CREATION OF A 2-FLOOR HOME NETWORK

Jain, Ansh Ashwini   
23308320  
National College of IrelandDublin, Ireland  
x23308320@student.ncirl.ie

***Abstract-*The goal here is to create a 2-floor Home Area Network setup and to make it realistic with the use of actual devices. Then with the vulnerabilities found in the devices, I decided on three attack vectors which are Denial of Service, Memory Corruption and Remote over-the-air attack and discussed them in detail how effective can the attack be in the network. Then comes the mitigations which focuses on areas which can be done to avoid the attacks mentioned.**

***Keywords: Home, DDOS, Memory corruption, remote over-the-air, Network***

1. NETWORK SELECTION

The research for this is based on a Home Area Network (HAN), which basically means that a network where in how all of the devices present are connected within a home. I decided to go with a 2-floor setup of a smart home, with multiple smart devices used in the network. First floor consists of a hall with devices present, a kitchen and a room with the utilities of detectors and smart doorbells. The second floor also consists of a master bedroom, with an office setup present as well. There were multiple network types that I researched, more on that in detail below, before I decided to go ahead with specifically this network. The reason behind my choices is because I felt I could be more comprehensive and realistic about the reality of the attacks that can occur within a Home Area Network as compared to any other. Plus, given all places should have max security as and where possible, but in my opinion, I found out that a place like home and it’s security should be talked about more as we live all of our personal lives within this small place for most of our times. A Home Area Network will always have potentially the most sensitive data present in it considering it has multiple personal devices present, hence the risk associated will always be at the peak. Hence any way possible of an attack will need to be discussed to understand what can be done to mitigate the issue.

1. NETWORK SETUP

Now to understand the approach for this network setup, I first decided to understand which network type to work on, so for that I researched multiple networks present. For starters I researched different network types present, which included of, but not limited to:

* Local Area Network (LAN) & Wide Area Network (WAN):

A Local Area Network is a basic computer network which has a range of upto 2kms, which connects the network present in a limited area. They are simple and less complicated as compared to a Wide Area Network which covers a much larger geographical area for a network which can mean at a global scale as well [1].

* Metropolitan Area Network (MAN):

This network basically consists of a bunch of LAN’s connected over to share resources with the range being less than a WAN, means it can be limited to a city or a region.

* Storage Area Network (SAN):

The main goal with this network is to ensure a network connection between a server and a storage device. This can also include software devices and network switches. The main purpose with this network is to ensure storage access and the range is specific to data centres present.

* Near Me Area Network (NAN):

A Near Me Area Network is specifically for devices which are connected to each other within a proximity or a few meters away from each other by using short-range communications technologies. Examples include of Bluetooth, NFC etc; Majorly used in contactless payments, and sharing of resources within a proximity [2].

* Campus Area Network (CAN):

A Campus Area Network is used in educational environments such as our very own university like NCI. The main goal is to ensure that multiple separate LAN’s present are connected through a single network for ease of communication. The CAN is heavily confined to a specific campus and is owned by one single organization which manages it.

Then is when I stumbled across the Home Area Network (HAN) [3], and in a way I felt I could combine some to most of the network types present in a single network and I started to design the layout of the home I had in my head. It’s a smart home with IOT devices, and consists of 2 floors, the ground floor having all of the detectors, smart doorbell, A kitchen with multiple smart devices and a bedroom with a hall present. The first floor includes of a office with a storage present, and another master bedroom. There is a main router through which ethernet cables are pulled out to connect to streaming devices and a extended switch which connects to the first floor with ethernet cables connecting. There are also 2 mesh node’s for the Wireless Connection present, one for each floor. The main internet connects to the modem which is then connected to the router. Keeping all of this in mind I designed my network and started researching specific devices I will need to make my network. Following is the network setup diagram. The topology I used is a hybrid one with the main router connected through a star topology to all rooms present, left hand side being the ground floor, and right being the first floor. Each room has a wireless access point connected to its nearby devices in a wireless connection. The smart home is the doorbell with each camera representing a security camera in the room.

