Proactive Defense Strategies for Emerging LAN Threats

A Research Paper into LAN Network Securing

Max Dabbs

4-25-2018

Table of Contents

Summary

Much of an average person's focus and consideration for internet security and protection is aimed at protecting and obfuscating communication with and to the wider internet from interception and snooping, what about the devices within their LAN? In this project, I looked into the current and emerging issues applicable to residential network security, and possible ways to counter/mitigate. After narrowing it down, I then chose one promising solution to simulate using GNS3 simulation software.

The results of my research and simulation indicated that the most promising solution would be the combination of network segmentation and minimum password requirements, with the potential addition of device MAC address whitelisting. I suggested that due to the complexity and risks of not setting up a network segmentation correctly, users should use the basic ‘Guest Network’ in their router until more consumer-friendly segmentation software is developed. Even with my promising results, I identified multiple issues with my simulations, suggesting the need for further testing beyond what I was able to achieve.

Introduction

While not seeming to be a major concern, with the potential of backdoors and exploitation of the increasing number of internet-enabled devices and always-on smart home appliances in the home, the risk is ever increasing.

Given network security is a never-ending matter of trying to stay ahead of intruders and exploits, there is always changes and breakthroughs in network security to consider. Additionally, since the majority of consumers have little to no understanding of network and device security and importance, it is unreasonable to assume devices and infrastructure in residential networks is up to date, nor to expect users to deal with more stringent/strict policies employed in business/government networks.

Background

IoT

Internet of things (IoT) is a term usually used to describe interconnect networked devices, often time small and low power, that connect and exchange data between other devices over the internet or an intranet (Internet of things, 2025). In 2018, there were estimated to be 8.4 billion IoT devices worldwide, which grew to nearly 20 billion in 2024 (Sinha, 2024). While the interconnected nature of IoT is their main benefit, it is also their biggest weakness, as the combination of their weak security and network addressability creates a large and alluring target for attackers (Chapman & Uren, 2018).

Risks

When it comes to IoT devices, there are several major threats, the most major being lack of hardening, insecure storage and transfer, lack of device management, botnets, weak credentials, and insecure APIs.

Physical Hardening

As the majority of IoT devices are deployed and interacted with remotely, there is no feasible way to properly secure them against physical attacks (SecurityScorecard, 2021). As a result, attackers can physically interact with the IoT device, allowing them to perform all sorts of attacks, such as reading the on-board memory, attaching or detaching hardware, and even installing equipment to intercept/modify in and outgoing communications (SecurityScorecard, 2021).

Data Storage/Transfer

As IoT devices often store confidential and sensitive data — for example, API keys, credentials, etc — on unencrypted onboard storage, if an attacker can remotely login or physically access the IoT device, they can extract and download this data (Information-technology Promotion Agency, 2008).

Related to this, IoT devices often times employ unencrypted data transfers to communicate and send data (SentinelOne, 2024). An attacker with the ability to snoop on the wired or wireless communications could therefore intercept confidential information in transit.

Given these two concerns, with minimal effort, an attacker can gain important and sensitive information about the IoT devices and, potentially, more traditional devices, such as databases, web servers, etc, that the IoT devices interact with.

Device Management

As many IoT devices are expected to operate with little to no interaction, they are often not actively monitored or managed by an entity (SecurityScorecard, 2021). This means that should a device become compromised or taken offline temporarily, it is unlikely for someone to immediately notice or proactively intervene (SecurityScorecard, 2021).

Botnets

As there are so many IoT devices, should an attacker devise a way to compromise a large enough number of devices, they can potentially create a massive botnet (SecurityScorecard, 2021). As IoT devices are distributed and numerous, they can be hard to track and mitigate when part of an attack. This is not even a hypothetical issue, as there has been at least one botnet consisting of majority IoT/smart devices (BBC, 2017).

Credentials

As a lot of IoT devices are shipped with very weak and often times identical ‘factory’ passwords that are not often updated by the user, the attackers can easily, often times autonomously, log into these devices and gain access and control (SentinelOne, 2024). As these attacks are so straightforward and easily automated, for example by trying the same set of credentials on all open ports or devices of a domain, they are often times the go-to attack by hackers and thieves seeking access (SentinelOne, 2024).

Weak APIs

Application programming interfaces (APIs) are software interfaces that allow two applications or systems to communicate effectively without the need for a deep understanding or access permissions or the target system. As APIs are usually external facing and designed to interact with external connections, they act as a very tempting attack vector for attacks (SecurityScorecard, 2021). If the API is badly designed or overly general, attackers can exploit weaknesses and oversights in the API to gain access or create a backdoor into a device or network.

Impact

Not only can IoT device attack cause inconvenience and headaches for the individuals or groups that operate and rely on them, but given the growth in IoT devices in crucial infrastructure and devices (Chapman & Uren, 2018), an attack or takeover could disable thing like traffic lights, power grids, trains (Chapman & Uren, 2018), or even healthcare equipment (Wheatly, 2013).

