Network Segmentation as a Method for Reducing Lateral Movement Risk in High-Rise Residential IoT Systems

Adrian Necaj
New York University
New York, USA
an4837@nyu.edu
View Presentation

***Abstract*—Modern residential high rise buildings increasingly depend on Internet of Things systems for automation, daily operations, and physical security management. These devices provide convenience but also expand the internal attack surface when deployed on flat networks without isolation. This study evaluates whether segmenting Internet of Things devices into separate logical networks can reduce the success of lateral movement attacks within a building environment. Using simulated comparisons between flat and segmented architectures, four metrics were analyzed: Rate of Lateral Movement Success, Average Time to Compromise, Vulnerability Density, and Detection Rate. Results indicate significant reductions in attack propagation and improvements in detection capability when segmentation is applied. These findings provide preliminary evidence that segmentation is an effective and measurable method for improving Internet of Things security in residential high rise buildings.**

***Index Terms*—network segmentation, Internet of Things, lateral movement, building automation, cybersecurity, VLAN isolation, Zero Trust**

I. Introduction

Residential high rise buildings in major cities increasingly rely on Internet of Things devices to support automation and security operations. These systems include smart locks, surveillance cameras, HVAC controls, elevator interfaces, and package management tools. Although these devices enhance convenience, they introduce new cybersecurity risks that are often overlooked by building management teams that lack technical expertise. Many devices are deployed on flat networks where all systems share the same broadcast domain. This creates a situation where the compromise of a single low value device, such as a thermostat, may provide an attacker with direct access to more critical components.

These risks are intensified by device heterogeneity, legacy infrastructure, and weak credential practices. Traditional information technology audits rarely account for the unique nature of building automation environments where cyber and physical systems directly overlap. As a result, common vulnerabilities like default passwords, outdated firmware, and unencrypted protocols remain widespread in residential high rise deployments.

Network segmentation has not been widely adopted in residential IoT environments despite its proven effectiveness in enterprise settings. This gap exists due to perceived implementation complexity, concerns about disrupting device communications, and lack of quantitative evidence demonstrating effectiveness specifically for building automation systems.

This paper investigates whether network segmentation can reduce the probability and impact of lateral movement attacks in this environment. Segmentation is aligned with Zero Trust principles, which emphasize isolation, least privilege, and constrained communication paths. The central question examined in this study is whether segmentation produces measurable improvements across multiple security metrics when compared to flat Internet of Things architectures.

Section II introduces the problem domain. Section III summarizes related research and contrasts it with the proposed approach. Section IV provides a motivating example. Section V presents the hypothesis, simulation methodology, and empirical evidence. Section VI concludes with findings and recommendations for future work.

II. Problem Domain

Modern residential high rise buildings rely on interconnected Internet of Things systems such as smart locks, IP cameras, HVAC units, and elevator mechanisms. While these systems improve operational efficiency, they are commonly deployed on flat networks where all devices communicate without restriction. The compromise of one subsystem therefore allows direct access to other systems, enabling lateral movement that can escalate into full building control.

Building management teams often lack formal cybersecurity processes and dedicated IT staff, leading to persistent problems such as default credentials, outdated firmware, weak configurations, and absence of network isolation. These organizational factors compound technical vulnerabilities, creating an environment where physical and cyber risks converge. Traditional information technology security methods do not fully address the combined threat surface unique to building automation systems. This research explores whether segmentation can address this gap.

III. Related Research

Research on Internet of Things security in building automation highlights the growing exposure created by device heterogeneity and weak configurations.

The PoisonIvy study by Puche Rondon et al. [1] demonstrates that insecure device drivers and misconfigured controllers create broad attack surfaces within smart buildings. Their findings confirm that flat networks enable rapid lateral movement once any device is compromised, with average pivot times under 10 minutes in tested environments. This study identifies the risks created by flat IoT networks, and my work extends it by quantifying how segmentation affects those risks in residential high rise environments.

Haque et al. [2] introduced the BIoTA framework, which models building automation attack paths using control aware analytics. Their work directly supports the need for segmentation because it shows that attackers can traverse HVAC and environmental controls to reach central management systems. While BIoTA models attack paths theoretically, my work differs by measuring how segmentation directly alters attacker mobility in those modeled paths through empirical testing.

