National College of Ireland

Optimizing Zero Trust Architecture for Corporate IoT Security: Addressing Vulnerabilities and Device Limitations

MSc Research Project
Masters in Cybersecurity

Shouvik Roychowdhury
Student ID: X23179015

School of Computing
National College of Ireland

Supervisor: Raza ul Mustafa

National College of Ireland

MSc Project Submission Sheet

School of Computing

Student Name:	Shouvik Roychowdhury
Student ID:	X23179015
Programme:	Masters in cybersecurity **Year:** 2024
Module:	Practicum part 2
Lecturer:	Supervisor
Submission Due Date:	12-12-2024
Project Title:	Research Report
Word Count:	6678 **Page Count: 22**

I hereby certify that the information contained in this (my submission) is information pertaining to research I conducted for this project. All information other than my own contribution will be fully referenced and listed in the relevant bibliography section at the rear of the project.
ALL internet material must be referenced in the bibliography section. Students are required to use the Referencing Standard specified in the report template. To use other author's written or electronic work is illegal (plagiarism) and may result in disciplinary action.

Signature:

Date: 12-12-2025

PLEASE READ THE FOLLOWING INSTRUCTIONS AND CHECKLIST

Attach a completed copy of this sheet to each project (including multiple copies)	☐
Attach a Moodle submission receipt of the online project submission, to each project (including multiple copies).	☐
You must ensure that you retain a HARD COPY of the project, both for your own reference and in case a project is lost or mislaid. It is not sufficient to keep a copy on computer.	☐

Assignments that are submitted to the Programme Coordinator Office must be placed into the assignment box located outside the office.

Office Use Only	
Signature:	

Date:	
Penalty Applied (if applicable):	

Optimizing Zero Trust Architecture or Corporate IoT Security: Addressing Vulnerabilities and Device Limitations

Shouvik Roychowdhury
X23179015

Abstract

The increasing adoption of IoT devices in corporate environments has expanded the attack surface for potential cyber threats, highlighting the limitations of traditional security approaches. The paper focuses on optimized Zero Trust Architecture tailored for IoT devices, it does so use the recommendations by Microsoft Threat modeling tool and simulating the network using Cisco Packet Tracer, thus leveraging both STRIDE model and ZTA principles. It was seen that common attacks on IoT devices such as VLAN hopping, ARP poisoning, and MAC flooding that often are being perpetrated because of vulnerabilities in end point devices or open ports are mitigated if Zero Trust principles are followed. The results demonstrate the efficiency of key principles of ZTA such as trust verification, network segmentation and the least privilege principle in mitigating lateral movement and unauthorized access.

Key Words: Corporate IoT security, Zero Trust Architecture, STRIDE Model

1 Introduction

This research paper aims to propose a comprehensive security framework based on the zero-trust architecture that addresses critical vulnerabilities that are present in vulnerabilities such as BLESA (Bluetooth Low Energy Spoofing Attack), Ripple20, KRACK (Key Reinstallation Attack), and Amnesia:33 (Fehér and Sándor). The primary issues in implementing a security framework are the overall low memory capacity and computation power present in these devices, as IOT devices need to be small in size for ease of use and to conserve battery life. In our daily lives there has been a rise of IOT devices in various sectors, including healthcare, industrial automation, and smart homes which has led to a bigger surface area of attack making it necessary to envelope the entire network perimeter in a smarter security framework than the traditional security measures.

Attacks such as the BLESA attack leverage the Bluetooth connection present in most IOT devices, the vulnerability exists in the reconnection functionality of Bluetooth which would cause attackers to bypass authentication and inject malware (Gupta and Varshney, Year) . Another prolific IOT vulnerability is the Krack vulnerability which targets the handshake protocol of the WIFI (WPA2). Despite the fact that most devices nowadays support WPA3, slower upgrade cycles and backwards compatibility are needed in a diverse range of devices. Other significant vulnerabilities can affect devices in crucial sectors of society such as healthcare, energy and transportation.

The real-world consequences of insecure IoT systems underscore the urgency for a robust security framework. For instance, vulnerabilities in Ecovacs robot vacuum allowed attackers to take control and harass users through compromised Bluetooth security (ABC News, 2024). Similarly, Kia vehicles were found susceptible to remote tracking and unauthorized access through their electronic doors due to web-based vulnerabilities which lead to remote code execution. (Wired, 2024)

The transition to ZTA marks a shift from traditional perimeter-based security to a model of continuous verification and behaviour-based network access privileges. This shift has now been even more prominent because of the rise of remote work and widespread behaviour-based on adoption of cloud-based platforms, which expose the limitations of trusting devices solely based on network access and while defence-in-depth strategies have attempted to enhance security by layering defences, they are often not feasible for resource-constrained IoT devices. This paper will look at Zero Trust Architecture as a solution for an efficient scalable alternative to IoT security.

Research question: How can a zero-trust framework be optimized to secure corporate IoT ecosystems while balancing device limitations and security requirements?

Objectives:

- Design and evaluate core Zero Trust components that have been optimized for home IoT devices, focusing on resource constraints such as low power and memory.
- Develop an adaptive security framework that dynamically adjusts security levels based on operational requirements and overall behavior of the device.
- Implement and analyze different security protocols and measure their effectiveness against common vulnerabilities.

2 Related Work

The U.S Department of Defense has implemented a Zero Trust Architecture to strengthen the cybersecurity framework, which is built around core pillars of User, Device, Network/Environment, Application, Data, Visibility & Analytics, and Automation & Orchestration. Each pillar includes capabilities such as multi-factor authentication, behavior-based device monitoring and micro-segmentation to restrict lateral movement within the network. In the context of IoT, ZTA uses behavior based conditional access to provide system privileges as it is more efficient for the usual resource constrained IoT devices. (U.S. Department of Defense, 2022).

