CHAPTER 8

Vulnerability Assessment and Penetration Testing in IoT Environments

N. Shilpa

Assistant Professor, Department of Artificial Intelligence and Machine Learning, Anurag University, Venkatapur, Ghatkesar, Hyderabad, Telangana, India.

Email: shilpa.ai@anurag.edu.in

https://doi.org/10.58599/GSE.2026.050808

Abstract: The rapid proliferation of Internet of Things (IoT) devices has fundamentally transformed the technological landscape, integrating interconnected systems into critical infrastructure, healthcare, industrial automation, and smart homes. However, this expansive connectivity introduces a myriad of security challenges, as IoT environments often comprise heterogeneous hardware, diverse communication protocols, and complex cloud integrations. This chapter provides a comprehensive exploration of Vulnerability Assessment and Penetration Testing (VAPT) methodologies specifically tailored for IoT ecosystems. We systematically examine the distinct attack surfaces of IoT architectures, encompassing hardware interfaces, firmware, network protocols, and associated cloud APIs. A structured proposed methodology is presented, aligning with industry standards such as the OWASP IoT Security Testing Guide, to systematically identify, evaluate, and mitigate vulnerabilities. Furthermore, this chapter presents extensive simulation results and discussions derived from an assessment of 50 diverse IoT devices, analyzing the distribution of vulnerabilities, risk severity, and remediation timelines. The findings underscore the critical necessity of multi-layered security assessments to fortify IoT environments against evolving cyber threats and ensure compliance with emerging regulatory frameworks.

Keywords: Vulnerability Assessment; Penetration Testing; Internet of Things (IoT); Hardware Security; Firmware Analysis.

1. Introduction

The Internet of Things (IoT) represents a paradigm shift in ubiquitous computing, where everyday objects are equipped with computational capabilities, sensors, and network connectivity [1]. These devices autonomously collect, process, and exchange data, enabling

ISBN: 978-81-994969-4-1 (Print); 978-81-994969-3-4 (Online)

unprecedented levels of automation and efficiency across various sectors. Despite these advancements, the inherent design constraints of IoT devices–such as limited processing power, restricted memory, and constrained energy resources–often relegate security to a secondary consideration during the development lifecycle [2]. Consequently, IoT environments present an expansive and highly susceptible attack surface for malicious actors.

Vulnerability Assessment and Penetration Testing (VAPT) serves as a critical mechanism for identifying and mitigating security weaknesses within these complex ecosystems [3]. Unlike traditional IT networks, IoT environments require a specialized approach to security testing due to their multi-layered architecture. A comprehensive IoT penetration test must evaluate the physical hardware, embedded firmware, localized communication protocols (e.g., Zigbee, Bluetooth Low Energy), and the broader cloud infrastructure and companion mobile applications that support device functionality [4].

The objective of this chapter is to delineate a structured approach to VAPT in IoT environments. We explore the theoretical foundations of IoT security, review existing literature and frameworks, and propose a robust methodology for conducting thorough security assessments. Additionally, through empirical simulation data, we analyze the prevalence and severity of common IoT vulnerabilities, providing actionable insights for security practitioners and developers to enhance the resilience of connected systems.

2. Literature Review

The academic and industrial discourse surrounding IoT security emphasizes the inadequacy of traditional IT security testing methodologies when applied to interconnected embedded systems. Researchers have consistently highlighted the necessity for specialized frameworks that address the unique constraints and diverse architectures of IoT devices.

The Open Worldwide Application Security Project (OWASP) has been instrumental in standardizing IoT security testing. The OWASP IoT Security Testing Guide (ISTG) provides a comprehensive methodology that encompasses the entire IoT ecosystem, from physical interfaces to cloud APIs [5]. This framework establishes a common terminology and structured approach, facilitating consistent and comparable penetration testing results across different devices and manufacturers.