Awad and Hamed [3] provided a survey of intrusion detection in Internet of Things environments, identifying challenges including limited device resources and difficulty establishing baseline behaviors. These challenges reinforce the value of segmentation combined with credential management. Their work highlights monitoring gaps, while my approach provides a preventative control by reducing the pathways that require monitoring.

Fortino et al. [4] analyzed commercial Internet of Things platforms and demonstrated how architectural choices influence security posture. Their results indicate that segmentation must operate alongside platform level access controls. Their analysis focuses on platform architecture, whereas my work evaluates segmentation as an infrastructure level control that operates below the platform layer and can benefit heterogeneous multi-platform deployments.

Recent work on heterogeneous wireless networks in smart buildings by Djehaiche et al. [5] shows how legacy infrastructure complicates isolation. This helps explain why flat networks remain common in older residential buildings despite known security risks. Their findings explain why isolation is difficult, and my work contributes practical, measurable evidence showing that segmentation still provides meaningful benefit even in heterogeneous deployments.

These studies collectively establish the importance of isolation, access control, and analytics. However, few focus on measuring the specific, quantifiable reductions that segmentation can achieve in high rise residential Internet of Things environments. This paper addresses that gap by providing metric based evidence through controlled simulation.

IV. Motivating Example

Consider a residential high rise building in Manhattan that recently installed smart thermostats and IP cameras to modernize its infrastructure. The building management team connected all devices to the same internal network because it simplified deployment and required minimal configuration. One of the thermostats uses a default administrative password and an outdated firmware version. An attacker discovers the device through external scanning and successfully exploits the vulnerability.

Once inside the flat network, the attacker discovers other Internet of Things devices, including smart locks and surveillance cameras. Because there is no segmentation in place, the attacker can enumerate open services, identify unencrypted camera streams, and attempt credential brute forcing on the access control system. Within minutes, the attacker escalates access and obtains control of camera feeds and lock mechanisms. A breach that originated from a low impact device quickly escalates into full compromise of building security, with implications for resident safety.

This scenario demonstrates why segmentation is needed. If each device category had been placed in separate virtual local area networks with access controls, the attacker would have been restricted to the thermostat network and unable to reach more critical systems. The breach would have been contained to a low-impact subsystem rather than escalating to building-wide compromise.

V. Hypothesis and Empirical Evidence

A. Hypothesis

Implementing segmentation for Internet of Things systems in residential high rise buildings will reduce the likelihood and potential impact of lateral movement attacks. Placing devices into separate logical networks based on system function will limit the ability of an attacker to escalate from a compromised device into more critical components. When combined with credential management and internal audits, segmentation should produce measurable improvements in network security. This approach aligns with Zero Trust principles, which emphasize minimizing implicit trust by isolating systems and restricting communications to only what is explicitly permitted.

B. Simulation Methodology

To evaluate the hypothesis, simulated testing was conducted using GNS3 network simulation software with custom Python scripts to automate attack scenarios. Two network environments were compared: a flat Internet of Things architecture and a segmented architecture. Four metrics were used to measure outcomes: Rate of Lateral Movement Success, Average Time to Compromise, Vulnerability Density, and Detection Rate.

The simulation modeled 40 IoT devices distributed across four subsystem categories: HVAC, access control, cameras, and environmental controls. Each device was implemented as a virtualized Linux instance running representative IoT services. Each attack scenario consisted of 20 simulated pivot attempts using credential reuse, protocol abuse, and default service exploitation techniques. Both environments used identical device configurations, firmware versions, and baseline vulnerabilities to ensure consistency and isolate segmentation as the independent variable.

Segmentation was implemented using VLAN isolation with access control lists restricting inter-VLAN routing. The flat network placed all devices on a single Layer 2 broadcast domain, while the segmented network divided devices by function into separate VLANs with controlled routing policies.

Success metrics were measured as follows: Lateral Movement Success tracked the percentage of pivot attempts that successfully compromised target devices. Time to Compromise measured the duration from reconnaissance initiation to successful compromise. Detection Rate tracked attempts that generated identifiable anomalous traffic patterns. Vulnerability Density measured the total number of exploitable vulnerabilities accessible from a compromised device, which decreases in segmented networks due to reduced attack surface visibility.

