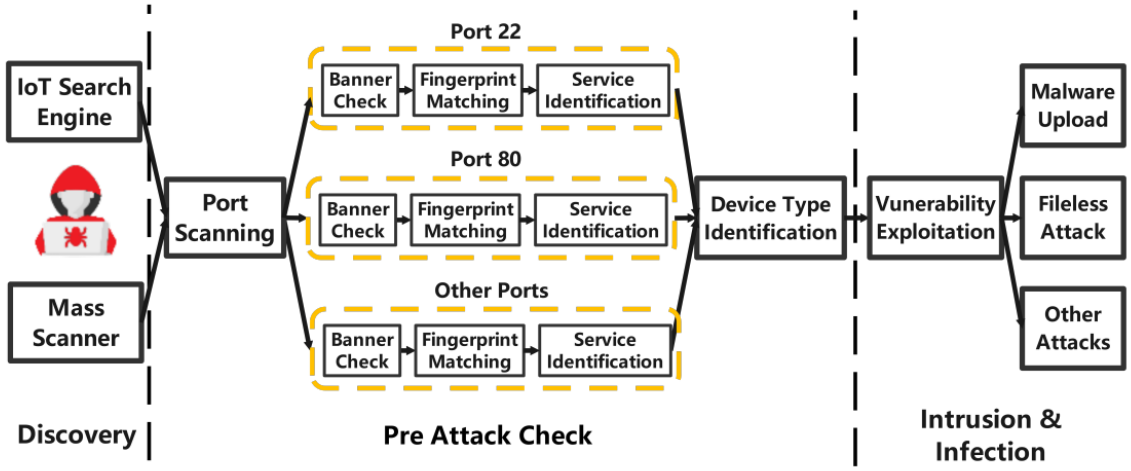
The rapid advancement of data processing and information technology in recent decades has led to one of the most significant innovations of this century: the Internet of Things (IoT). IoT combines the Internet with physical objects, enabling communication between these objects using RFID tags, sensors, actuators, and other devices without human intervention. The proliferation of the Internet has facilitated the growth of IoT, connecting devices through wired or wireless networks. Research into the origins of IoT traces back to the late 1960s when communication between computing devices began over computer networks. The introduction of TCP/IP in the early 1980s paved the way for the World Wide Web (WWW) in the early 1990s, fueling the expansion of the Internet and the subsequent rise of IoT in the late 1990s. The term "Internet of Things" was coined by Kevin Ashton, the executive director of the AutoID Center at the Massachusetts Institute of Technology (MIT), in 1999.

The exponential growth of the Internet has spurred the development of IoT applications across various fields, integrating into daily human life. However, as IoT applications rely on internet connectivity, security has become a critical concern due to the risk of data breaches and malicious attacks. Various types of attacks, such as Man-In-The-Middle (MITM), Sniffing, Denial of Service (DoS), Cryptographic attacks, Botnet attacks, Denial of Service (Dos), and Distributed Denial of Service (DDoS), pose significant threats to IoT systems.

This paper addresses the challenges of securing IoT devices against such attacks and proposes the use of honeypots as a solution. A honeypot is a strategic mechanism designed to mimic a server system, enticing potential hackers seeking unauthorized access to system data. Honeypots are used to monitor and analyze the behavior of attackers, providing valuable insights to enhance system security and prevent future attacks. They typically consist of a computer, applications, and information that simulate real system behavior to lure attackers.

Honeypots are categorized into two main types based on their deployment: production honeypots and research honeypots. Production honeypots are low-interaction systems that provide limited information about attacks, while research honeypots are high-interaction systems that offer detailed insights into attacker behavior, aiding organizations in defending against attacks. However, deploying and maintaining research honeypots can be challenging due to their complexity.

In this paper, we propose a solution using KF Sensor honeypot to enhance IoT security by effectively detecting and mitigating potential attacks, thus safeguarding IoT applications and networks.