Kehe Wu et al. (2023) explore the Zero Trust Model for IoT devices specifically, it proposes a two-component model focused on device trust evaluation and network access control. The trust evaluation of IoT devices enables real time data acquisition and proper communication with the central network. In trust evaluation, the devices are continuously monitored and upon analyzing behavior and characteristics a unique hash value is generated which is periodically verified by an authority determining any anomalies. On the other hand, the network access control component dynamically adjusts permission based on data and behavior, when abnormal behavior is detected, the organization can shut down the network

access. A stochastic Petri net model is used for analyzing system behavior as the model helps to map out all possible states of the terminal, thus identifying potential threats that deviate from normal behavior.

The paper by Pietro and Elena implements Zero Trust by using access controls through policy-based mechanisms such as Role-Based Access Control (RBAC), Attribute-Based Access Control (ABAC), and Access Control Lists (ACLs). This ensures that only authorized and verified users gain access to network and system resources. The strength in ZTA lies in its ability to adapt permission based on real time behavior data making it particularly effective against lateral movement and insider threats. However, a weakness of ZTA is that implementing it fully requires some infrastructural changes such as network segmentation which may pose a scalability challenge on older systems also particularly on the access controls, the ZTA access controls can be quite resource intensive as continuous verification process requires significant processing power (Patil et al., Year).

Samaniego and deters, developed a blockchain-based middleware called Amatista, that leverages Zero Trust principles to improve IoT network security. The ZTA model here integrates blockchain to manage trust by replacing centralized authorized with distributed validation authorities or "miners" in this case. The first-level miners handle immediate context-based validation of devices and second-level miners validate transaction blocks across the network. This approach of a distributed structure ensures data authenticity and limits lateral movement of unauthorized actions. However, this approach has its drawbacks as a distributed ledger is difficult to implement and is often unnecessary, and protocols of blockchain such as PBFT have a lot of resource demands and may not be sustainable for devices with limited computational power (Samaniego and Deters, 2018).

2.1 Conclusion of Related works

From the papers it can be seen that even though zero trust offers substantial improvements in security, there needs to be an optimized implementation of these security policies due to resource constraints and diverse nature of IoT devices. Current implementations such those of U.S. Department of Defense and that of Kehe Wu et al., show the strength of Zero Trust Architecture in securing IoT environments by applying methods like behavior-based monitoring, adaptive access control and dynamic trust evaluation. Although these implementations were successful, the implementation of ZTA often requires infrastructural changes like network segmentations which can be expensive and difficult to implement on older systems. There are also the concerns of less powerful devices not being able to implement resource-intensive security measures.

To address these limitations, this paper proposes an optimized Zero Trust framework tailored for corporate IoT environments, to achieve these lightweight adaptive security measures will have to be enforced. For example, instead of continuous device verification, the framework will implement periodic trust updates and event-triggered monitoring events. Additionally, the framework will have to be scalable and have simplified access control policies such as Attribute-Based Access Control that can limit lateral movement and unauthorized access without the need of heavy computational power.

3 Research Methodology

The methodology will focus on defining specific network traffic patterns and segmentation policies in a home IoT ecosystem. The methodology emphasizes creating a detailed model of a smart home network such as smart thermostats, security cameras, smart TV's and centralized lighting. All their behaviors will also have to be simulated, for example a smart camera generates high-bandwidth video data while something like a smart thermostat operates with low-data demands.

Integration of Zero Trust Architecture

To strengthen security of the simulated architecture, Zero Trust Architecture principles are integrated into the network, taking reference from previous studies and integrating it with IoT environment in Cisco Packet Tracer can be implemented by:

- **Device Identity Verification:** Each IoT device is assigned a unique identity tag to track it clearly across logs or real-time simulation, and unauthorized access can easily be flagged.

- **Micro-Segmentation:** The network is divided into isolated segments with its own devices and access permissions for example cameras can be separated from smart tv's and thermostats, thus preventing lateral movement in the case of attack.

- **Continuous Monitoring and Logging:** A logging system to track movements with a network and flag any unusual traffic or unauthorized access.

- **Principle of least privilege:** Principle of least privilege dictates that users be given the bare minimum privileges to perform their necessary jobs. By restricting access rights to the bare essentials, PoLP minimizes the risk of accidental or intentional misuse of privileges, thereby enhancing overall security.

Additionally, the simulation examines network behavior under different traffic loads and interference scenarios, providing insights into IoT functionality and resilience within a segmented, Zero Trust-protected environment.

4 Design Specification

The approach of this paper is to simulate corporate IoT architecture through cisco packet tracer and highlight threats using Microsoft Threat Modeling Tool. The feedback given from the threat model will then be used to set up network rules in cisco packet tracer that are in line with zero trust architecture and can be used to secure the IoT network.

Network infrastructure

The network will consist of a diverse range of home IoT devices and a central office gateway:

- **IoT devices:** A wide range of IoT devices in an office environment will have to be configured and simulated to give as accurate simulation of behavior and resource constraints as possible.

- **Office Gateway:** The gateway will have role-based policies to limit sensitive resource access to specific devices and block unknown devices, apart from that the gateway routes traffic and enforces access control lists.

- **IoT behavior model:** Cisco packet tracer can emulate IoT traffic behavior which includes updates from sensors and different endpoint devices, it can also simulate IoT behavior when controlled remotely such as one with a smartphone or a laptop.

- **Security Design:** Security features that are effective and can be simulated in cisco packet tracer include firewalls for controlling traffic flow and preventing unauthorized access, Access control list to authorize who gets access to which data and finally the network segmentation would isolate a traffic and reduce attack surfaces and get prevent lateral movements during attacks. Additionally, role-based access control and secure IoT device configurations help mitigate against vulnerabilities unique to IoT environments. There are some basic encryption protocols that can be setup in network devices such as WPA2, but these cannot be implemented to IoT devices due to the nature of their low computational power.