In addition to the risk of attacks disabling or affecting operation of equipment or services, there is also the risk of data breaches and illegal access. For example, not only could an attacker steal sensitive information from the communications with a server, but if they gained access to internet-connected security cameras, they could spy on you. There is also the risk of misuse, for example, bot attacks and DDoS attacks from thousands of compromised IoT devices (BBC, 2017).

Research

In order to identify the most serious IoT risks to try to remedy, I performed research into both current or emerging network risks applicable to residential LAN, but also cybersecurity practices and software/hardware that could be applicable to residential networks, and what identified risks they could counter.

Identification

Current/Future Risks

In my research, I identified countless issues though many were niche or already mitigated enough to not be a major issue.

Physical Access

If a person can physically access and interact with network equipment or wired ports, they are able to modify the setup and configuration, or add new devices and equipment within the network. As a result, an attacker could attach equipment to a network, for example, through attaching a device to an open ethernet port or placing an invisible 'tap' in the network communications chain. The attacker could then listen to communications, modify network device configuration, or even steal data from devices.

User Misuse

If an authorized and expected user of a network or device either intentionally or unintentionally accesses or modifies settings or files, or even add new devices, they can affect or completely compromise the security and safety of a network (Sophos Ltd., n.d.). Additionally, the user could potentially access or share sensitive or private information, and share or distribute it to people not permitted to see/know the contents.

While the user misuse might not be nefarious or intentional, attackers can use the actions taken or instruct user to perform actions as to access or exploit a system that would otherwise be inaccessible or secure.

Misconfigured Network Equipment

If network equipment, such as firewalls and routers, is set up or configured incorrectly, exploits, holes in the security and/or ruleset issues can allow attackers to attack and gain access to an otherwise secure network (Sophos Ltd., n.d.). By periodically ensuring the configurations are correct, and employing automated monitoring software, the number and impact of misconfiguration issues can be reduced.

Weak Wi-Fi Security

With the first encryption for Wi-Fi, WEP, being introduced in 1999 (Information-technology Promotion Agency, 2008) and the latest, WPA3, coming out in 2018 (Wi-Fi, 2025), there is plenty of time and old equipment to cause networks operating on older, less secure wireless encryption protocols.

One of the largest issues with using outdated Wi-Fi security protocols is the ability for an attacker to exploit weaknesses in the protocol (Information-technology Promotion Agency, 2008) that were mitigated by later revisions (Wi-Fi, 2025) (Wi-Fi Alliance, 2025). By exploiting these exploits, an attacker can gain access to the network, allowing for snooping on devices and giving a foothold for deeper or further attacks.

Weak Wi-Fi security can be mitigated by employing the new WPA3 protocol, as it mitigates many issues present in WPA2 (Wi-Fi Alliance, 2025). If this is not possible — for example, an old/ISP Wi-Fi router that does not support WPA3 — then ensuring that the wireless protocol is set to WPA2-AES, and not TKIP or TKIP/AES, will reduce the risk of exploits as WPA2-AES employs the strongest security protocol currently available for WPA2 (Fitzpatrick & Hoffman, 2023) (Information-technology Promotion Agency, 2008).

Unsecured Wi-Fi

While not as common as it used to be (Mathews, 2021), Wi-Fi networks without a password may be convenient as there is no need to enter and remember a password, it leaves the network open to anyone nearby to connect to. This allows attackers not only use the connection for launching attacks on other networks, but to see within the local network, and more easily attack or exploit local devices.

Network Services

By exploiting weaknesses in common network services, attackers can potentially gain access to devices and networks (Remote Services Exploitation - Definition, Examples, & Prevention, n.d.). For example, WannaCry ransomware uses a SMB1 exploit to spread itself around networks (Remote Services Exploitation - Definition, Examples, & Prevention, n.d.).

While it is not possible to completely prevent exploitations in network services, by ensuring software is kept up-to-date and unnecessarily services are disabled, the risk of exploitation can minimized.

Viruses and Malware

Malicious software (Malware) is any software designed to harm, exploit, or compromise personal devices or network hardware (What Is Malware?, 2025). Malware is usually designed to perform one type of attack, such as adding additional ads, keylogging, network spying, backdoor access, crypto mining, ransoming, or taking devices/networks offline (What Is Malware?, 2025). Malware can be spread through multiple methods, including, USB drives, downloaded files, links, and even a file server/share (What Is Malware?, 2025).

Computer viruses spread by first infecting the files and system of a computer system by copying itself before infecting any devices or drives that are attached in order to spread itself to other systems (CISA, 2023). Nowadays, most viruses are spread through email attachments (CISA, 2023), though it is still possible to be infected through downloaded or transferred files. While viruses are often mainly harmless, they are sometimes designed to damage or destroy files and/or the entire installation.