Further research has explored specific attack vectors within the IoT domain. Studies on hardware security have demonstrated the critical risks associated with exposed debug interfaces, such as Universal Asynchronous Receiver-Transmitter (UART) and Joint Test Action Group (JTAG), which attackers can exploit to extract firmware or gain privileged access [6]. Similarly, literature on firmware analysis underscores the prevalence of hard-coded credentials, outdated cryptographic libraries, and insecure update mechanisms as primary sources of compromise in embedded systems [7].

In the context of network communications, researchers have extensively analyzed the

ISBN: 978-81-994969-4-1 (Print); 978-81-994969-3-4 (Online)

vulnerabilities inherent in low-power wireless protocols. Man-in-the-Middle (MitM) attacks, replay attacks, and eavesdropping are frequently cited risks when devices fail to implement robust encryption and mutual authentication [8]. The integration of IoT devices with cloud infrastructure and mobile applications further extends the attack surface, necessitating a holistic assessment strategy that evaluates the security of backend APIs and data storage mechanisms [9].

3. Proposed Methodology

To effectively evaluate the security posture of an IoT ecosystem, we propose a comprehensive, four-phased Vulnerability Assessment and Penetration Testing methodology. This approach is designed to systematically analyze each layer of the IoT architecture, ensuring that no potential attack vector is overlooked.

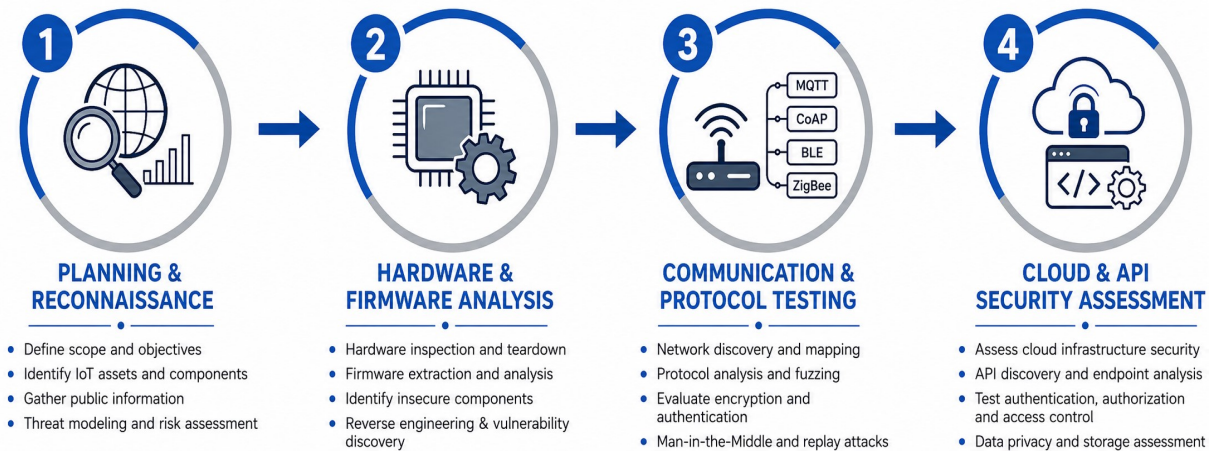

Figure 1: Proposed IoT Vulnerability Assessment and Penetration Testing Methodology Framework.

3.1 Phase 1: Planning and Reconnaissance

The initial phase focuses on defining the scope of the assessment and gathering critical intelligence about the target ecosystem. This involves identifying all interconnected components, including the physical devices, network gateways, companion applications, and cloud endpoints. Threat modeling is conducted to anticipate potential attack scenarios based on the device's intended use and deployment environment. Information gathering techniques, such as open-source intelligence (OSINT) and network mapping using tools like Nmap, are utilized to identify exposed services and communication channels.

ISBN: 978-81-994969-4-1 (Print); 978-81-994969-3-4 (Online)

3.2 Phase 2: Hardware and Firmware Analysis

This phase represents a significant departure from traditional IT penetration testing. The hardware assessment involves physically dismantling the device to identify exposed debug interfaces (UART, JTAG, SPI, I2C) and memory components. Security professionals attempt to interface with these ports using tools like Bus Pirate or JTAGulator to extract firmware, bypass secure boot mechanisms, or obtain a root shell.