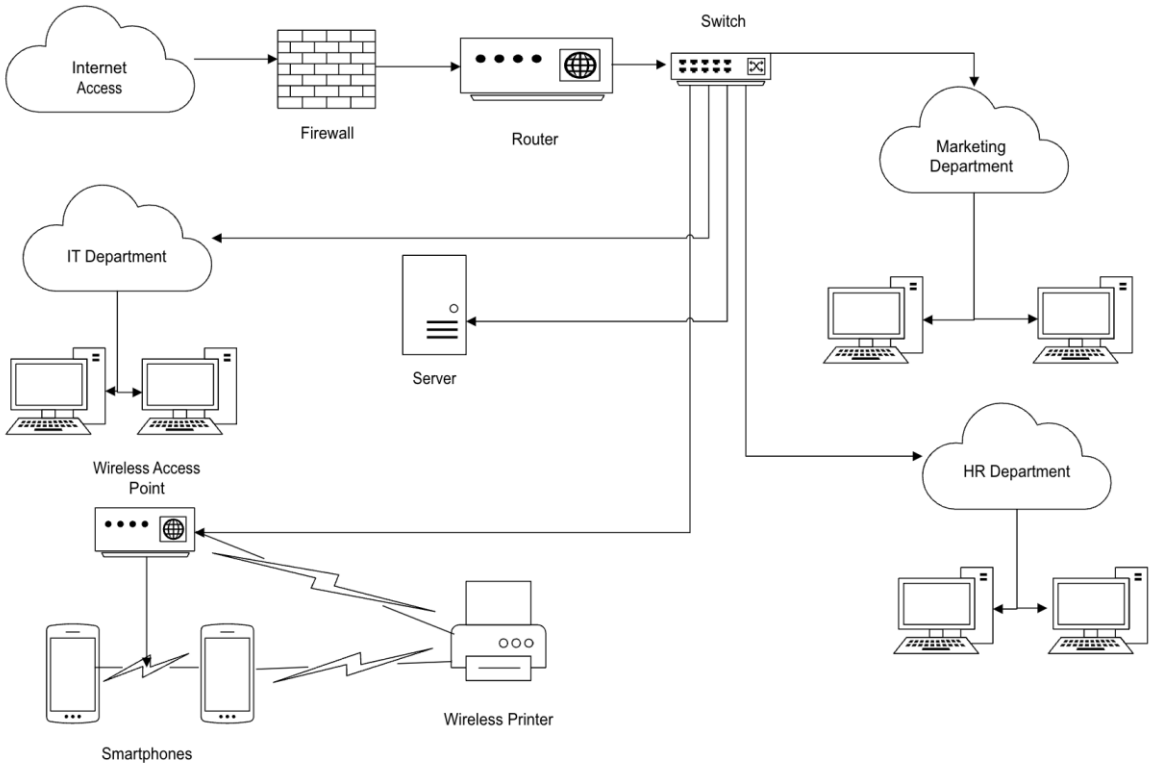

Figure 1. Network Architecture of the corporate network

Microsoft Threat Modeling Tool

The Microsoft threat model tool works on STRIDE methodology which provides systematic feedback on the following potential threats: (Khan et al.)

- Spoofing: Spoofing is an attack where an outside entity impersonates another identity.
- Tampering: Tampering is when an unauthorized modification is done to data or code.
- Repudiation: Repudiation is when users can deny actions or transactions without any record of it.
- Information Disclosure: An outside entity gaining access to sensitive information.
- Denial of Service: Any action taken to degrade or prevent access to resources by an attacker is a denial-of-service attack.
- Elevation of Privilege: Unauthorized escalation of rights such as getting administrator permission with a regular account.

Microsoft threat modeling tool allows users to record each threat and give recommendations for mitigations techniques. Some of the recommendations include encryption techniques, network segmentation and application of access control lists. The tool also generates reports that summarizes all threats, impacts and recommendations for mitigations for the simulated IoT network.