As both malware and viruses can easily be spread by accident through file transfers and shared drives, an attacker just needs to infect one device within a network to potentially infect all the devices within the LAN. This means through an action as simple as opening an email or a link, an attacker can gain backdoor access to the network through the infected devices, or have the infection kill or ransom important devices and data.

Ethernet Data Interception

As the ethernet protocol doesn't have a built-in method for ensuring the message origin or integrity (Patel & Khoussainov, 2000), an attacker could intercept, and potentially modify, the data packets between the sender and the destination in the local network (Sophos Ltd., n.d.).

While this can potentially be remedied by using encryption, most local communications are assumed to not be public or exposed enough to need encryption or obfuscation (Why isn't Ethernet encrypted?, n.d.), leaving them open to interception by someone with access or a compromised network device, such as a switch. While Wi-Fi is usually encrypted nowadays, it is still susceptible to a similar attack, that being a Man-in-the-Middle attack.

Man-in-the-Middle (MITM) Attack

As Wi-Fi relies on wireless communications, the strength of the connection between the client and the base station affects the reliability, latency, and speed of the connection (ELI5: How does wifi signal strength affect internet speed, if at all?, n.d.). As a result, devices will try to connect to the strongest signal in a Wi-Fi mesh network.

If an attacker broadcasts a Wi-Fi network, either a relay or a separate internet connection, with the same attributes as a target network, client devices that are closer to the attacker than the real base station, and therefore receiving a stronger connection from the attacker, will communicate with the attacker's device instead (Bialy, 2022). The attacker can then intercept, read, and even modify the data before sending it onto the destination (Information-technology Promotion Agency, 2008) (Bialy, 2022).

While this is a serious issue, MITH attacks can be mitigated by keeping unauthorized users off network by having the Wi-Fi configured with strong encryption, though an authorized user can still perform an attack if they know the password. With the new WPA3, as long as the connection is not downgraded to a WPA2 connection, MITM attacks are completely prevented through operating channel validation, which uses more complicated key exchanges than WPA2/WPA/WEP that cannot be spoofed or brute forced by an attacker (Halbouni, Ong, & Leow, 2023).

Weak Passwords

Weak passwords not only include old/short passwords, but also the default passwords that came with equipment, such as the default credentials for a wireless camera, and easy-to-remember passwords, such as address, birthdates, and family member/pet's name.

While these short and/or easy to remember passwords are convenient, their length and commonness makes them quick and easy to brute force with free tools like hashcat (Mathews, 2021) (hashcat - advanced password recovery, n.d.). Attackers therefore can quickly gain access to devices and networks where these weak passwords are employed, allowing complete and unauthorized access to networks and information.

Shared Credentials

While having the same login credentials for multiple devices can make login and inter-device connections more streamlined, if an attacker obtains the login credentials for one of these devices, they thereby gain access to all devices that share those credentials. Threfore, like websites, it is recommended to have distinct and different login for each device in the network.

Possible Solutions

While I was able to find many idea and possible solutions to counter many of the identified risks, many required complex, and often expensive, equipment and setups to operate effectivly. I therefore narrowed the potential solutions to consider to just a handful based on their feasibility for an average user, their potential to be implemented with little or minimal additional hardware, and their minimal costs.

MAC Whitelist

Media access control (MAC) whitelists work by only allowing devices whose MAC address is listed as permitted to successfully connect and interact with the network . This concept should be effective mainly in countering weak Wi-Fi security and physical access, though this might be additionally effective in preventing user misuse and data interception due to restricting additional device's access the LAN.

As MAC addresses are spoof-able (Is a MAC address whitelist good security for my network?, 2009), this will not prevent an attacker with enough time or existing knowledge of the network and/or approved devices to connect, but should prevent most unauthorized connections (Is a MAC address whitelist good security for my network?, 2009).

Network Segmentation/Guest Network

Network segmentation works by dividing the network into smaller parts by controlling how traffic flows among the parts (Cisco, n.d.). This can a complete blocking of flow between segments, or just allowing only a limited type or destination of packets (Cisco, n.d.). This can be accomplished using firewalls, in addition to software configurations like Access Control List and VLAN (Cisco, n.d.).

As many attacks rely on attacking the network from an added or compromised device, by limiting what devices can see and interact with each other limits the potential and impact of most of the identified risks, including malware and viruses, physical access, weak Wi-Fi security, user misuse, and network services. The biggest issue with this is the additional time and software/equipment needed to set up and maintain. In addition, there is the potential for segmenting devices in such a way as to defeat the benefits, for example, by placing the majority of devices in the same segment. A simpler and (currently) more consumer-oriented/friendly variation of this would be placing less secure and guest/temporary wireless IoT/smart devices into the guest Wi-Fi network that can be activated on all/most residential Wi-Fi routers (Sophos Ltd., n.d.).