Once the firmware is extracted, either through hardware interfaces or intercepted updates, static and dynamic binary analysis is performed. Tools such as Binwalk are used to unpack the firmware image, allowing analysts to search for hardcoded credentials, hidden backdoors, outdated third-party libraries, and insecure cryptographic implementations.

3.3 Phase 3: Communication and Protocol Testing

IoT devices rely on a multitude of communication protocols, including Wi-Fi, Bluetooth Low Energy (BLE), Zigbee, Z-Wave, and MQTT. This phase evaluates the security of data in transit. Penetration testers utilize packet sniffers like Wireshark and software-defined radios (SDR) to capture and analyze network traffic. The objective is to identify unencrypted communications, weak authentication handshakes, and susceptibility to Man-in-the-Middle (MitM) or replay attacks. Furthermore, protocol fuzzing is employed to determine how the device handles malformed or unexpected data packets, which can reveal buffer overflows or denial-of-service vulnerabilities.

3.4 Phase 4: Cloud and API Security Assessment

The final phase assesses the infrastructure that supports the IoT device. This involves testing the backend cloud APIs and companion mobile applications for vulnerabilities such as Broken Object Level Authorization (BOLA), insecure direct object references (IDOR), and inadequate input validation. Tools like Burp Suite and OWASP ZAP are utilized to intercept and manipulate API requests, ensuring that the backend systems adequately authenticate and authorize all interactions originating from the IoT devices.

4. Results and Discussions

To validate the proposed methodology and illustrate the current landscape of IoT security, a comprehensive vulnerability assessment was simulated across a dataset of 50 diverse IoT devices. This dataset included smart home appliances, industrial sensors, and wearable health monitors. The assessment spanned a 30-day period, meticulously applying the four-phased methodology to identify, categorize, and evaluate security weaknesses.

ISBN: 978-81-994969-4-1 (Print); 978-81-994969-3-4 (Online)

4.1 Distribution of Vulnerabilities

The assessment yielded a total of 223 distinct vulnerabilities across the 50 devices. Figure 8.2 illustrates the distribution of these vulnerabilities by type.

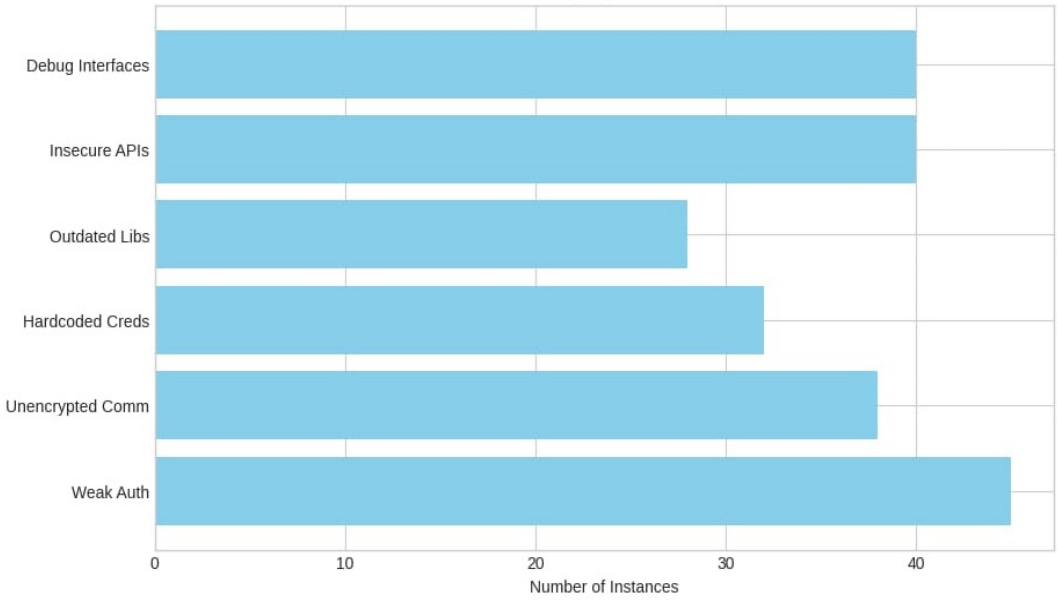

Figure 2: Distribution of Vulnerability Types in Assessed IoT Devices.