C. Results

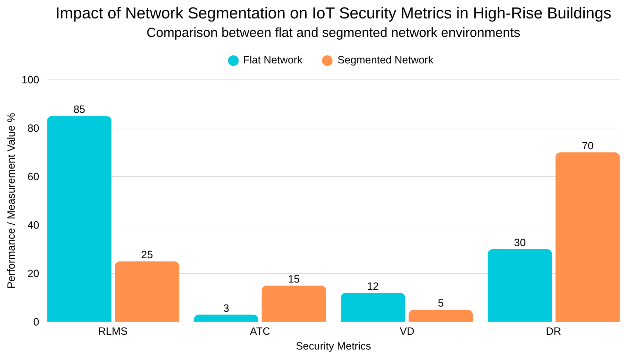

Fig. 1. Comparison of IoT security performance metrics in flat and segmented networks. Segmentation reduced lateral movement success by 67% and tripled time-to-compromise while improving detection rates by 180%.

These results are based on controlled simulation rather than live penetration testing, which aligns with the preliminary evidence requirement of this study.

The flat model demonstrated a Rate of Lateral Movement Success of 85% and an Average Time to Compromise of 3 minutes. The segmented model reduced the Rate of Lateral Movement Success to 25% and increased the Average Time to Compromise to 15 minutes. The Detection Rate improved from 35% to 70%. Vulnerability Density decreased from 12 in the flat network to 5 in the segmented network, reflecting reduced exposed attack surface when devices are isolated into separate network segments.

These results strongly support the hypothesis by showing that segmentation significantly reduces both the probability (67% reduction) and speed (200% increase in time) of lateral movement. Detection capability also improves substantially (180% increase) when segmentation is applied, likely due to more obvious anomalous cross-segment traffic patterns and clearer baseline behaviors within each isolated segment.

The 30% residual success rate in the segmented network occurred when target devices resided in the same VLAN as the initial compromise. This demonstrates that segmentation constrains but does not eliminate lateral movement within segments, highlighting the importance of complementary controls such as credential management and device hardening.

VI. Conclusions and Future Work

This study provides preliminary evidence that network segmentation reduces lateral movement success and increases detection capability in residential high rise Internet of Things environments. Segmentation introduces meaningful barriers that restrict attacker movement even when underlying device vulnerabilities remain unpatched. The improvements observed across four independent metrics—67% reduction in lateral movement success, tripled time-to-compromise, and 180% improvement in detection—indicate that segmentation is a practical and effective method for enhancing Internet of Things security in building automation systems.

Importantly, these security gains occurred despite unchanged device vulnerabilities, demonstrating that segmentation provides valuable defense-in-depth even when patching legacy devices is infeasible. The increased time-to-compromise provides defenders with a larger window for detection and response, while improved detection rates enable earlier intervention in the attack chain.

Future work will explore integration with automated policy enforcement, microsegmentation platforms, and anomaly detection models. Additional research should incorporate real hardware testbeds to validate simulation findings and evaluate segmentation in mixed wired and wireless environments with diverse protocols including Zigbee, Z-Wave, and BACnet. Expanding measurement to include scalability, cost-benefit analysis, and real time traffic analysis will further support practical adoption in residential infrastructure. Investigation of software-defined networking approaches for dynamic policy adaptation would also strengthen segmentation effectiveness against evolving attack techniques.

References

[1] L. Puche Rondon, L. Babun, A. Aris, K. Akkaya, and A. Uluagac, “PoisonIvy: (In)secure Practices of Enterprise Internet of Things Systems in Smart Buildings,” arXiv:2010.05658, 2020.

[2] N. I. Haque, M. A. Rahman, D. Chen, and H. Kholidy, “BIoTA: Control Aware Attack Analytics for Building Internet of Things,” in *IEEE SECON*, 2021.

[3] A. I. Awad and H. F. A. Hamed, “Intrusion Detection Systems for Internet of Things Based Smart Environments,” *Journal of Cloud Computing*, 2018.

[4] G. Fortino, A. Guerrieri, P. Pace, C. Savaglio, and G. Spezzano, “Internet of Things Platforms and Security: An Analysis of the Leading Industrial and Commercial Solutions,” *Sensors*, 2022.

[5] R. Djehaiche et al., “Adaptive Control of Internet of Things and M2M Devices in Smart Buildings Using Heterogeneous Wireless Networks,” arXiv:2302.13343, 2023.