A diagram of a computer network

Description automatically generated

Fig. 1. The Home Network Setup.

TABLE I. SUMMARY OF MAIN DEVICES

|  |  |  |  |
| --- | --- | --- | --- |
| **Device Type** | **Device Name** | **Company Name** | **Release Date** |
| Router [4] | Archer AX21 (AX1800) | TP-Link | Dec 2022 |
| Modem [5] | CM3000 | Netgear | Sept 2024 |
| Network Switch [6] | GS110MX | Netgear |  |
| Wifi Extenders [7] | RE655BE | T-P Link | Nov 2024 |
| Network Attached Storage [8] | DS224+ | Synology | Aug 2024 |
| LIVING ROOM (Ground Floor) | | | |  |  |  |  |
| Smart TV [9] | S90 OLED | Samsung | 2024 |  |
| Streaming Device [10] | Fire Cube | Amazon | Oct 2022 |  |
| Smart Speaker [11] | Echo Spot | Amazon | Aug 2024 |  |
| Smart Lighting [12] | Hue Secure Line | Philips | Aug 2023 |  |
| Smart doorbell [13] | Video Doorbell (2nd Gen) | Ring | Aug 2020 |  |
| Smart plugs and switches [14] | Smart Plug | Wemo | Feb 2021 |  |
| KITCHEN (Ground Floor) | | | |  |  |  |  |
| Smart Refrigerator [15] | Bespoke 4-Door Flex | Samsung | June 2023 |  |
| Smart oven [16] | GE ProfileSmart Oven | GE | Feb 2023 |  |
| Smart dishwasher [17] | DFC612FV | LG | Feb 2023 |  |
| Smart coffee maker [18] | BES880 | Breville | Nov 2023 |  |
| OFFICE (First Floor) | | | |  |  |  |  |
| Desktop computer (wired) | Mac Studio (M2 Ultra) | Apple | June 2023 |  |
| External monitor | FlexScan EV3895 | Eizo | Sept 2020 |  |
| Work laptop | ThinkPad X1 Carbon Gen 11 | Lenovo | June 2023 |  |
| ROOM (Ground Floor) | | | |  |  |  |  |
| Smart Speaker [19] | Sonos S2 | Sonos | Oct 2023 |  |
| Smart lighting system | Hue Secure | Philips | Nov 2024 |  |
| Tablet | S9 FE | Samsung | Oct 2023 |  |
| ROOM (First Floor) | | | |  |  |  |  |
| Gaming console | PS 5 | Playstation | Nov 2020 |  |
| Smart TV | S90 OLED | Samsung | 2024 |  |
| Laptop | ThinkPad X1 Carbon Gen 11 | Lenovo | June 2023 |  |
| OTHER DEVICES | | | |
| Smart motion detector | Motion and Light Sensor P2 | Aqara | Jan 2024 |  |
| Smart smoke detector | Smoke Detector | Aqara | Nov 2024 |  |
| Security Cameras [20] | Wyze Cam V3 | Wyze | March 2024 |  |

1. ATTACK VECTORS

I decided to go for three different ranges of attack that can possibly happen on smart home area network, which include a Password Spraying attack on the routers, Denial of service attack on the security cameras and lastly the Remote over-the-air attack on the speakers. All the three attack vectors are backed by market analysis and vulnerabilities found are real and not assumed. The range specifically in the three attacks are different with each having their own approach and affected areas being different. Plus, post attack growth for all three is also very different from each other which I will be discussing further.

|  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- |
| Attack No. | Type | Technique | CVE Number | Device | Date of Incident |
| 1 | Denial of Service | Remote code Execution  Password Spraying | CVE-2023-1389 | Router | Apr 2024 |
| 2 | Memory Corruption | Heap-Based Buffer Overflow | CVE-2024-6246  CVE-2024-6247 | Security Camera | Nov 2024 |
| 3 | Remote over-the-air | Remote code execution | CVE-2024-20018  CVE-2023-50809  CVE-2023-50810 | Speaker | Aug 2024 |