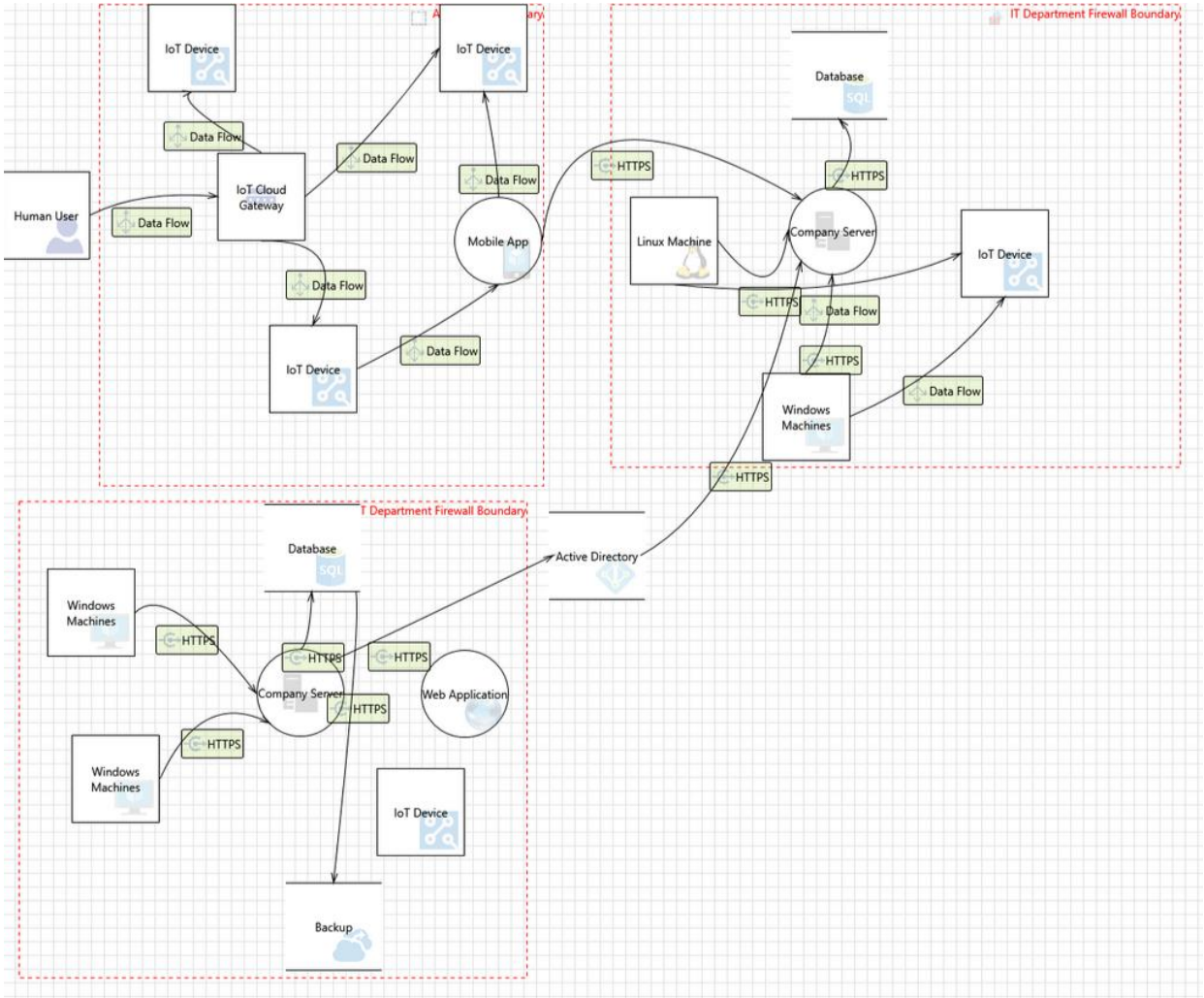

Figure 2. Threat Model based on STRIDE Framework

Reporting: After the modeling of structure, the tool can be used to generate detailed insights based on the model created, along with highlighting insecure data flows and identifying trust boundaries. Once the automated report is generated based on the STRIDE framework, each threat is generated giving a description of the threat, affected components, severity and mitigation recommendations.

User reports can include visual representations of the areas where threats are found, these visual aids help non-technical people understand how threats can arise and why mitigation is necessary, the reporting structure also follows all industry standards like *GDPR, ISO 2007 a*nd more. After which the report can be exported as Excel, PDF or HTML report.

5 Implementation

5.1 Threat Model

To implement Zero Trust Architecture, a threat model is needed to be defined first, for that key component like IoT devices (sensors, automated doors, security cameras), cloud gateways, internal servers, database servers and endpoints like computers and smartphones will have to be defined and their behavior simulated.

The threat model for the simulated office network, gave the following results:

- Simulate data flows and Trust Boundary: To represent the data flows, each element in the network has connection paths setup with other elements and certain trust boundaries are set up to signify network segmentation and places where data enters and exits securely. Trust boundaries can help identify points where additional security controls are necessary.

- Threat Generation: MTMT uses STRIDE framework to automatically generate potential threats and rank them based on severity for the and stage of design cycle and how concerning the vulnerability is.

- Strengthening Device Identity and Authentication: To enhance device identity and authentication within the ZTA, each IoT device is assigned a unique identifier to enable precise tracking and monitoring. Additionally, periodic validation of device trustworthiness is conducted using behavior analysis and anomaly detection where devices behaving abnormally can be identified and removed from the network.

Based on the results of the threat model tool, the paper will propose a solution in two-fold. The first being security features that change configurations and implement a solution based on data of common security attacks on switches, routers, hubs and end point devices. The second being that of a Zero trust model which proposes overall security of the network architecture

5.2 Securing IoT network by referencing common vulnerabilities

For this framework the initial security features are implemented which starts with fixing misconfigured ports and implementing various attack vector mitigations such as VLAN hopping, ARP poisoning, mac spoofing and DHCP starvation.

1. **VLAN hopping** attacks exploit vulnerabilities in VLAN configurations such as incorrectly configured switches or when factory settings are not changed by companies before using them. Small businesses especially will not have IT teams to change the configurations properly. In case of these misconfigurations, an attacker can gain unauthorized access to other VLANs, and bypass logical network segmentation.

   VLAN hopping attacks have been observed in internal penetration testing and real-world breaches where network misconfigurations exist, although the prevalence is limited compared to more direct attack vectors. Such attacks highlight the critical need for proper VLAN management and configuration.
   To defend against VLAN hopping attacks the following mitigation steps are necessary:

   - Transferring the ports from default to a separate office VLAN: By default, all ports are assigned to VLAN 1, therefore if the default settings are left unchanged, any attacker can exploit the common vulnerabilities and perform a VLAN hopping attack. The problem is resolved by creating a native VLAN and transferring the working ports to it.

   - Disable Trunking on Access Ports: VLAN hopping attacks often exploit dynamically negotiated trunk modes. By forcing an access port to act as a trunk to mitigate this we can simply disable access mode and DTP preventing them from becoming trunks.

   - Shutdown Unused ports and assign them to a Blackhole VLAN: Unused ports left unchecked can be an easy entry point for attackers, to stop this all unused ports are assigned to a Blackhole VLAN and disabled. So that even if the ports are left enabled the VLAN is still a blackhole VLAN and not a currency used one.

2. **Mac Flooding Attacks:** Mac Spoofing involves an attacker changing their mac address of a device to copy that of a trusted device on the network, this would allow them to bypass network access controls such as mac filters on ports or firewalls. Mac Spoofing allows attackers to intercept traffic and hijack sessions, they can also evade detection and conduct denial of service attacks. Mac flooding then involves overwhelming the switch with a flood of fake MAC addresses, forcing it to broadcast all traffic like a hub, exposing sensitive data.