MACsec/IPSec

IPSec is a set of communication protocols and rules created in the 1990s for setting up secure communications over a network (Amazon Web Services, Inc., n.d.). IPSec adds encryption and authentication to the standard IP communications (Amazon Web Services, Inc., n.d.). In addition to encryption, IPSec also authenticates the source of the data (Amazon Web Services, Inc., n.d.).

MACsec is a point-to-point encryption over Ethernet within a network (Dubroca, 2016). MACsec defines secure channels to allow symmetric encrypted communication between ‘nodes’ over Layer 2 (Dubroca, 2016). While MACsec is useful, due to being designed for Ethernet connections, it cannot work over Wi-Fi (Dubroca, 2016), which has offered its own encryption since 1999 (Information-technology Promotion Agency, 2008), though this mean neither encryption will apply on the wired portion for communications between Wi-Fi and Ethernet devices.

The main difference between IPSec and MACsec is that IPSec operates on the network layer (Layer 3) while MACsec operates on the data link layer (Layer 2) (Gargan, 2024). As a result, IPSec is considered better suited for encryption over different networks, for example, between offices, while MACsec is suited more for connections within the same LAN (Gargan, 2024). Either way, IPSec and MACsec are well suited for mitigating data interception risks.

Minimum Password Requirements

By enforcing a minimum password requirements, you can ensure everyone on the network has a minimum level of protection against password attacks. According to the National Institute Standards and Technology (NIST), to ensure security, you should ensure the longest possible password/phrase possible, preferably with a minimum length of 8 characters and a max of 64 (National Institute of Standards and Technology, 2017). In addition, NIST recommends against the use of a password 'hints' or allowing the use of certain items in the password, such as previously compromised passwords, dictionary words, repetitive or sequential characters, and context-specific words/phrases (service name, username, etc) (National Institute of Standards and Technology, 2017).

An alternative to traditional passwords, there is the 'random' word-based passphrases — think 'correct horse battery staple' from xkcd (Munroe, 2011). While the complexity of a word-based passphrase is not necessarily stronger than a strong password of similar length (Is "Password Strength" (still) legit?, n.d.), the strength lies in being easier to remember than a similar strength random-character password (Are passwords with words really safer than passwords with complex characters?, n.d.). Like the NIST guidelines, the use of passphrases would require enforcing a minimum word length, and may be more secure/implementable if the passphrase was automatically generated instead of being entered by the user.

Minimum password/passphrases requirements will not only mitigate issues with weak passwords, but if implemented network-wide, it could also prevent shared credentials by ensuring, for example, the hash does not match with any other device or local account.

WPA3

Release in 2018 (Wi-Fi, 2025), WPA3 is the newest version of Wi-Fi security. It offers changes to mediate the shortcoming of WPA2, including MITM attacks, DNS snooping, and brute-forcing access (Halbouni, Ong, & Leow, 2023). In addition, the inclusion of Opportunistic Wireless Encryption allows for encrypted communications on a unsecured WPA3 network (Halbouni, Ong, & Leow, 2023), something not previously possible.

One issue with WPA3 in its current form is the ability to force a device to 'downgrade' from WPA3 to WPA2 through fallback, thereby allowing attacks that are possible in WPA2 (Halbouni, Ong, & Leow, 2023), such as those listed in the above paragraph. In addition, WPA3 is susceptible to various side-channel attacks to get insight into the password based on attributes like response time and memory access patterns (Halbouni, Ong, & Leow, 2023).

Conclusion

Although I was able to identify many risks and solutions, I had limited time and resources to perform testing. I therefore decided to limit my simulation testing to a virtual local area network (VLAN) network segmentation and whether it mitigated: physical access, user misuse, misconfigured network equipment, network service exploits, viruses/malware, data interception, weak passwords, and shared credentials. Network segmentation was chosen as it was the most promising option I could feasibly simulate on available hardware.

Testing

In order to identify the actual improvement compared to an average residential LAN network, in addition to a VLAN simulation, I decided to also simulate a star network as a control/baseline. This acts as a stand-in for an average residential network where all devices are attached directly to the ISP-provided modem/router through Ethernet and/or Wi-Fi.

Setup

Simulation System

For the simulation, I chose GNS3 due to being open-source, powerful, and used by industry professionals (GNS3, n.d.). For the system, I used a Lenovo ThinkPad T550 laptop with a Intel i7-5600U with 4GB of DDR3 ram. GNS3 was installed on a Kingston A400 SSD and ran with Python 3.11.2. This setup was chosen not only due to issues with trying to run GNS3 under macOS 15, mainly with the GNS3 VM running correctly (GNS3 VM with Virtualbox 7: Host-only adapter not available any more · issue #3472, 2023) and not being recognized by GNS3 itself, but also Linux not requiring running both the GNS3 and the GNS3 VM to use all features (Getting started with GNS3 - Should you use the GNS3 VM?, n.d.).