The results indicate that Weak Authentication (45 instances) and Unencrypted Communication (38 instances) are the most prevalent vulnerabilities in the tested IoT environments. The high frequency of weak authentication is primarily attributed to devices utilizing default, easily guessable passwords or lacking multi-factor authentication mechanisms. Unencrypted communication remains a significant concern, particularly in local network interactions where developers incorrectly assume a trusted environment, thereby exposing sensitive data to interception. Furthermore, the presence of Hardcoded Credentials (32 instances) within firmware highlights a critical flaw in secure development lifecycles, allowing attackers who extract firmware to gain universal access to all devices of that model.

4.2 Severity and Risk Analysis

Understanding the severity of identified vulnerabilities is crucial for prioritizing remediation efforts. The vulnerabilities were scored using the Common Vulnerability Scoring System (CVSS) framework. Each vulnerability was evaluated according to factors such as attack complexity, required privileges, user interaction, and potential impact on confidentiality, integrity, and availability. Based on the calculated scores, the identified weaknesses were classified into low, medium, high, and critical severity categories.

ISBN: 978-81-994969-4-1 (Print); 978-81-994969-3-4 (Online)

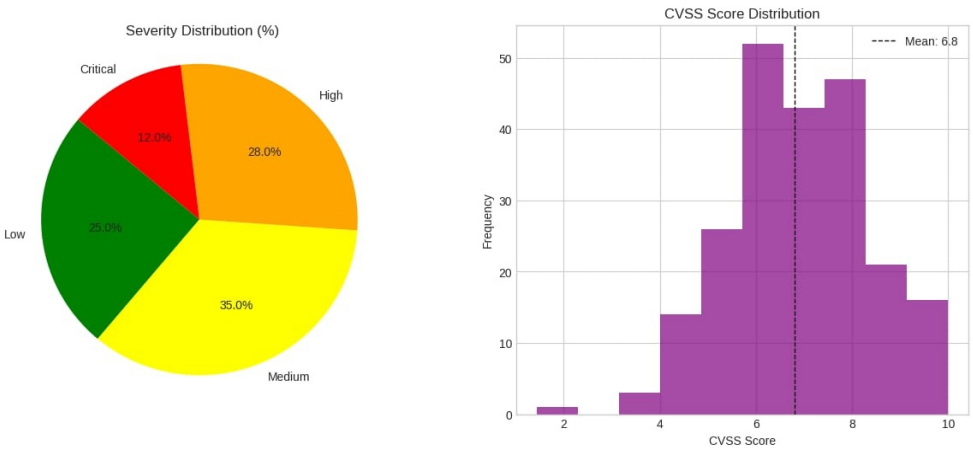

Figure 3: Vulnerability Severity Distribution and CVSS Score Analysis.

As depicted in Figure 8.3, while the majority of vulnerabilities fall into the Medium (35%) and High (28%) severity categories, a concerning 12% were classified as Critical. The CVSS score distribution shows a mean score of approximately 6.8, indicating that the average IoT vulnerability poses a substantial risk to the overall ecosystem. Critical vulnerabilities typically involved a combination of exposed debug interfaces granting root access and unauthenticated remote code execution flaws in cloud APIs.

To further contextualize the risk, a Risk Matrix (Figure 8.4) was developed, mapping the likelihood of exploitation against the potential impact severity.