Mitigating Mac Flooding using Zero Trust Principles: In Zero Trust network permits that no device is trusted and deemed not to be checked by the system. It's imperative that every device is granted privileges only after successful verification and authorization of the user or device. Additionally, device behavior should be monitored to restrict access in accordance with the user's role. In zero trust a device would undergo authentication and authorization when accessing a resource, implementing this measure would limit any lateral movement of threat actors within the network and stop them from stealing any sensitive information.

3. **DHCP Starvation Attacks:** A DHCP starvation attack targets the DHCP server which dynamically assigns IP addresses to devices on a network. In this attack the attacker sends a flurry of DHCP requests using spoofed MAC addresses. Each request appears as a legitimate client, quickly exhausting the DHCP server's pool of IP addresses. As a result, actual legitimate users cannot obtain IP addresses, and thus effectively being denied access to the network. Moreover, DHCP starvation is often a precursor to DHCP server impersonation attacks, where attackers set up rogue DHCP servers to issue malicious network configurations, enabling man-in-the-middle (MITM) or DNS spoofing attacks.

   Mitigation Strategies simulated in Cisco Packet Tracer: In all DHCP servers the number of allowed MAC addresses per port can be configured and if the limit is reached, additional DHCP requests can be blocked or flagged. The other very effective method that is simulated in the aforementioned Cisco packet tracer network architecture is rate limiting or restricting the number of DHCP requests allowed per second per client, which would prevent a sudden flood of DHCP requests.

4. **ARP Poisoning Attacks:** Also known as ARP spoofing, it is a man-in-the-middle attack where an attacker sends forged ARP messages to associate their MAC address with an IP address of a real device on the network. This can theoretically allow them to perform man in the middle attacks such as the ability to intercept, manipulate or even drop traffic intended for an actual user of the system.

   Mitigation strategies that can be implemented and simulated in Cisco packet tracer include Dynamic ARP inspection which validates ARP packets based on IP-MAC mappings stored in the DHCP database. When this is enabled on a switch, DAI intercepts ARP packets and checks their authenticity before allowing them through. However, the most effective way to prevent ARP poisoning is access control lists , these ACLs block traffic from unauthorized sources or to restrict ARP traffic to trusted devices.

5. **Spanning Tree Protocol Attack:** Spanning Tree Protocol (STP) is used in Layer 2 networks to prevent loops by selecting a single root bridge to manage forwarding paths. An attacker can exploit STP by sending forged Bridge Protocol Data Units, which forces legitimate devices to recognize the attacker's device as the root bridge leading to traffic interception.

The mitigation strategies include a collection of filters and guards to filter out unknown endpoint devices. The guards include:

- Bridge Protocol Data Unit (BPDU) guard, which protects edge ports by disabling them if BPDU is received.
- Similarly, the root guard ensures that only authorized devices can become the root bridge by placing a port in a root-inconsistent state if it receives superior BPDUs.
- The BPDU filters also block BPDUs on specific ports to ensure STP does not run on those interfaces, reducing the attack surface.

5.3 Securing top threats of the threat model with Zero Trust Architecture

The threats can be summarized into 4 major categories:

Threat Name	Severity	Details	Proposed Mitigation
Unauthenticated Access	High	Lack of access controls on sensitive data	Implement strict access controls and conditional access policies
Data Breaches	Critical	There is a possibility of data leaks due to weak encryption protocols	Enforcing data encryption at rest and in transit.
Misconfigured Services	High	Certain cloud services when misconfigured with respect to security, may expose endpoints that are not intended to be exposed. Same goes for switch ports	Regular security audits and internal pentesting can mitigate this by closing unused ports and stopping unneeded or vulnerable services.
Insider Threats	Medium	Employees or contractors with authorized access misusing their privileges, either intentionally or inadvertently, leads to data theft or misuse of services.	Implementing robust logging and monitoring of all critical actions and periodic review of access of crucial resources.

Figure 3. Summary table of threats

Each of the components of the model can be broken down into different threats categories as per the STRIDE model, this paper will discuss and implement the solutions wherever possible by simulating it in the model of cisco packet tracer:

1. **Elevation of Privilege:** Lack of proper identity and Access management usually lead to some uses gaining more privileges than necessary and exposing sensitive resources. Identity and access management systems are crucial in that regard of enforcing access policies across a platform.

   In the threat model of corporate IoT devices, the elevation of privilege is found in IoT devices such as a smart door lock, where the device could be unlocked through remote code execution in the server connected to the door, conversely an attacker might exploit weak or default credentials, or vulnerabilities in authentication mechanism to gain access to the admin panel of the IoT device. Some instances of this are smaller non-tech-based companies setting up weak WIFI router passwords or leaving the default setting of switches.

   - **Potential Impacts:** If the privilege of the system is escalated successfully to an admin account, the attacker would gain unauthorized access to admin features which would enable them to alter critical configurations such as changing access policies or disabling security. Privileged access would also allow attackers to gain access to control IoT devices operating anything from doors to servers of the company.

   - **Mitigations Proposed:** The field IoT field gateway should be set up to authorize the user to check if the user asking for the resource has the relevant permissions to perform the action requested. For physical locks such as a smart door, there needs to be a remote command that makes it so that no key can unlock the door, the command can be set up by the cloud gateway. Other solutions include a Role-Based Access Control, that ensures only authorized users can access privileged features, and IP whitelisting that restricts access to admin interfaces and services.

2. **Tampering:** In a corporate network with IoT devices, this threat arises when malicious actors gain access to the device or communication channels and can alter sensitive configurations or data at transit if it is unencrypted.

   - **Potential Impacts:** Prominent components that can be hacked are security cameras which are connected to a server, once intercepted the footage can be injected or altered making physical security unreliable. Tampering may also occur due to poor device security in non-tech-based companies, such as failing to update IoT device firmware. For instance, a smart water meter with outdated software could be modified to send incorrect usage data to the central server, leading to billing errors or resource mismanagement.