TABLE II. ATTACK VECTORS

1. DENIAL OF SERVICE

The Router (Archer AX21 (1800)) by TP Link has been considered for this scenario which when compromised can cause various issues. Motive behind hacking a router can be assumed to eavesdrop and steal information for further ransom or other reasons. As the root of all devices is the router, The Network Traffic can be monitored by malicious actors, and the devices communicating with are compromised. The main used is password spraying attack by 16000 botnets which basically means that a brute force attack is carried out, and thousands of IP addresses try an attempt at logging in [21]. Because an individual device only logs in a few times, it becomes difficult to detect the attack. Now specifically for this router, it has been found to be vulnerable to CVE-2023-1389 [25] which contains a command injection vulnerability where in a specific parameter mess up can cause the attacker to run commands at root level with POST request. This weakness is linked to CVE-77 which basically means ‘Improper Neutralization of Special elements used in a command’ [22].

Affected Devices

The Router is the main source of any network present. As it is the centre, all the related devices are at a risk of being compromised. This includes, IOT devices, smart home gadgets, networks etc. Following is a list on what can happen next if that device is compromised.

1. Wireless Access Points: The attacker can gain access to the WAP’s and affect all the networking in the house, the traffic can be monitored or altered. The attacker can even carry out a Man in the middle attack and cause disruption by redirecting the owner to malicious websites.

2. IOT Devices: All devices connected get exposed to potential attacks, including malware installation which can cause theft of data. The data on the device and the device as well can be potentially locked out for a ransom or spyware, keyloggers can be installed to capture sensitive information like passwords, bank details [23].

3. Network Outage: The whole of network can be possibly shut down causing disruption with connection and living can become much more difficult as nothing will seem to be in control [24].

The password spraying attack by the botnets affected silently attacked the TPLink devices present, and for this router present it exploited the command injection vulnerability and kept causing disruptions to the router. This attack is called the denial-of-service attack as it overwhelms the system with passwords silently without triggering the mechanisms for brute-force.

1. MEMORY CORRUPTION

The security cameras are the eyes of the house, which when compromised can allow the attackers to gain live feed access, record the footage which can be used as ransom at a later stage, or even as simple as spying which is an invasion of privacy. A lot of information is gained as to understanding the day-to-day activity carried out, so the chances of a break-in increase, or exploitation of other devices can be carried out to because once in they can visibly see passwords entered or device information to find vulnerabilities out [26]. For example, the cameras used in the picture are Wyze Cameras V3, which has been reportedly facing multiple issues with their customers and been getting negative feedback.

Vulnerabilities

First Outage: Back in February 2024, a denial-of-service attack claimed to show footage of one user to the other without giving proper consent. Around 13000 customers were affected by this. The company claimed that due to a third-party caching client library issue, system was caused with unprecedented load conditions which caused all of the devices to start up all at once. This caused a chaos in the IDs between the users and the devices, and this rose up to accounts being able to see other accounts. There was no CVE that was generated for this attack nor any exploit found online but this issue caused a lot of customer backlash and negative marketing [27].

Different vulnerabilities: After this outage, there were a lot more vulnerabilities found in the Wyze CAM V3.

|  |  |  |
| --- | --- | --- |
| **CVE-Number** | **Description** | **Explanation** |
| CVE-2024-6246 [30] | Heap-Based Buffer Overflow | This vulnerability allowed attackers to execute malicious code, on the affected cameras by being there present physically. This issue is a result of lack of proper validation of the length of the user-supplied data before it can be copied to a heap-based buffer. |
| CVE-2024-6247 [29] | WiFi SSID OS Command Injection | The vulnerability lies in how SSIDs embedded in scanned QR codes are processed. It stems from insufficient validation of a user-provided string prior to its use in a system call. This flaw could allow an attacker to execute code with root privileges. |
| CVE-2024-6248 [31] | Cloud Infrastructure Improper Authentication | The vulnerability for this is in the run\_action\_batch endpoint of the cloud. This is when MAC address is used as the only source of authentication.[28] |

TABLE III. CVE’s

All of the vulnerabilities mentioned above are means for a user to attack and hack the security cameras. The impact of these vulnerabilities is still under analysis.