The above figure illustrates the typical attack process targeting IoT devices. Initially, the attacker employs reconnaissance tools like Masscan or IoT search engines to discover vulnerable devices. Subsequently, the attacker conducts port scans and probes to gather additional information about the target device. Responses from the remote host can reveal known fingerprints of existing honeypots. For instance, open-source honeypots often exhibit limited banners or static HTTP responses, serving as fingerprints for identification by attackers.

During these preliminary checks, if the attacker detects honeypot fingerprints or inconsistencies between the simulated device and the provided service, they may suspect interaction with a honeypot. In response, the attacker might evade these honeypots by blacklisting their IP addresses or launching DDoS attacks to take them down. Moreover, the responses can help identify the services running on the remote host, aiding in pinpointing the type of victim IoT device. For example, if port scan results indicate video streaming services through RTSP on port 554 and a web server for camera control on port 80, the device is likely an IoT camera.

Once the remote host is identified, the attacker can speculate about existing vulnerabilities on the target IoT device and launch exploitation attacks. Successful attacks may lead to subsequent actions such as uploading malware or disabling the device. Honeypots serve as a defense mechanism against IoT device attacks, with conventional IoT honeypots primarily focusing on emulating specific protocols like telnet or SSH. However, attackers may notice missing services or limited interaction levels, raising suspicion.

To address these challenges, there is a growing need for adaptive high-interaction IoT honeypots capable of interacting with attackers, bypassing pre-attack checks, and misleading them into uploading malicious code. Such honeypots would enhance defense capabilities against sophisticated attackers in IoT environments.

Background and Related Works

A. Internet of Things

The IoT encompasses a vast network of connected physical objects, or "things," that communicate data with other devices and systems via the internet. These objects include sensors and actuators, which offer diverse services and enable the creation of semantic-rich applications. However, the heterogeneous nature of IoT devices and networks, driven by various manufacturers and communication protocols, exposes them to vulnerabilities such as weak or hardcoded passwords.

B. Honeypot for Cybersecurity

Deception techniques play a crucial role in cybersecurity, with honeypots being a prominent example. Honeypots are designed to deceive attackers or gather information about their attack patterns. They serve as a strategic tool for capturing attacks on IoT devices, offering insights into malicious activities. Honeypots are categorized based on their level of interaction, with high, low, and hybrid interaction levels, along with a newer concept of intelligent interaction based on machine learning.

C. Related Works

Low-Interaction Honeypots: Low-interaction honeypots provide attackers with limited interaction, emulating specific services or devices. While they are relatively simple to deploy, their fixed behavior makes them easily detectable by attackers.

High-Interaction Honeypots: High-interaction honeypots offer attackers full control over real operating systems, allowing for the collection of advanced information on cyber attacks. However, their complexity and resource consumption pose challenges in deployment and maintenance.
Intelligent-Interaction Honeypots: Intelligent-interaction honeypots optimize interaction with attackers to enhance attack detection. They emulate full devices and exhibit self-adaptability, offering versatility in capturing attacks.

Honeypots in IoT Security

A. Overview of Honeypots in IoT

Honeypots play a crucial role in bolstering the security of IoT devices by deceiving attackers and capturing valuable information about their tactics. They offer insights into emerging threats and help organizations enhance their cybersecurity posture in the face of evolving attack vectors.

B. Deployment Strategies for IoT Honeypots

Deploying honeypots in IoT environments requires careful consideration of factors such as interaction level, scalability, and resource utilization. Organizations must choose the appropriate honeypot deployment strategy to effectively mitigate cybersecurity risks.

Case Studies and Important Research

Kippo SSH Honeypot

Overview of the Kippo SSH Honeypot: The goal of this research is to examine and comprehend the strategies that attackers employ to compromise SSH services. Because SSH (Secure Shell) is frequently the subject of brute-force assaults and unauthorized access attempts, network defenders must thoroughly understand this topic.