   - **Mitigations Proposed:** Encrypting data at rest and transit by enabling protocols of AES-256 and TLS 1.2 or above will mitigate issues where data

even if intercepted cannot be read or manipulated. Along with that integrity verification systems can also be implemented which verify integrity during transit and storage.
To protect endpoint devices against tampering, software like BitLocker and Secure Boot can be used on Windows devices running Windows 10 and above. For IoT devices specifically, Windows 10 IoT core has a lightweight version of BitLocker which has UEFI bootloader.

3. **Information Disclosure:** Sensitive information like user credentials, API keys and other personally identifiable information might be exposed due to insecure configurations and over-privileged roles.

    - **Potential Impacts:** When data breaches occur, sensitive information like user credentials, and personal data is leaked. Which goes against a lot of compliance regulations such as GDPR and HIPAA. This would have severe legal repercussions and fines imposed which would also lead to loss of reputation.

    - **Mitigations Proposed:** Use API gateways and enforce strong authentication mechanisms like OAuth 2.0. Plus encrypting sensitive data at all times would protect data at rest and transit.

4. **Spoofing:** Spoofing occurs when attackers impersonate legitimate users, services or devices. One of the more popular versions of this by attackers is MAC spoofing where attackers can manipulate their MAC addresses and impersonate a device on the network, this can then be used to gain access to the network.

    - **Potential Impacts:** Attackers could impersonate authorized users or even users with admin access and gain access to the admin panel of IoT devices. Using IP spoofing or MAC address spoofing, an attacker could bypass network-level controls or impersonate a trusted device to infiltrate the corporate network.

    - **Mitigations Proposed:** As detailed in the previous section, the common spoofing attacks like MAC spoofing and ARP spoofing can be mitigated by using dynamic ARP inspection and MAC limiting. Spoofing has also been highlighted in the active directory component of the network, thus connecting the AD to services like OAuth 2.0 and OpenID connect. It supports various scenarios, including user sign-in for web or single-page applications, apps accessing web APIs, and background services or server applications interacting with APIs. This makes it easier for developers to integrate authentication and resource access across diverse application types.

5. **Denial of Service:** Leveraging the low power IoT devices, attacks can be carried out by targeting exposed endpoints in the network.

    - **Potential Impacts:** Attack on compromised systems like smart HVAC could cause overheating or freezing in critical rooms like the server room, causing disruptions to the company. A DoS on IoT gateways or routers can lead to network wide shutdowns, such as security cameras connected to the network not working or smart doors being locked.

    - **Mitigations Proposed:** Services like Azure DDoS Protection or AWS Shield will detect and mitigate sudden volumetric attacks automatically. These services analyze traffic and block malicious traffic before it reaches the main servers.
      Configuring Access Control Lists on routers and switches would block and restrict malicious IPs or restrict traffic to servers and firewalls can monitor and block abnormal traffic.
      The most effective solution however is rate-limiting policies on APIs and IoT devices to restrict the number of requests allowed from any single client.

6. **Repudiation:** In corporate IoT networks, repudiation occurs when a user or device denies performing an action or transaction, making it difficult to trace or verify their activities. Attackers or insiders could exploit this to hide unauthorized access, changes, or malicious activities within the ecosystem.

    - **Potential Impacts:** This attack used by the combination of other attacks like data privilege escalation would mean attackers would be able to install a backdoor access very easily and remove all traces of their presence.

    - **Mitigations Proposed:** The two types of mitigations would be active and passive mitigations; active mitigations include deployment of Siem tools to monitor traffic in the network. Passive mitigations on the other hand are application of strong logging system which tracks all logs in a location separate from other devices in the network so that attackers would not have access to it during a cyberattack.

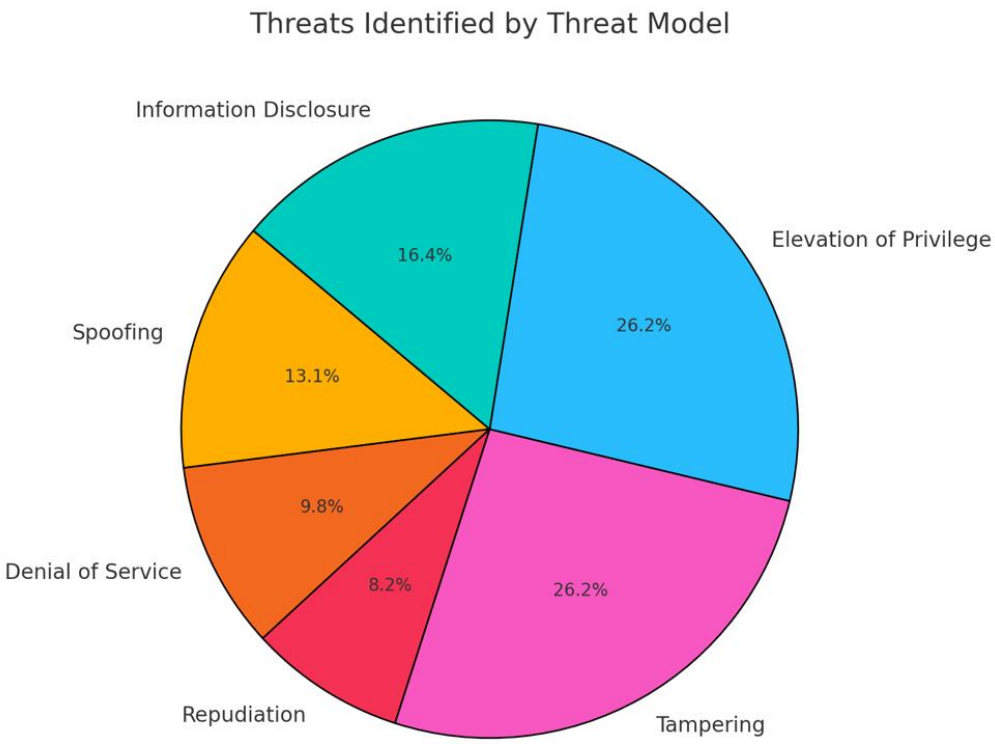

Figure 4. Threats identified by percentage

6 Evaluation

Cisco Packet Tracer is a tool that can simulate network protocols and zero trust architecture with industry standard devices. For this paper security measures were simulated based on the threats shown by the threat model. The security measures implemented are:

1. **Network Segmentation:** Network segmentation into separate smaller networks, isolating them into zones to control flow of traffic would mitigate lateral movement attacks by isolating systems of critical infrastructure. The objective in the simulation was to separate IoT devices, admin systems such as company servers and other network components.