1. REMOTE OVER-THE-AIR

In this attack specifically, the speakers are the targeted device, and which are used to eavesdrop into the rooms where the speakers are present and can have a listen on the users present. The Sonos Speakers have the following vulnerabilities present:

1. CVE-2023-50809: Vulnerability present in the Sonos One Gen 2 Wi-Fi Stack which does not validate an information while an ongoing WPA-2 handshake, which has the potential to lead to remote code execution [35].
2. CVE-2023-50810: This is regarding a vulnerability present in the U-boot component, which allows for code execution with the highest privileges [36].
3. CVE-2024-20018: In the WLAN driver, because of the invalid input validation, there is a chance of an out of bounds write which can lead to local escalation of privilege as well. The user will need not be present for the same and no additional privileges will be needed too [34].

ISSUES

There are many issues that can occur if a hacker gains access to the speakers by exploiting the vulnerabilities mentioned above. Following is some of them.

* Eavesdropping: The attacker after the hack will be able to listen to each and every thing in the room and can record for ransom later or gain access to sensitive information.
* Unauthorised Control: The controls of the speaker will now be in the hand of the attacker which can cause a significant disruption in the household [32].
* Network Vulnerabilities: As the speakers are connected in a network in the household, an attacker can use them as gateway to exploit other devices present over and cause further issues.

The speakers present in the scenario are hacked via remote code execution with an attacker who is in the WiFi range of the speaker. The function in the WPA2 four-way handshake, notably known as, WpaParseEapolKeyData function, contains a bunch of weak points, which when clubbed together can be used to achieve a stack buffer overflow. A detailed test conducted by the NCC group revealed all the issues and a post exploitation scenario where in to understand the impact of the vulnerability found was conducted. The impact of the issues found was successfully carried out and the speaker was hacked from both vulnerabilities found [33].

1. MITIGATIONS

These are all the issues that can happen from the vulnerabilities that we discussed. There are multiple ways and techniques present to ensure that the individual who is creating the same home network can use to avoid such mishaps from happening. Mitigating the issue to the best possible is a very important part as without incorporating the practices there can be major losses.

Practices

Strong passwords: Here it will be very critical and important to understand that the passwords being used are unique and strong, for each and every device used, and whenever and wherever possible, Multi-Factor Authentication is enabled to ensure there is an added layer of security.

Threat Intelligence: As we saw with the first attack vector, the botnet attack, one way can be to block malicious IP addresses when found and also use geofencing to restrict the number of times user logs in. CAPTCHA as a method can also be implemented when a few failed attempts is hit.

Secure Update Mechanisms: The update firm to prevent remote attacks needs to be transmitted via proper end-to-end encryption to prevent any data tampering. Plus a fail-safe mechanism needs to present like rolling back to the previous version for when an update fails.

Network Enhancement: Proper usage of firewalls, Intrusion Detection Systems and VPN’s needs to be adhered to. Firewalls to make sure that any unauthorised over the air request is detected early and blocked. IDS also to see that the anomalous traffic is not entering the network.

Network Isolation: One can also segregate and isolate the critical devices like a router, or the cameras we saw above, and put them in a separate VLAN network, to ensure that there is limited access to it.

Secure Programming Practices: With the memory corruption attack, we saw the vulnerability and it turned out to be a command injection parameter issue, which can be avoided with proper input validation and making sure to avoid unsafe functions.

With these practices, one can be sure about an enhanced security being implemented.