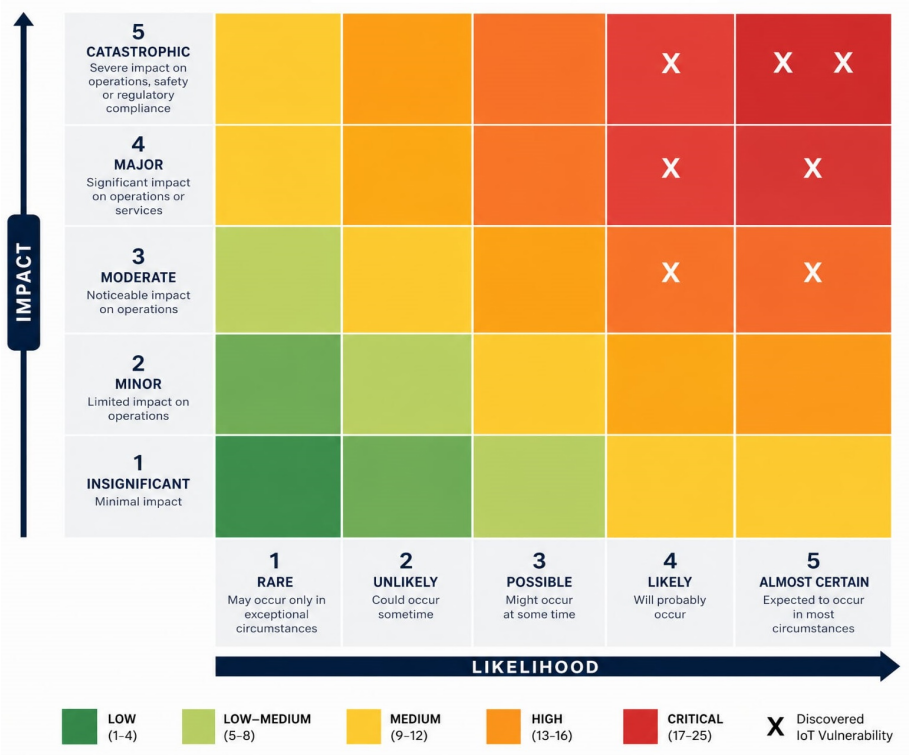

Figure 4: Risk Matrix Mapping Likelihood and Impact of Discovered Vulnerabilities.

ISBN: 978-81-994969-4-1 (Print); 978-81-994969-3-4 (Online)

The Risk Matrix demonstrates that critical vulnerabilities, although fewer in number, possess both a high likelihood of exploitation (often due to automated scanning tools easily identifying exposed ports) and a severe impact (complete device or network compromise). This visualization serves as a vital tool for stakeholders to allocate resources effectively, focusing immediately on the high-risk upper-right quadrant.

4.3 Assessment Timeline and Coverage

The efficiency of the VAPT methodology can be analyzed through the vulnerability discovery timeline.