Baseline/Control System

For the control, I attached a network switch to a NAT interface to allow the system to access the internet, in addition to this being similar in function to a common modem and router combo. I then attached two virtual PC simulators (VPCS), PC1 and PC2, to represent two personal devices, such as computers and phones. I then created 5 additional VPCS, IoT1 through IoT5, to represent smart or IoT devices that might be found in a home.

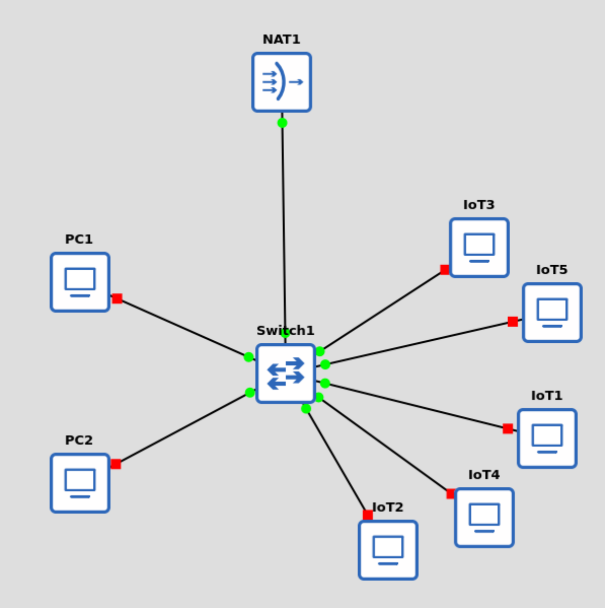

Figure 1: Screenshot of the system in GNS3

Network Segmentation

For the VLAN network segmentation simulation, like the control, I created the NAT interface and network switch to represent the router/modem combo. While not necessary for functionality, I additionally created two more network switches, labeled PCLAN and IoTLAN, to make the VLAN segmentation and what devices are connected clear.

VLAN 1, identified in the GNS3 simulation as PCLAN, contained the two VPCS representing the personal devices. VLAN 2, labeled IoTLAN, contains the 5 VPCS representing IoT devices. White boxes were added behind the devices in GNS3 to further help differentiate the two VLANs.

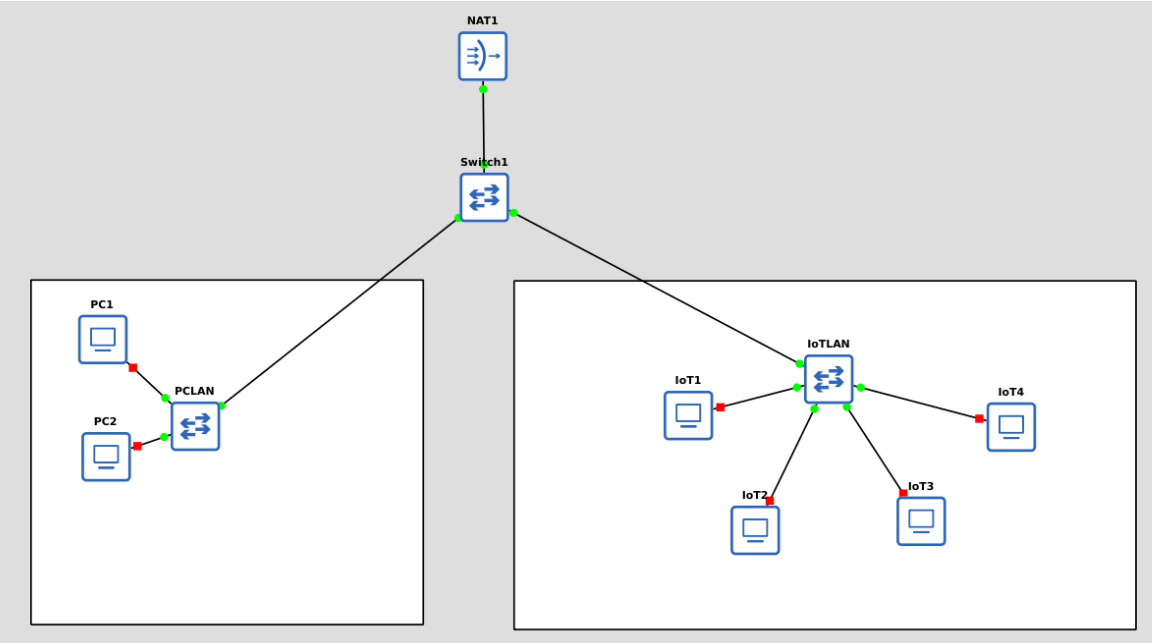

Figure 2: Screenshot of VLAN Network Segmentation Simulation

Simulation

To test the security of both GNS3 simulations, I attempted to query other devices in the simulation using ping. This was chosen as ping is a commonly available basic networking utility (Frisvold, 2020), but also due to only receiving a response if the destination is reachable by the sender (ping Command, n.d.). I had additionally planned to test if devices could intercept and/or read the network traffic in and out of the network, hence the NAT interface, but due to package issues, I was unable to get GNS3 to recognize the Wireshark installation, and therefore could not perform package monitoring or snooping inside GNS3.