NIST Guidelines

The National Institute of Standards and Technology (NIST) provides with guidelines and standards for enhancing cyber security and ensuring that the rules are adhered to. All of these are kept in mind and with a goal which is to simply make the system more resilient. Ranging from various domains like development to data protection, they have it all covered. For a DDOS attack security, NIST SP 800-61 Rev.2: Computer Security Incident Handling Guide provides guidelines on how to respond to DDOS attacks and NIST SP 800-44 Rev. 2: Guidelines to securing public web servers covers techniques which help preventing DDOS attacks which target web servers including rate limiting and firewalls. Remote over-the-air attacks includes following guidelines like NIST SP 800-57 Part 1 Rev. 5: Recommendation for key management, which provides OTA updating mechanisms and guidance on cryptography management. Also NIST SP 800-63-3: Digital Identity Guidelines which addresses secure authentication practices, crucial for OTA update and access control. Memory Corruption Attacks, one guideline NIST SP 800-218: Secure Software Development Framework Version 1.1 provides with really secure coding guidelines to prevent vulnerabilities like buffer overflow and memory corruption. All these guidelines should be followed by the companies and organizations at hand.

1. USER PERSPECTIVE

For the user who must implement the security devices and the functionalities, there might be scenarios where they will look for cheaper alternatives. Some might think that using a stronger password will be a better option over installing WPA3 security or priority of security usage might only be given to few devices instead of all. All these points can be a bit challenging for the user to decide which can lead to compromising on security.

1. CONCLUSIONS

Setting up a home area network comes from its own sets of benefits and challenges. Initial stages of the research included creating the network, understanding what the setup will be, learning about different network types. That led to understanding the devices that will be part of the network, which took a lot of research. Knowing which device to use, the vulnerability a device might have, what goes with the network. Most of the devices are of recent times and certain devices are with vulnerabilities that have been reported as an issue or a possible issue, with a few having fixes already present.

With this home network, which is realistic as well as limited with devices listing, as I believe there can be more devices present in a home which can help curate a smart home. If I had more time, I would have taken time to research more on the attack vectors and try to include multiple devices with vulnerabilities present to display how a complete take over can compromise the whole network.