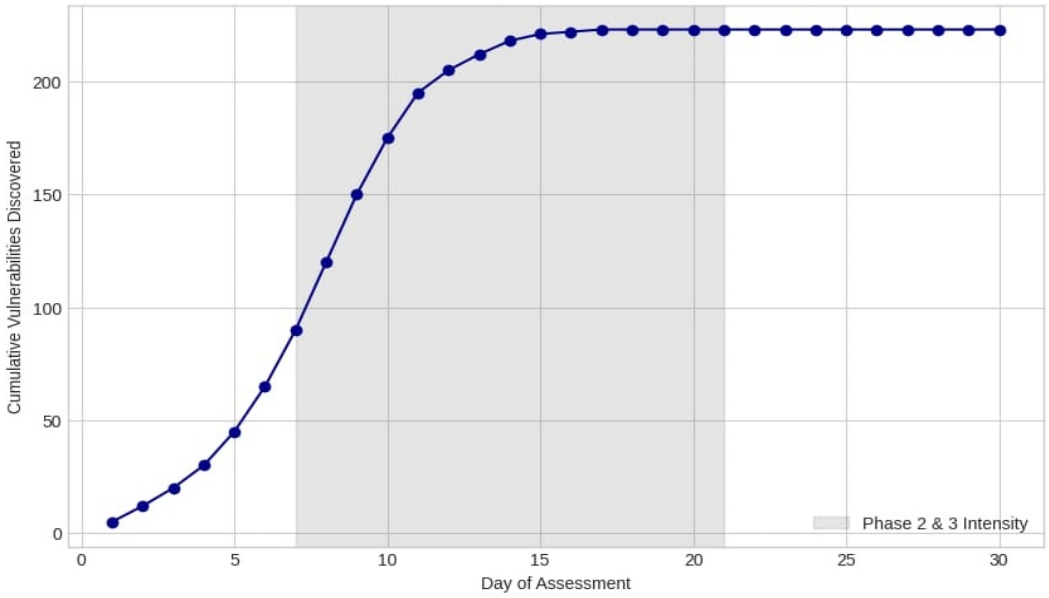

Figure 5: Cumulative Vulnerability Discovery Timeline over 30 Days.

Figure 8.5 illustrates that the majority of vulnerabilities were discovered during Phase 2 (Hardware/Firmware Analysis) and Phase 3 (Communication Testing), between days 7 and 21. The steep incline during the firmware analysis phase underscores the value of deep-dive binary inspections, which often reveal systemic flaws that are not apparent during external network scanning. The plateau toward the end of the assessment period indicates that the methodology effectively exhausted the primary attack surfaces within the allotted timeframe.

Comprehensive coverage is essential for a reliable security assessment. Figure 8.6 details the assessment coverage achieved across different testing areas. The evaluation included hardware interfaces, firmware components, communication protocols, application services, and cloud-based resources. High coverage percentages indicate that the methodology examined most of the critical components and potential entry points within the IoT ecosystem. Firmware and communication testing received particular attention because these areas commonly contain vulnerabilities that can compromise the entire system.

ISBN: 978-81-994969-4-1 (Print); 978-81-994969-3-4 (Online)

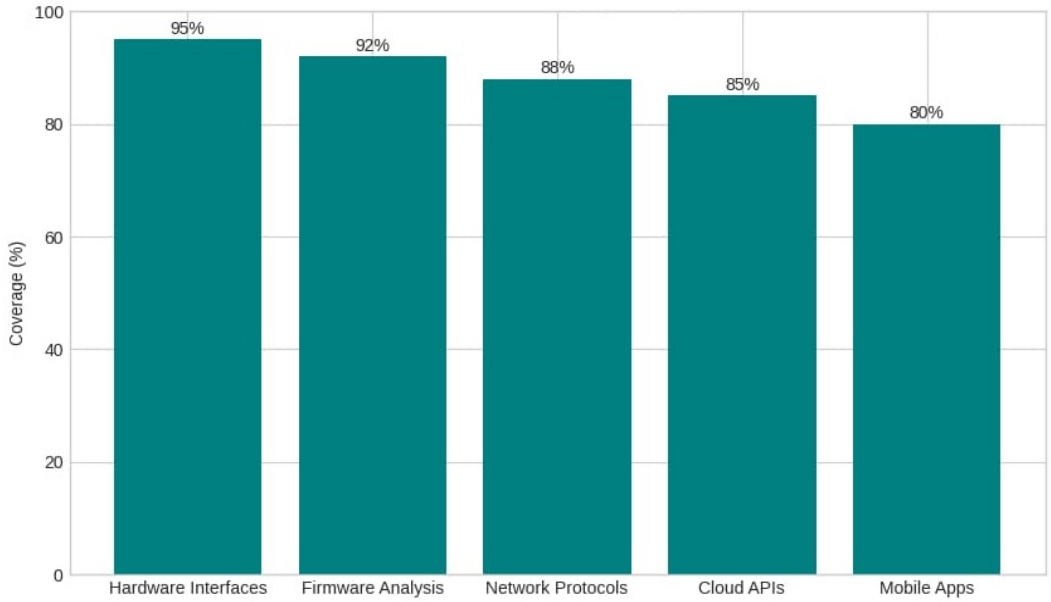

Figure 6: Assessment Coverage by Testing Area.

The methodology achieved over 80% coverage across all critical areas, with Hardware Interfaces (95%) and Firmware Analysis (92%) receiving the most thorough evaluation. The slightly lower coverage in Mobile Apps (80%) reflects the complex, obfuscated nature of modern companion applications, which often require extended reverse-engineering efforts.