2. **Identity-Based Access Control:** Using AAA (Authentication, Authorization, and Accounting) to authenticate users accessing network devices. The purpose of this is to authenticate users before they access a router or switch by using a secret password to authenticate and enforce identity verification for access to networking devices.

3. **Least Privilege Access:** One of the core principles of zero trust is to not provide any unnecessary privileges and to users when not needed. Instead of granting the minimum level of permissions needed for the job, in the case of the simulation, this paper will have 2 separate login permission levels. That being a user which has only read permission and the other being admin having full access. To monitor who has

accessed and through what permission. A logging trap can be setup, that implements tracking activities on devices.

4. **Continuous Verification:** With access control lists, Cisco packet tracer can simulate whitelisting and blacklisting on Ip addresses, protocols and ports. This ensures that only authorized traffic is let through. Role based access controls are also implemented in the firewalls for further filtering within the network.

5. **Rate Limiting:** To prevent DoS attack from occurring, rate limiting is set up which restricts excessive traffic from one single source. The configuration is setup in the router which is connected to all IoT devices. The rate in this model has been limited to 20 requests per second from 2000.

6. **Port Security:** Port Security is a critical Layer 2 feature used to safeguard switch ports by restricting the number of devices that can connect to them and specifying which devices are allowed based on MAC addresses. It prevents attacks such as MAC flooding and spoofing attacks. While access ports typically enforce port security, trunk ports (which carry traffic for multiple VLANs) can also be secured by limiting the devices allowed to send or receive VLAN traffic, reducing the risk of VLAN hopping attacks. It will also prevent any Man in the Middle or eavesdropping attacks.

7. **Snooping on devices:** By using Dynamic ARP inspection, ARP Snooping cross-references ARP packets with trusted IP-to-MAC mappings stored in DHCP Snooping database.
   DHCP Snooping is a security feature that monitors and filters DHCP traffic on switches to protect against attacks such as DHCP starvation attacks. A rogue DHCP server can then issue malicious configurations, enabling man-in-the-middle (MITM) attacks or directing traffic to attacker-controlled systems.

6.1 Comparison with Existing Solutions

Traditional Perimeter-Based Security: The baseline model relied on traditional security such as firewalls at the network edge and static rules for access control. This approach has several gaps such as:

1. Lateral Movement: Without internal network segmentation, attackers can move freely inside the system after getting an initial foothold in the system.

2. Identity Verification: The absence of dynamic identity checks, means that the initial network device trust is the only security in place. This would make the network vulnerable to compromised credentials.

Defence-in-Depth an alternative to Zero Trust Solution: The defence-in-depth is an approach that adds multiple protection systems such as intrusion detection system, endpoint protection and multiple firewalls. While this provides much enhanced security in a

simulated environment, its feasibility with IoT devices are untested and the increased complexity is often not been tested in a complete corporate system.

6.2 Discussion

The experiments conducted in this study were designed to evaluate the effectiveness of implementing Zero Trust focussing on addressing vulnerabilities such as VLAN hopping, ARP poisoning, and MAC flooding. These tests were performed within a simulated office network using tools such as Cisco Packet Tracer and the Microsoft Threat Modelling Tool (MTMT).

6.3 Limitations

1. **Simplified Environment:** Cisco Packet Tracer provides a simulated environment that lacks the complexity of real-world networks. Factors like latency, hardware-specific vulnerabilities, or advanced attack vectors cannot be fully replicated.

2. **Static Implementations of Zero Trust rules:** Configurations such as ACLs and rate-limiting are static in nature, making behavior based zero trust adaptation does not present in the simulation.

3. **Micro Segmentation:** Cisco Packet Tracer can simulate network segmentation, but the capabilities are limited, different devices can be given separate default gateways, however micro segmentation cannot be simulated.

4. **Integration of outside security features and Operating system tools:** Tools like Azure DDoS guard or AWS DDoS protection are OS level proprietary software and thus cannot be simulated in cisco packet tracer.

5. **Integrating it with outside tools:** Real Time monitoring tools like the SIEM tools cannot be simulated and the simulation can only rely on logs.

7 Conclusion and Future Work

This study demonstrates the critical importance of adopting a Zero Trust Architecture to secure corporate IoT ecosystems in an era of escalating cybersecurity threats. It shows the necessity of transitioning to a Zero Trust security model for corporate IoT networks, given the limitations of traditional perimeter-based approaches. By using Cisco Packet Tracer and the Microsoft Threat Modeling Tool, this paper has simulated practical scenarios and proposed mitigations for common vulnerabilities, demonstrating the viability of ZTA in resource-constrained environments. The proposed framework offers a path for small to medium-sized enterprises to adopt ZTA frameworks. Additionally, exploring compliance with legal standards and laws will ensure that the architecture remains relevant and practical in diverse operational contexts. Key measures, including network segmentation, least

privilege access, continuous verification, and advanced access control mechanisms, were successfully simulated to prevent lateral movement, unauthorized access, and denial-of-service attacks.
The study highlights that network segmentation reduced the risk of lateral movement by isolating critical servers and IoT devices by segmenting them into separate zones. The principle of least privilege ensured that users only have the basic privileges and to maintain them the process of continuous verification come in place. Additionally, features like rate limiting and port security mitigated risks associated with resource exhaustion and Layer 2 vulnerabilities, such as MAC flooding.