REFERENCES

1. D. Darah, “7 types of networks and their use cases,” *TechTarget*, Apr. 18, 2022. <https://www.techtarget.com/searchnetworking/feature/7-types-of-networks-and-their-use-cases>
2. “Types of Computer Networks,” *GeeksforGeeks*, May 01, 2021. <https://www.geeksforgeeks.org/types-of-computer-networks/>
3. J. Arshad, A. Ur Rehman, S. G. Niazi, D. Kalra and W. Mansoor, "A Review on Security Attacks and countermeasure in Home Area Network (HAN)," 2022 International Conference on Cyber Resilience (ICCR), Dubai, United Arab Emirates, 2022, pp. 1-6, doi: 10.1109/ICCR56254.2022.9995810.
4. “AX1800 Dual-Band Wi-Fi 6 Router,” [*www.tp-link.com*](http://www.tp-link.com). <https://www.tp-link.com/us/home-networking/wifi-router/archer-ax21/>
5. NETGEAR, “CM3000 Mid/High-Split Cable Modem 2.5Gbps DOCSIS 3.1 | NETGEAR,” *NETGEAR*, 2024. <https://www.netgear.com/home/wifi/modems/cm3000/> (accessed Dec. 22, 2024).
6. NETGEAR, “Gigabit with 10-Gigabit/Multi-Gigabit,” *NETGEAR*, 2024. <https://www.netgear.com/business/wired/switches/unmanaged/gs110mx/> (accessed Dec. 22, 2024).
7. “BE11000 Tri-Band Wi-Fi 7 Range Extender,” *Tp-link.com*, 2024. <https://www.tp-link.com/us/home-networking/range-extender/re655be/> (accessed Dec. 22, 2024).
8. S. Inc, “DiskStation DS224+ | Synology Inc.,” [*www.synology.com*](http://www.synology.com). <https://www.synology.com/en-us/products/DS224+>
9. “front Black Titanium,” *Samsung India*, Apr. 20, 2023. <https://www.samsung.com/in/tvs/oled-tv/s90c-55-inch-qa55s90caklxl/?srsltid=AfmBOoqbAj1_aUaZufu3vDhGSZYT6qSXShb2E8Tc_12-FbhlePTlgvXy> (accessed Dec. 22, 2024).
10. “Fire TV Cube | Hands-free streaming device with Alexa | 4K Ultra HD : Amazon.in: Home & Kitchen,” *Amazon.in*, 2024. <https://www.amazon.in/Fire-TV-Cube/dp/B083VWSQJC> (accessed Dec. 22, 2024).
11. “Amazon.in,” *Amazon.in*, 2015. <https://www.amazon.in/Echo-Spot-Stylish-screen-Black/dp/B01J6A7FGQ> (accessed Dec. 22, 2024).
12. “Smart Security,” *Philips Hue*. <https://www.philips-hue.com/en-us/products/smart-security>
13. “Video Doorbell (2nd Gen),” *Ring.com*, 2020. <https://ring.com/gb/en/support/products/doorbells/video-doorbell-gen-2?page=1&srsltid=AfmBOoqsL6UTRJ6dH90GXo43wtSgt3os8aL1Axcp2lj9PYZza5OwF5jr> (accessed Dec. 22, 2024).
14. “Wemo Smart Home | Belkin IN,” *Belkin IN*, 2024. <https://www.belkin.com/in/products/wemo-smart-home/> (accessed Dec. 22, 2024).
15. French, “\*\*Bespoke 4-Door French Door Refrigerator (29 cu. ft.) with Beverage CenterTM in Stainless Steel\*\*,” *Samsung Electronics America*, 2021. <https://www.samsung.com/us/home-appliances/refrigerators/bespoke/bespoke-4-door-french-door-refrigerator-29-cu-ft-with-beverage-center-in-stainless-steel-rf29bb8600qlaa/>
16. “GE Smart Ranges & Ovens | GE Appliances,” [*www.geappliances.com*](http://www.geappliances.com). <https://www.geappliances.com/ge/connected-appliances/ranges-ovens-cooking.htm>
17. Place, “LG QuadWashTM Dishwasher, 14 Place Settings, EasyRackTM Plus, Inverter Direct Drive, Platinum Silver color | LG Levant,” *LG Levant*, 2024. <https://www.lg.com/levant_en/dishwashers/lg-dfc612fv> (accessed Dec. 22, 2024).
18. “the Barista TouchTM,” *Breville*, 2022. <https://www.breville.com/en-us/product/bes880> (accessed Dec. 22, 2024).
19. “Sonos App and Web App Controller - Sonos,” *Sonos*, 2024. <https://www.sonos.com/en-in/controller-app> (accessed Dec. 22, 2024).
20. “Google Nest Audio + Wyze Bundles,” *Wyze Labs, Inc.*, 2024. <https://www.wyze.com/products/google-nest-audio-smart-speaker?srsltid=AfmBOor49widbYE3swAUCLXQoGB2AHqAYEaY38TBa8OkyDVcF_HzO4q1> (accessed Dec. 22, 2024).
21. Petter Ahrnstedt and J. Lee, “Thousands of hacked TP-Link routers being used to hijack Azure accounts,” *PCWorld*, Nov. 04, 2024. <https://www.pcworld.com/article/2509553/thousands-of-hacked-tp-link-routers-being-used-to-hijack-azure-accounts.html> (accessed Dec. 22, 2024).