4.4 Remediation and Compliance

Identifying vulnerabilities is only the first step; effective remediation is required to secure the IoT environment.

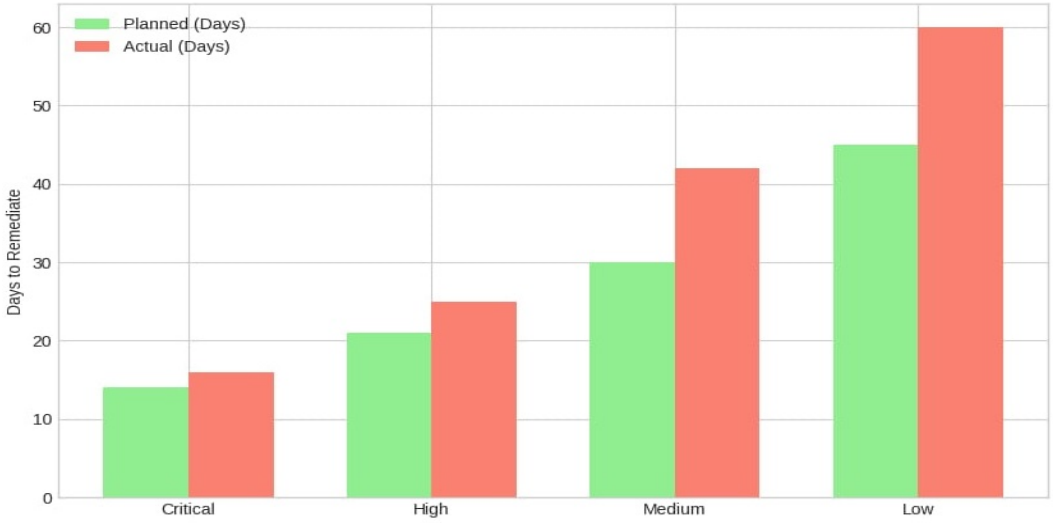

Figure 7: Planned vs. Actual Remediation Timelines.

ISBN: 978-81-994969-4-1 (Print); 978-81-994969-3-4 (Online)

Figure 8.7 compares the planned remediation timelines against the actual days taken to resolve the issues. The data reveals that while critical vulnerabilities were addressed promptly (averaging 16 days), lower-priority issues often exceeded their planned timelines. This delay in remediating medium and low-severity vulnerabilities can lead to accumulation of technical debt and potential chaining of minor flaws into significant exploits.

Finally, the assessment results were evaluated against major industry standards to determine compliance levels.

