Bachelor Thesis

February 1, 2026

From Security by Obscurity to Imminent Exposure:

Security Risks for IoT Devices in the IPv6 Transition

Jorge Miguel Angel Vite Espinosa

of University of Zurich, Switzerland (23-746-399)

supervised by

Prof. Dr. Ivan De Oliveira Nunes

University of Zurich[UZH]

Bachelor Thesis

From Security by Obscurity to Imminent Exposure:

Security Risks for IoT Devices in the IPv6 Transition

Jorge Miguel Angel Vite Espinosa

University of Zurich[UZH]

Bachelor Thesis

Author: Jorge Miguel Angel Vite Espinosa, jorgemiguelangel.viteespinosa@uzh.ch

URL: https://github.com/Vite04/ThesisCode

Project period: 2026-01-15 - 2026-07-01

Security and Privacy of Information, Networks, and Systems (SPINS)
Department of Informatics (IfI), University of Zurich

Acknowledgements

Abstract

Contents

1 Introduction **1**
- 1.1 The IPv4 to IPv6 Transition . . . 1
- 1.2 Loss of NAT and IoT Exposure . . . 1
- 1.3 Research Objectives & Questions . . . 1
- 1.4 Contributions . . . 1
- 1.5 Thesis Structure . . . 1

2 Background and Related Work **3**
- 2.1 IPv6 Architecture vs. IPv4 . . . 3
- 2.2 The IoT Security Landscape . . . 3
- 2.3 Network Perimeter Security . . . 3

3 Methodology **5**
- 3.1 Research Design . . . 5
- 3.2 Experimental Setup . . . 5
- 3.3 Ethical Considerations . . . 5

4 Configuration and Risk Analysis **7**
- 4.1 Default Router Configurations . . . 7
- 4.2 IPv6 Attack Vectors . . . 7

5 Experimental Demonstration **9**
- 5.1 Scenario: Global Accessibility of an IoT Device . . . 9
- 5.2 Scanning and Enumeration Results . . . 9
- 5.3 Vulnerability Exploitation . . . 9

6 Mitigation Strategies **11**
- 6.1 Recommendations for Network Administrators . . . 11
- 6.2 Recommendations for Manufacturers . . . 11
- 6.3 End-User Best Practices . . . 11

7 Discussion and Limitations **13**
- 7.1 Interpretation of Results . . . 13
- 7.2 Limitations . . . 13
- 7.3 Threats to Validity . . . 13

8 Conclusion and Future Work **15**

A First Appendix **17**

B Second Appendix **19**

1. Introduction

This thesis explores how global IPv6 addressing increases the attack surface of the Internet of Things (IoT) environment. The study combines not only a comprehensive literature review but also an empirical assessment of default system configurations through controlled laboratory demonstrations, highlighting how the adoption of new network standards can potentially affect the security of millions of end devices.

The IPv4 to IPv6 Transition is the result of an inherent limitation in the design of IPv4's address space, which only supports 2^{32} unique addresses. A boundary already exceeded by the estimated 16 billion IoT devices alone in 2024 **iotanalytics2024**. IPv6 mitigates this limitation by implementing a 128-bit architecture, offering a virtually infinite address space. Despite its technical advantage, the global adoption has been gradual due to the current scale of IPv4-based infrastructures and the cost of migration. Therefore, technologies like Network Address Translation (NAT) were adopted to extend the utility of IPv4.

Loss of NAT and IoT Exposure

Research Objectives & Questions

Contributions

Thesis Structure

2. Background and Related Work

IPv6 Architecture vs. IPv4

The IoT Security Landscape

Network Perimeter Security

3. Methodology

Research Design

Experimental Setup

Ethical Considerations

4. Configuration and Risk Analysis

Default Router Configurations

IPv6 Attack Vectors

5. Experimental Demonstration

Scenario: Global Accessibility of an IoT Device

Scanning and Enumeration Results

Vulnerability Exploitation

6. Mitigation Strategies

Recommendations for Network Administrators

Recommendations for Manufacturers

End-User Best Practices

7. Discussion and Limitations

Interpretation of Results

Limitations

Threats to Validity

8. Conclusion and Future Work

A. First Appendix

B. Second Appendix