Techniques:

1. Deployment: Kippo SSH honeypots, which usually resemble Linux-based SSH servers, are positioned strategically within network settings.
2. Monitoring: The honeypot watches for attempts by attackers to establish SSH connections and records their conversations.
3. Data Collection: During SSH sessions, hostile actors may run commands, attempt logins, and engage in other activities that are recorded.
4. Analysis: Examining recorded information to spot attack trends, like frequently used users, passwords, and attack instruments.

Principal Results:

1. Attack Patterns: Determining the most common SSH attack techniques, such as brute-force and dictionary-based password guessing.
2. Tool Usage: Finding attacker tools used to take advantage of SSH vulnerabilities, such as Hydra, Metasploit, or custom scripts.
3. Tactics: Information on how attackers move around and escalate their privileges in compromised systems after a compromise.
Importance:

- **Security Insights**: Offers insightful information about SSH attack methods and vectors, assisting in the creation of preemptive security plans.
- **Configuration Hardening**: Assists in enhancing SSH server setups and putting in place efficient access controls.
- **Threat Intelligence**: By spotting new attack patterns and guiding incident response procedures, collected data helps to build threat intelligence.

Dionaea Honeypot Study

The goal of the Dionaea honeypot study is to collect and examine malware samples as well as the actions of attackers on several network services, such as FTP, HTTP, SMB, and MySQL.

Techniques:

1. Service Emulation: In order to draw in and engage with attackers looking to take advantage of known vulnerabilities, Dionaea imitates weak network services.
2. Malware Capture: During exploitation attempts, attackers disseminate malware samples, which the honeypot records.
3. Behavior Analysis: Examining malware that has been captured to comprehend payload delivery techniques, infection channels, and attacker goals.
4. Data sharing: Sending malware samples and discoveries to antivirus software providers and security experts for additional debugging and analysis.

Principal Results:

1. Malware Collection: Dionaea gathers a wide variety of malware types that aim to compromise various protocols and services, offering important samples for malware study.

2. Attack strategies: Information on how to infiltrate susceptible systems using exploit kits and other propagation strategies. **3. Threat Intelligence**: By recognizing novel malware strains and comprehending the progression of cyberthreats, one can make a contribution to threat intelligence.

Importance:

• Malware Research: Aids in the development of efficient detection and mitigation techniques and allows for a thorough analysis of malware behavior.

• Security Cooperation: By sharing intercepted data with the cybersecurity community, cooperation and group defense against dynamic threats are promoted.

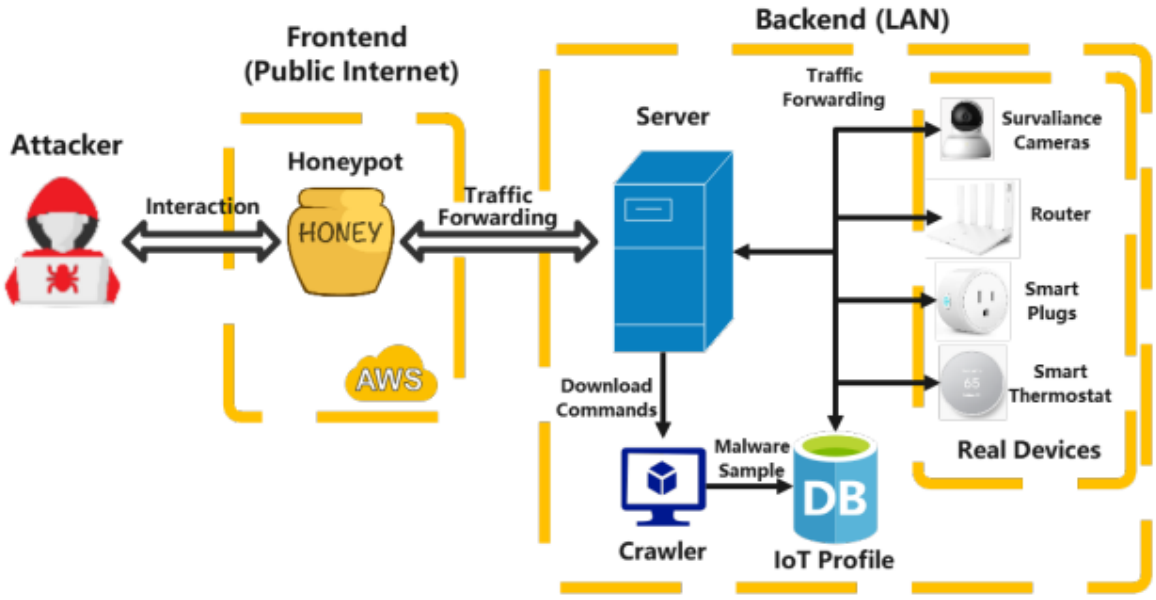
• Strengthening Defenses: To strengthen network defenses, intrusion detection signatures and firewall rules are developed using data from Dionaea honeypots.