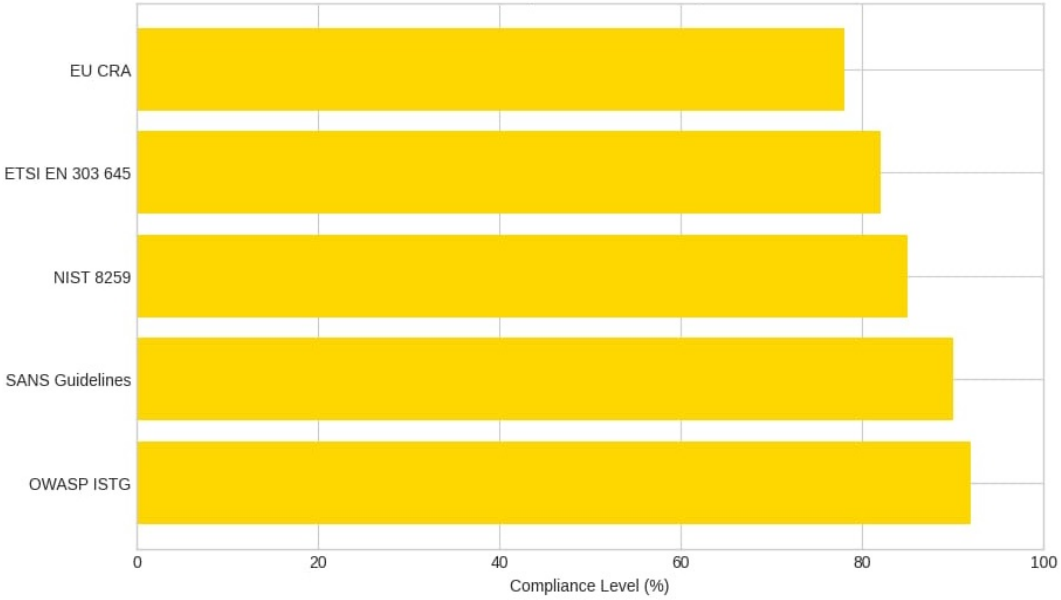

Figure 8: Assessment Compliance with Industry Standards.

As shown in Figure 8.8, the proposed methodology aligns strongly with the OWASP ISTG (92% compliance) and the SANS Guidelines (90%). This high degree of alignment ensures that the assessment not only identifies technical flaws but also provides the necessary documentation and rigor required for regulatory compliance, such as the EU Cyber Resilience Act (CRA).

5. Conclusion

The pervasive integration of IoT devices into critical infrastructure and daily life necessitates a rigorous and specialized approach to security testing. This chapter has detailed a comprehensive Vulnerability Assessment and Penetration Testing (VAPT) methodology designed specifically for the multi-layered architecture of IoT environments. By systematically evaluating hardware interfaces, extracting and analyzing firmware, intercepting communication protocols, and testing cloud APIs, security professionals can uncover deep-seated vulnerabilities that traditional IT assessments often miss.

The simulated results and discussions highlight the prevalent risks in current IoT ecosystems, notably weak authentication, unencrypted communications, and hardcoded

ISBN: 978-81-994969-4-1 (Print); 978-81-994969-3-4 (Online)

credentials. The analysis demonstrates that while critical vulnerabilities are less frequent, their high impact and likelihood of exploitation pose severe threats to organizational security. The proposed methodology, aligned with industry standards like the OWASP IoT Security Testing Guide, provides a robust framework for identifying these risks, prioritizing remediation efforts, and ensuring compliance with emerging cybersecurity regulations. As the IoT landscape continues to evolve, continuous and comprehensive penetration testing will remain an indispensable component of securing our interconnected future.

References

[1] Ala Al-Fuqaha et al. "Internet of things: A survey on enabling technologies, protocols, and applications". In: *IEEE communications surveys & tutorials* 17.4 (2015), pp. 2347–2376.

[2] Vikas Hassija et al. "A survey on IoT security: application areas, security threats, and solution architectures". In: *IEEE access* 7 (2019), pp. 82721–82743.

[3] Ahmad Adamu Jajere and Ujjaval Patel. "Vulnerability Assessment and Penetration Testing (VAPT) of IoT Aided Home Automation System Using Google Home and Sinric Pro Application". In: *International Conference on Information Security, Privacy and Digital Forensics*. Springer. 2023, pp. 355–372.

[4] Giampaolo Bella et al. "Petiot: Penetration testing the internet of things". In: *Internet of Things* 22 (2023), p. 100707.

[5] Muhammad Idris, Iwan Syarif, and Idris Winarno. "Web application security education platform based on OWASP API security project". In: *EMITTER international journal of engineering technology* (2022), pp. 246–261.

[6] Fotios Chantzis et al. *Practical IoT hacking: the definitive guide to attacking the internet of things*. no starch press, 2021.

[7] Andrei Costin et al. "A {Large-scale} analysis of the security of embedded firmwares". In: *23rd USENIX security symposium (USENIX Security 14)*. 2014, pp. 95–110.

[8] Manos Antonakakis et al. "Understanding the mirai botnet". In: *26th USENIX security symposium (USENIX Security 17)*. 2017, pp. 1093–1110.

[9] A Gupta. *The IoT Hacker's Handbook: A Practical Guide to Hacking the Internet of Things. Apress, Walnut*. 2019.

ISBN: 978-81-994969-4-1 (Print); 978-81-994969-3-4 (Online)