Future research should focus on enhancing ZTA frameworks with advanced behavioral analysis and real-time threat detection and response. This optimized approach can serve as a foundational security model for corporate IoT ecosystems, ensuring both operational efficiency and robust defense against cyberattacks.

Future Work

This research establishes a foundational framework for securing corporate networks with IoT devices in mind. However given more time, several areas do warrant a further exploration and enhancement for a more complete solution:

1. **Dynamic Adaptation of Zero Trust Policies:** Future implementations taking inspirations from this paper should focus on incorporating dynamic policies that adapt to real-time behavior such as behavior-based access control lists and real time threat monitoring.

2. **Integrating with Advanced Security tools:** This study mainly focused on Microsoft threat model and cisco packet tracer, however a more in-depth simulation or an actual office network would be able to levy tools like AWS Shield, Azure DDoS Protection and SIEM tools. Making sure of ZTA's effectiveness when all the tools are used.

3. **Lightweight Cryptographic Mechanisms:** Given the resource constraints of IoT devices, there is a need for lightweight yet robust cryptographic techniques. Research into new encryption algorithms and authentication mechanisms tailored for low-power devices.

4. **Simulation of Complex, Real-World Mechanisms:** Expanding the simulation to more complex environments that replicate real-world corporate IoT ecosystems and multi-cloud architectures.

5. **Behavior-Based Access Controls:** Integrating behavior-based access control systems that use historical data and real-time inputs to refine permissions can help enhance security. These systems can dynamically alter user and device privileges based on contextual factors, such as location, time of access, or device health.

References

1. Gupta, C. and Varshney, G., Year. *An improved authentication scheme for BLE devices with no I/O capabilities*. [online] Available at: https://www.sciencedirect.com/science/article/pii/S0140366423000014?casa_token=j0W3YSqrpsoAAAAA:C9vIfawT-yVwCEwt4bbpPdtOID3waAXcTUO9ChhX73vDzLAHojli7RR1K-0z2auNhhZoB4-pOdIk [Accessed 11 Dec. 2024].

2. Fehér, D.J. and Sándor, B., Year. *Effects of the WPA2 KRACK Attack in Real Environment*. [online] Available at: https://ieeexplore.ieee.org/stamp/stamp.jsp?tp=&arnumber=8524769 [Accessed 11 Dec. 2024].

3. Rajkumar, V.S., Stefanov, A., Musunuri, S., and de Wit, J., Year. *Exploiting Ripple20 to Compromise Power Grid Cyber Security and Impact System Operations*. [online] Available at: https://ieeexplore.ieee.org/stamp/stamp.jsp?tp=&arnumber=9692179 [Accessed 11 Dec. 2024].

4. ABC News, 2024. *Robot vacuum yells racial slurs at family after being hacked*. [online] Available at: https://www.abc.net.au/news/2024-10-11/robot-vacuum-yells-racial-slurs-at-family-after-being-hacked/104445408 [Accessed 11 Dec. 2024].

5. Wired, 2024. *Kia web vulnerability allows hackers to track vehicles*. [online] Available at: https://www.wired.com/story/kia-web-vulnerability-vehicle-hack-track/ [Accessed 11 Dec. 2024].

6. Jadidi, Z., Pal, S., Li, Q., and Foo, E., Year. *Cyber Security Resilience in Industrial Control Systems using Defence-in-Depth and Zero Trust*. [online] Available at: [Accessed 11 Dec. 2024].

7. U.S. Department of Defense, 2022. *Zero Trust Reference Architecture (ZT-RA) Version 2.0*. [online] Available at: https://dodcio.defense.gov/Portals/0/Documents/Library/(U)ZT_RA_v2.0(U)_Sep22.pdf [Accessed 11 Dec. 2024].

8. Wu, K., Cheng, R., Xu, H., and Tong, J., Year. *Design and Implementation of the Zero Trust Model in the Power Internet of Things*. [online] Available at: [Accessed 11 Dec. 2024].

9. Colombo, P., Ferrari, E., and Tumer, E., 2021. *Access Control Enforcement in IoT: state of the art and open challenges in the Zero Trust era*. In: *Proceedings of the IEEE Transactions on Industrial Informatics*, vol. [1], pp. 159–166. doi: 10.1109/TPSISA52974.2021.00018.

10. Patil, A.P., Karkal, G., Wadhwa, J., Sawood, M., and Reddy, K.D., Year. *Design and Implementation of a Consensus Algorithm to Build Zero Trust Model*. [online] IEEE. Available at: [Accessed 11 Dec. 2024].

11. Samaniego, M. and Deters, R., 2018. *Zero-Trust Hierarchical Management in IoT*. In: *Proceedings of the 2018 IEEE International Congress on Internet of Things (ICIOT)*, doi: 10.1109/ICIOT.2018.00019.

12. Khan, R., McLaughlin, K., Laverty, D., and Sezer, S., *STRIDE-based threat modeling for cyber-physical systems*. [online] IEEE. Available at: [Accessed 11 Dec. 2024].

13. SecureW2, Year. *How do MAC spoofing attacks work?* [online] Available at: https://www.securew2.com/blog/how-do-mac-spoofing-attacks-work [Accessed 11 Dec. 2024].

14. The Hacker News, 2019. *Hackers Steal MAC Addresses from ASUS Routers via a Backdoor*. [online] Available at: https://thehackernews.com/2019/03/asus-hack-mac-addresses.html [Accessed 11 Dec. 2024].

15. Author(s), Year. *Title of the article*. *Journal Name*, [online] Volume (Issue), pp. [page range]. Available at: https://www.sciencedirect.com/science/article/abs/pii/S0045790612001140 [Accessed 11 Dec. 2024].

16. Author(s), Year. *Title of the article*. *Journal Name*, [online] Volume (Issue), pp. [page range]. Available at: https://www.sciencedirect.com/science/article/abs/pii/S0045790612001140 [Accessed 11 Dec. 2024].