The in-depth analyses of the Dionaea and Kippo SSH investigations demonstrate their usefulness in cybersecurity research. Researchers can obtain practical insights into malware patterns, attack strategies, and vulnerabilities that are exploited in the wild by utilizing honeypots such as Dionaea and Kippo. In order to effectively mitigate increasing cyber threats, the findings reinforce cyber defenses, improve incident response capabilities, and advance threat intelligence. An essential part of proactive cybersecurity efforts to comprehend, identify, and discourage hostile activity in network environments is the deployment and research of these honeypots.

Dynamic Attack Trace Acquisition from Real IoT Devices

A system has been developed for capturing attack traces resulting from interactions between attackers and authentic IoT devices. Illustrated in Figure, the setup comprises a frontend virtual machine hosted on AWS, a backend server for traffic management and initial traffic scrutiny, and a selection of IoT devices encompassing various models of cameras, routers, and smart plugs, each characterized by their respective vulnerabilities. The system engages with attackers by relaying received packets to designated IoT devices to observe their subsequent actions. Upon the attacker's requests, the relevant IoT device furnishes the necessary files or responses, facilitating the attacker's continued interaction. This iterative process persists until the attacker either uploads exploit code or ceases interaction with the IoT devices. The system diligently logs these traces and occasionally necessitates rebooting to recover from attacks. Subsequently, a fresh cycle commences, potentially targeting different IoT devices or protocols for varied attacker profiles.

To monitor and classify traffic events, the open-source SysFlow project [19] is leveraged, facilitating event-driven analysis to discern request types. Commands containing download instructions like Wget or Curl are meticulously filtered out and redirected to a sandbox-base.



Honeypot Limitations and Challenges

1. Legal and Ethical Concerns

• **Legality vs. Deception**: Running honeypots requires lying, which presents ethical and legal issues in some places. Businesses need to make sure that they are adhering to all applicable laws and rules on data privacy and cybersecurity procedures.

• **Data Capture:** Honeypots record potentially private details about attackers, such as their strategies and equipment. It is essential to handle and use personal data in a way that respects privacy rules.

2. Resource Intensiveness

• **Maintenance Overhead:** To stay safe and functional, honeypots need regular upkeep, surveillance, and updates. Budgetary and IT resource constraints may result from this.

• **False Positives**: Handling and examining data from honeypots may result in false positives, wasting time and energy looking into harmless activity.

3. Detection and Evasion by Attackers

• **Honeypot Identification**: The efficacy of honeypots can be compromised by skilled attackers who can identify and avoid them.

• **Attack Evasion**: Skilled adversaries can study defensive strategies using honeypots, and they can modify their approach to get around actual security measures.

4. Data Integrity and Misuse Risks

• **Data Integrity**: If honeypot data is compromised, attackers may alter it to confuse or mislead defenses.

• **Attackers' Misuse**: Honeypots may be used by attackers to initiate follow-up assaults or obtain unauthorized access to other areas of the network.