Results

Baseline/Control System

For the control system simulation, attempts to interact and query any other peers, including from the opposite device category, was met with no restrictions or barriers. Like expected, there is no restrictions built into the star configuration as to querying any devices reachable by the router.

Network Segmentation

Unlike the baseline, in the segmented network, device were still able to successfully ping with devices within their VLAN, example, IoT1 could ping IoT2 through 5, but they were unable to ping VPCS in the other VLAN (PCx can't ping IoTx and vice versa). This indicates that the VLAN was successful in preventing communications with other VLANs, therefore preventing attacks or snooping across segments.

Conclusion

Control/Baseline

The baseline/control simulation indicated that the risk and impact would line up with what was found in the research. Therefore, it is safe to assume all risks are not mitigated.

Network Segmentation

Based on the simulation results, network segmentation, in this case with VLAN, will be effective in mitigating or potentially even preventing some of the risks identified.

Physical Access

As VLAN relies on a configuration to properly segment devices, an attacker with physical access could potentially reconfigure the VLAN, thereby allowing previously inaccessible devices to interact. Additionally, while not necessarily obvious from the simulation, VLANs don't inheritably prevent newly attached devices from connecting, as VLAN configuration are usually done by physical port (VLAN (Virtual LAN)? How VLAN Works, n.d.), meaning an attacker with physical access can attach a device to an open port and have it assigned to a segment automatically. This can potentially be mitigated with the addition of a MAC whitelist in addition to the VLAN segmentation.

User Misuse

Assuming the user doesn't have permissions to modify the VLAN configuration, segmentation would prevent user devices from accessing or interacting with devices or components outside what they require access to. While this won't prevent them from causing backdoors or leaks within their VLAN, it will at least prevent access or leaks to the wider network.

Misconfigured Equipment

As VLAN relies on a proper configuration, misconfiguration could easily void the benefits of segmentation by allowing devices to communicate and connect beyond their allowed connections.

Network Service Exploitation

By segmenting the network into smaller segments, the devices that can attack network services within the LAN is reduced, potentially reducing the chance of exploits. Attacks from outside the network — for example, from a forwarded port — would not be affected by the VLAN segmentation as the network will still work the same when interacting with outside the network.

Viruses/Malware

By segmenting the network into smaller sub-LANs, the spread, and therefore impact, of malware and viruses would be reduced compared to an unified LAN.

Data Interception

By segmenting the network, the devices that can potentially see or intercept the data transmissions is theoretically reduced. By placing the more susceptible and/or open devices, smart devices for example, on a separate segment from the rest of the network, the segmentation would prevent a compromised device in the segment from snooping on the inter-device communications of the 'main' segment(s).

Weak Passwords

A VLAN segmentation by itself will not prevent or mitigate weak passwords, though it would potentially reduce the potential for a compromised device to attack other device on the network.

Shared Credentials

A VLAN segmentation does not prevent the impact of shared credentials if they are learned, though it would prevent additional devices from being accessed if they are on different network segment(s).

Limitations

Real-World Application

As all the testing was performed within GNS3 simulations, there is the possibility that a real-world implementation would present issues or weaknesses not identified or modeled in a simulation. There is additionally the possibility that the positive results I obtained would be found to not be applicable to a real local network.

Size of Tests

As I was running the tests from a decade-old laptop, I was limited in the size and depth of the tests I could perform. I was unable to, for example, run simulations on networks with much larger number of devices like, for example, the developers of IoTSecSim could perform (Chee, Ge, Bai, & Kim, 2024).

Single Round of Simulation

Given the limited time for the project, I was only able to perform one simulations based on my research results. I was unable to take the results of the simulations, and perform recursive simulations with changes, for example, adding device whitelisting to the segmentation and re-testing.

Software Issues

Due to issues with getting GNS3 to recognize installed packages and interfaces, I was unable to perform certain actions, such as wiretapping using Wireshark or more complex network interfaces available through GNS3.

Hardware

As the laptop used was a dual-core system with only 4GB of RAM and 1GB swap, I was unable to use more complicated network devices, ex VMs, than the built-in VPCS. An actual OS simulation would likely have more complex operations and tests that could be performed. For example, some installations like Kali Linux have tools designed for performing pen testing, and therefore would be better suited to represent an attacker.

