A Penetration-Testing Process for IoT Devices

Nguyễn Hoàng Hà
Thai Nguyen University of Information and Communication Technology
Thai Nguyen University, Thai Nguyen, Vietnam
dtc19h48020008@ictu.edu.vn

***Abstract*—This undergraduate thesis investigates a penetration-testing process for Internet of Things devices. Networked devices require repeatable security assessment across hardware, firmware, and communication interfaces. The student surveys IoT testing criteria, applies a documented process to a Honeywell IP camera, examines the reported weaknesses, and builds a Sofia-based screening tool. The thesis reports identified camera risks and a proof-of-concept analysis within the tested setup; it also documents a quick scan of devices using Sofia software. The findings concern the specific device and tool configuration in the manuscript. The summary does not establish vulnerability prevalence across other devices or safe operation in production networks. The contribution is a documented student study or prototype whose stated scope can guide further testing.**

***Index Terms*—IoT security, penetration testing, IP camera, vulnerability assessment**

I. Introduction

Networked devices require repeatable security assessment across hardware, firmware, and communication interfaces. This thesis investigates a penetration-testing process for Internet of Things devices. It begins from a practical engineering need and explains the technologies and workflow chosen for the case. The objective is to document a student implementation or comparative investigation, together with the evidence available in the manuscript. Broader operational or economic effects require separate measurements and are not assumed from the existence of a prototype [1]. Earlier ICTU student work on related designs is included here for context [2], [3], [4]. Related published studies provide context for the subject and methods [5], [6], [7], [8], [9], [10]. These contextual works were selected for this English summary; they are not asserted to appear in the original thesis bibliography.

II. Methods

The student surveys IoT testing criteria, applies a documented process to a Honeywell IP camera, examines the reported weaknesses, and builds a Sofia-based screening tool. The source is summarized through its stated design, implementation material, examples, and conclusion. Features shown in the manuscript are distinguished from proposals for later development. This review does not add a new experiment, fill missing measurements with estimates, or treat a planned capability as an observed result. The source thesis remains the provenance for the reported work [1].

Supervisor: Nguyễn Anh Chuyên, Thai Nguyen University of Information and Communication Technology (nachuyen@ictu.edu.vn).

III. Results

The thesis reports identified camera risks and a proof-of-concept analysis within the tested setup; it also documents a quick scan of devices using Sofia software. The report's screens, configurations, examples, or measurements constitute the evidence for this summary. A capability described only as a design intention is not counted as a validated operational outcome. No additional performance, adoption, financial, or safety figure has been introduced here. The result is interpreted within the scope of the student's documented setup [1].

IV. Discussion

The findings concern the specific device and tool configuration in the manuscript. The summary does not establish vulnerability prevalence across other devices or safe operation in production networks. Further work could validate findings through authorized testing of additional models, record reproducible test conditions, and assess remediation before broader deployment. These limitations affect how the evidence should be read. The current manuscript can support understanding of the design and reported demonstration, while independent tests would be needed for stronger claims. Any later deployment should document its environment and separate observed outcomes from intended benefits [1].

V. Conclusion

The thesis documents a penetration-testing process for Internet of Things devices. The thesis reports identified camera risks and a proof-of-concept analysis within the tested setup; it also documents a quick scan of devices using Sofia software. The findings concern the specific device and tool configuration in the manuscript. The summary does not establish vulnerability prevalence across other devices or safe operation in production networks. Further work could validate findings through authorized testing of additional models, record reproducible test conditions, and assess remediation before broader deployment. Accordingly, the present contribution is a source-grounded account of the student work and its tested or illustrated scope. Claims about broader effectiveness should be assessed in later work using explicit evaluation conditions [1].

References

[1] Nguyễn Hoàng Hà, "A Penetration-Testing Process for IoT Devices," internal undergraduate thesis (original in Vietnamese), Thai Nguyen University of Information and Communication Technology, 2024.

[2] ICTU Student 129, ”Construction of a Network Security System for the Commercial Bank of Vietnam Hanoi Branch,” internal undergraduate thesis, Thai Nguyen University of Information and Communication Technology, 2009.
[3] ICTU Student 130, ”Construction of a Network Security System for a College of Education in Thai Nguyen,” internal undergraduate thesis, Thai Nguyen University of Information and Communication Technology, 2009.
[4] Nguyễn Tiến Bộ, ”Design of an IoT-Based Home Electrical Device Monitoring and Control System,” internal undergraduate thesis, Thai Nguyen University of Information and Communication Technology, 2021.
[5] Chung-Kuan Chen et al., ”Penetration Testing in the IoT Age,” Computer, 2018. doi:10.1109/mc.2018.2141033.
[6] Rohit Akhilesh et al., ”Automated Penetration Testing Framework for Smart-Home-Based IoT Devices,” Future Internet, 2022. doi:10.3390/fi14100276.
[7] Marlon Intal Tayag et al., ”IoT Security: Penetration Testing of White-label Cloud-based IoT Camera Compromising Personal Data Privacy,” International Journal of Computer Science and Information Technology, 2020. doi:10.5121/ijcsit.2020.12503.
[8] Geetanjali sao et al., ”CRITICAL ANALYSIS OF PENETRATION TESTING PROCESS AND TOOLS,” EPRA International Journal of Research & Development (IJRD), 2021. doi:10.36713/epra8540.
[9] Bako Ali et al., ”Cyber and Physical Security Vulnerability Assessment for IoT-Based Smart Homes,” Sensors, 2018. doi:10.3390/s18030817.
[10] Geeta Yadav et al., ”IoT-PEN: An E2E Penetration Testing Framework for IoT,” Journal of Information Processing, 2020. doi:10.2197/ipsjjip.28.633.