22. D. Goodin, “Thousands of hacked TP-Link routers used in years-long account takeover attacks,” *Ars Technica*, Nov. 02, 2024. <https://arstechnica.com/information-technology/2024/11/microsoft-warns-of-8000-strong-botnet-used-in-password-spraying-attacks/>
23. “Multiple botnets exploiting one-year-old TP-Link flaw to hack routers,” *BleepingComputer*. <https://www.bleepingcomputer.com/news/security/multiple-botnets-exploiting-one-year-old-tp-link-flaw-to-hack-routers/>
24. Petter Ahrnstedt and J. Lee, “Thousands of hacked TP-Link routers being used to hijack Azure accounts,” *PCWorld*, Nov. 04, 2024. <https://www.pcworld.com/article/2509553/thousands-of-hacked-tp-link-routers-being-used-to-hijack-azure-accounts.html>
25. “NVD - CVE-2023-1389,” *Nist.gov*, 2023. <https://nvd.nist.gov/vuln/detail/CVE-2023-1389>‌
26. E. Revell, “Wyze breach allowed 13,000 customers to peek into other’s homes,” *FOXBusiness*, Feb. 20, 2024. <https://www.foxbusiness.com/technology/wyze-breach-allowed-13000-customers-peek-into-others-homes>
27. S. Harding, “‘So violated’: Wyze cameras leak footage to strangers for 2nd time in 5 months,” *Ars Technica*, Feb. 19, 2024. <https://arstechnica.com/gadgets/2024/02/wyze-cameras-gave-13000-people-unauthorized-views-of-strangers-homes/>
28. “Bitdefender-PReport-Wyze-7745,” Bitdefender, May 2024. Available: <https://blogapp.bitdefender.com/labs/content/files/2024/05/Bitdefender-PReport-Wyze-7745.pdf>
29. “CVE - CVE-2024-6247,” *Mitre.org*, 2024. <https://cve.mitre.org/cgi-bin/cvename.cgi?name=2024-6247> (accessed Dec. 22, 2024).
30. “CVE - CVE-2024-6246,” *Mitre.org*, 2024. <https://cve.mitre.org/cgi-bin/cvename.cgi?name=2024-6246> (accessed Dec. 22, 2024).
31. “NVD - CVE-2024-6248,” *Nist.gov*, 2024. <https://nvd.nist.gov/vuln/detail/CVE-2024-6248> (accessed Dec. 22, 2024).
32. R. Herrera and A. Plaskett, “Listen Up: Sonos Over-The-Air Remote Kernel Exploitation and Covert Wiretap -BlackHat USA 2024 Whitepaper.” Accessed: Dec. 22, 2024. [Online]. Available: <https://www.nccgroup.com/media/uzbp3ttw/bhus24_sonos_whitepaper.pdf>‌
33. Xynik, “Vulnerability Allowed Eavesdropping via Sonos Smart Speakers – Xynik,” *Xynik.com*, Aug. 09, 2024. <https://xynik.com/index.php/2024/08/09/vulnerability-allowed-eavesdropping-via-sonos-smart-speakers/> (accessed Dec. 22, 2024).
34. “NVD - CVE-2024-20018,” *Nist.gov*, 2024. <https://nvd.nist.gov/vuln/detail/CVE-2024-20018> (accessed Dec. 22, 2024).
35. “NVD - CVE-2023-50809,” *Nist.gov*, 2023. <https://nvd.nist.gov/vuln/detail/CVE-2023-50809> (accessed Dec. 22, 2024).
36. “NVD - CVE-2023-50810,” *Nist.gov*, 2023. <https://nvd.nist.gov/vuln/detail/CVE-2023-50810> (accessed Dec. 22, 2024).‌
37. P. Cichonski, T. Millar, T. Grance, and K. Scarfone, “Computer security incident handling guide,” *Computer Security Incident Handling Guide*, vol. 2, no. 2, Aug. 2012, doi: <https://doi.org/10.6028/nist.sp.800-61r2>.
38. W. Servers, M. Tracy, W. Jansen, K. Scarfone, and T. Winograd, “Special Publication 800-44 Version 2 Guidelines on Securing Public,” Sep. 2007. Available: <https://nvlpubs.nist.gov/nistpubs/Legacy/SP/nistspecialpublication800-44ver2.pdf>
39. E. Barker, “Recommendation for key management”:, *NIST Special Publication 800-57 Part 1 Revision 5*, May 2020, doi: <https://doi.org/10.6028/nist.sp.800-57pt1r5>.
40. P. A. Grassi, M. E. Garcia, and J. L. Fenton, “Digital identity guidelines: revision 3,” *NIST Special Publication 800-63-3*, Jun. 2017, doi: <https://doi.org/10.6028/nist.sp.800-63-3>.
41. M. Souppaya, K. Scarfone, and D. Dodson, “Secure Software Development Framework (SSDF) Version 1.1: (Draft),” *NIST Special Publication 800-218*, vol. 1, no. 1, Feb. 2022, doi: <https://doi.org/10.6028/nist.sp.800-218>.