Discussion

My findings suggest that while network segmentation is effective in reducing risks in residential LAN setups, there are still risks identified not mitigated at all/enough by segmentation. These risks would likely require the addition of one or more solutions to be implemented along-side to mitigate.

Of the possible solutions I identified, the most effective for further mitigation would likely the addition of password requirements. Minimum password requirements would slow down or prevent an brute-force attack, including a physical access attack, given the attacker does not already have or know credentials. As VLAN does not prevent new devices from being added to segments, the addition MAC whitelisting would further mitigate the effectiveness, likelihood, and speed a nefarious device could connect.

Given the complexity of correctly configuring a software-based network segmentation, it is not realistic to assume the average consumer could set up a successful segmentation without creating misconfigurations, thereby exacerbating one of the identified risks. I would therefore suggest, at least until more user-friendly software becomes available, users to utilize the 'Guest Network' option in the router settings. While not as robust as a proper network segmentation, it would allow more risky devices to be 'quarantined' separately from the more sensitive devices.

Given the limitations in my testing, further testing is likely needed to confirm results and speculation. The next step would be to do larger network tests with more powerful hardware or real networking hardware.

Conclusion

In this project, I looked into the risks facing home networks with the rise of IoT and smart devices. My research identified several major risks that needed to be mitigated or completely resolved, in addition to a handful of possible solutions to remedy some or all of these risks. Of the solutions identified, I found network segmentation to the most promising. Given these results found, I performed simulations using GNS3; the results confirmed the research results.

Although segmentation was effective, I identified multiple risks still not mitigated. I propose the addition of minimum password requirements being enforced network wide, with the aim of slowing down or preventing unauthorized physical access and brute-force attacks. I also suggested implementing a device whitelist based on device MAC address to prevent unknown devices connecting.

Given the complexity of network segmentation and the real risk of misconfiguration, I suggest, at least for now, users employ the guest network setting in their existing router to create a very basic network segmentation. This would hopefully be a stop-gap until consumer-friendly network segmentation software is created or popularized.

Although my simulation was effective in testing how applicable a possible solution would be, there were still major limitations, mainly the lack of further testing with real hardware, the small and basic simulation due to weak hardware and software installation issues. I suggest further testing be performed with both/either more powerful simulation hardware or actual network hardware.

References

Amazon Web Services, Inc. (n.d.). *What is IPSec? - IPSec Protocol Explained*. Retrieved April 2025, from Amazon Web Services (AWS): https://aws.amazon.com/what-is/ipsec/

Are passwords with words really safer than passwords with complex characters? (n.d.). Retrieved April 2025, from r/crypto: https://www.reddit.com/r/crypto/comments/oqrg1e/are_passwords_with_words_really_safer_than/

BBC. (2017, January 20). *https://www.bbc.com/news/technology-38678466*. Retrieved from BBC News: https://www.bbc.com/news/technology-38678466

Bialy, M. (2022, January 8). *LAN security and how it is hacked*. Retrieved from Grandmetric: https://www.grandmetric.com/lan-security-attacks/

Chapman, E., & Uren, T. (2018, March 19). *The Internet of Insecure Things*. Retrieved from Australian Strategic Policy Institute | ASPI: https://www.aspi.org.au/report/InternetOfInsecureThings

Chee, K., Ge, M., Bai, G., & Kim, D. (2024, January). IoTSecSim: A framework for modelling and simulation of security in Internet of things. *Computers & Security, 136*. doi:10.1016/j.cose.2023.103534

CISA. (2023, March 17). *Virus Basics*. Retrieved from CISA: https://www.cisa.gov/news-events/news/virus-basics

Cisco. (n.d.). *What Is Network Segmentation?* Retrieved April 2025, from Cisco: https://www.cisco.com/c/en/us/products/security/what-is-network-segmentation.html

Dubroca, S. (2016, Febuary). MACsec: Encryption for the wired LAN. *netdev 1.1*.

ELI5: How does wifi signal strength affect internet speed, if at all? (n.d.). Retrieved April 2025, from r/explainlikeimfive: https://www.reddit.com/r/explainlikeimfive/comments/2rphm2/eli5_how_does_wifi_signal_strength_affect/

Fitzpatrick, J., & Hoffman, C. (2023, March 12). *Wi-Fi Security: Should You Use WPA2-AES, WPA2-TKIP, or Both?* Retrieved from How-To Geek:

https://www.howtogeek.com/204697/wi-fi-security-should-you-use-wpa2-aes-wpa2-tkip-or-both/

Frisvold, J. (2020, Febuary 11). *Ping, traceroute, and netstat: The network troubleshooting trifecta*. Retrieved from Red Hat: https://www.redhat.com/en/blog/ping-traceroute-netstat

Gargan, R. (2024, July 16). *MACsec vs IPsec - Unpacking The Differences*. Retrieved from Netmaker: https://www.netmaker.io/resources/macsec-vs-ipsec