5. Deployment and Integration Challenges

• **Network Impact**: When honeypots are incorrectly installed, they can cause network disruptions or delay, which can impact users and services that are legitimate.

• **Integration with Security Infrastructure**: It can be difficult and necessitate specific knowledge to integrate honeypot data with current security procedures and technologies.

6. Limited Real-time Protection

• **Passive Nature**: The majority of honeypots don't actively thwart attacks in real time. They are more of a monitoring and detecting tool.

• **Need for Complementary Defenses**: In order to react quickly to threats that are detected, organizations must combine active defenses with honeypot installations.

Addressing Limitations and Challenges

In order to address the constraints and difficulties linked to honeypots, establishments may implement the subsequent tactics:

• Legal Compliance: Verify that the placement of honeypots complies with all relevant rules and legislation.

• Resource Allocation: Provide enough resources for data processing, monitoring, and honeypot upkeep.

• Continuous Improvement: To improve efficacy and lower detection risks, update and modify honeypot deployments on a regular basis.

• Data Protection: To prevent misuse or compromise of honeypot data, implement strong data protection procedures.

• Automation and Integration: To enhance incident response capabilities, automate and orchestrate the integration of honeypot data with current security processes.

REFERENCES:

[1] N. Neshenko, E. Bou-Harb, J. Crichigno, G. Kaddoum, and N. Ghani. Demystifying IoT security: An Exhaustive Survey on IoT Vulnerabilities and a First Empirical Look on Internet-Scale IoT Exploitations. IEEE Commun. Surveys & Tutorials, April 2019.

[2] O. Alrawi, C. Lever, M. Antonakakis, and F. Monrose. SoK: Security Evaluation of Home-Based IoT Deployments. IEEE Symp. on Security and Privacy, May 2019.

[3] O. Alrawi, C. Lever, K. Valakuzhy, R. Court, K. Snow, F. Monrose, and M. Antonakakis. The Circle Of Life: A Large-Scale Study of The IoT Malware Lifecycle. USENIX Security Symp., 2021.

[4] M. Ozmen, X. Li, A. Chu, Z. Celik, and X. Zhang B. Hoxha. Discovering IoT Physical Channel Vulnerabilities. ACM CCS, 2022.

[5] M. Antonakakis, T. April, M. Bailey, M. Bernhard, E. Bursztein, J. Cochran, Z. Durumeric, J. A. Halderman, L. Invernizzi, M. Kallitsis, et al. Understanding the Mirai Botnet. USENIX Security Symp., 2017.

[6] Mozi Botnet Accounts for Majority of IoT Traffic. https://threatpost.com/mozibotnet-majority-iot-traffic/159337/.

[7] Nmap: Open-source network scanner. https://nmap.org/.

[8] Shodan Honeyscore. https://honeyscore.shodan.io/.

[9] Send-Safe Honeypot Hunter. http://www.send-safe.com/honeypot-hunter.html.
[10] Y. Pa, S. Suzuki, K. Yoshioka, T. Matsumoto, T. Kasama, and C. Rossow. IoTPOT: Analysing the Rise of IoT Compromises. USENIX Workshop on Offensive Technol., 2015.
[11] Masscan. https://github.com/robertdavidgraham/masscan.
[12] Shodan: Search Engine for the Internet of Everything . https://www.shodan.io/.
[13] J. Franco, A. Aris, B. Canberk, and S. Uluagac. A Survey of Honeypots and Honeynets for Internet of Things, Industrial Internet of Things, and CyberPhysical Systems. IEEE Commun. Surveys & Tutorials, August 2021.
[14] S. Morishita, T. Hoizumi, W. Ueno, R. Tanabe, C. Gañán, M. van Eeten, K. Yoshioka, and T. Matsumoto. Detect Me If You. . . Oh Wait. An Internet-Wide View of Self-Revealing Honeypots. IFIP/IEEE Symp. on Integrated Network and Service Management, 2019.