Getting started with GNS3 - Should you use the GNS3 VM? (n.d.). Retrieved April 2025, from GNS3 Documentation: https://docs.gns3.com/docs#should-you-use-the-gns3-vm

GNS3. (n.d.). Retrieved from GNS3 | The software that empowers network professionals. : https://www.gns3.com/

GNS3 VM with Virtualbox 7: Host-only adapter not available any more · issue #3472. (2023, May 24). Retrieved from GNS3/GNS3-gui. GitHub: https://github.com/GNS3/gns3-gui/issues/3472

Halbouni, A., Ong, L.-Y., & Leow, M.-C. (2023). Wireless Security Protocols WPA3: A Systematic Literature Review. *IEEE Access, 11*, 112438-112450.

hashcat - advanced password recovery. (n.d.). Retrieved from https://hashcat.net/hashcat/

Information-technology Promotion Agency. (2008). 10 Major Security Threats. Retrieved from https://www.ipa.go.jp/en/security/vulnerabilities/gg76us0000008owo-att/000016942.pdf

Internet of things. (2025, April 14). Internet of things. Wikipedia. Retrieved from https://en.wikipedia.org/w/index.php?title=Internet_of_things&oldid=1285526227

Is "Password Strength" (still) legit? (n.d.). Retrieved April 2025, from r/xkcd: https://www.reddit.com/r/xkcd/comments/8vb9x3/is_password_strength_still_legit/

Is a MAC address whitelist good security for my network? (2009, Septemeber 27). Retrieved from r/netsec - Technical Information Security Content & Discussion: https://www.reddit.com/r/netsec/comments/9on4s/is_a_mac_address_whitelist_good_security_for_my/

Mathews, L. (2021, October 28). *70% Of Passwords For Home Wi-Fi Networks Are Terrible*. Retrieved from Forbes: https://www.forbes.com/sites/leemathews/2021/10/28/70-of-passwords-for-home-wi-fi-networks-are-terrible/

Munroe, R. (2011, August 10). *Password Strength*. Retrieved from xkcd: https://xkcd.com/936/

National Institute of Standards and Technology. (2017, June). *SP 800-63B, Digital Identity Guidelines: Authentication and Lifecycle Management* . Retrieved from CSRC: https://nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.800-63b.pdf

Patel, A., & Khoussainov, R. (2000). LAN security: problems and solutions for Ethernet networks. *Computer Standards & Interfaces, 22(3)*, 191-202.

ping Command. (n.d.). Retrieved April 2025, from Oracle Documentation: https://docs.oracle.com/cd/E19683-01/806-4075/6jd69oa8n/index.html

Remote Services Exploitation - Definition, Examples, & Prevention. (n.d.). Retrieved April 2025, from ExtraHop: https://www.extrahop.com/resources/attacks/remote-services-exploitation

SecurityScorecard. (2021, August 4). *8 Internet of Things Threats and Risks to Be Aware of.* Retrieved from SecurityScorecard: https://securityscorecard.com/blog/internet-of-things-threats-and-risks/

SentinelOne. (2024, November 5). *Top 10 IoT Security Risks and How to Mitigate Them*. Retrieved from SentinelOne: https://www.sentinelone.com/cybersecurity-101/data-and-ai/iot-security-risks/

Sinha, S. (2024, September 3). *State of IoT 2024: Number of connected IoT devices growing 13% to 18.8 billion globally*. Retrieved from IoT Analytics: https://iot-analytics.com/number-connected-iot-devices/

Sophos Ltd. (n.d.). *What is a local area network (lan)?* Retrieved April 2025, from Sophos: https://www.sophos.com/en-us/cybersecurity-explained/local-area-network-lan

VLAN (Virtual LAN)? How VLAN Works. (n.d.). Retrieved April 2025, from ExterNetworks: https://www.extnoc.com/learn/networking/what-is-virtual-lan

What Is Malware? (2025, April). Retrieved from Palo Alto Networks: https://www.paloaltonetworks.com/cyberpedia/what-is-malware

Wheatly, M. (2013, July 31). *Death By Internet of Things: How Smart Gadgets Kill*. Retrieved from SiliconANGLE: https://siliconangle.com/2013/07/31/death-by-internet-of-things-how-smart-gadgets-kill/

Why isn't Ethernet encrypted? (n.d.). Retrieved April 2025, from r/hacking: https://www.reddit.com/r/hacking/comments/ktjai1/why_isnt_ethernet_encrypted/

Wi-Fi. (2025, April 12). Wikipedia. Retrieved from https://en.wikipedia.org/w/index.php?title=Wi-Fi&oldid=1285250662&useskin=monobook

Wi-Fi Alliance. (2025, April). *Security*. Retrieved from Discover WiFi: https://www.wi-fi.org/discover-wi-fi/security