Internet of Things and Cybersecurity in A Smart Home

Kiran Vokkarne, Raji Sundararajan
School of Engineering Technology, Purdue University,
West Lafayette, IN-47907, United States

***Abstract*:- With the ability to connect to networks and send and receive data, Internet of Things (IoT) devices involve security risks and threats, for a given environment. This is even more of a concern in a Smart Home network, where there is a lack of a security IT team, unlike a corporate environment. While user interface and ease of use is at the front and center of a Smart Home experience enabling faster adoption of IoT devices, often security and privacy are an afterthought and do not usually keep pace with its growth. Therefore, a dangerous possibility exists where malicious actors could exploit vulnerable devices in a domestic home environment.**

In this study, various types of cyberthreats that affect IoT devices were examined. Since IoT devices are commonplace in today's homes, it becomes vitally important to detect intrusions and unauthorized accesses. There are also privacy issues at stake. The results and data gathered from various tools in this study is used to analyze its impact on detection of cybersecurity vulnerabilities and risks in a smart home environment. They also indicate that several vulnerabilities exist in most cases and the importance of how taking precautions can help alleviate those risks.

Keywords: IoT, Cybersecurity, Monitoring, Smart Home, Privacy, Regulation

INTRODUCTION

Internet of Things (IoT) refers to the extension of the current Internet to objects that are able to communicate, either directly or indirectly, with electronic devices that are themselves connected to the Internet [1]. IoT devices are getting to be more common in our society every day and growing rapidly at 18% annually to 14 billion devices globally [2]. Cybersecurity is of critical importance due to the threats posed by Cybercriminals, such as hackers and state sponsors/actors [3]. While the benefits of IoT devices have made people's lives more convenient, it has also given rise to the threat of Cyberattacks and risk to privacy and security and exposure of personal data to theft and compromise in a smart home.

A smart home is a residence that includes various automation services, based on Internet of IoT devices, which are equipped with sensors, cameras, and lighting [4]. These devices can be remotely controlled via smartphones or voice enabled devices. In a smart home network, IoT devices collect and process various data, related to motion, temperature, lighting control, and other factors and store more diverse and complex user data. Today's Smart Home consists of various IoT devices, such as video doorbells, smart thermostat, smart lights and plugs, Android and other connected devices, baby monitors, voice enabled speakers such as Alexa, Google Home etc. [4].

A typical smart home illustration shown in Figure 1, will be used for the purpose of this study that includes thermostat, smart lights, smart tv, voice enabled devices, etc.

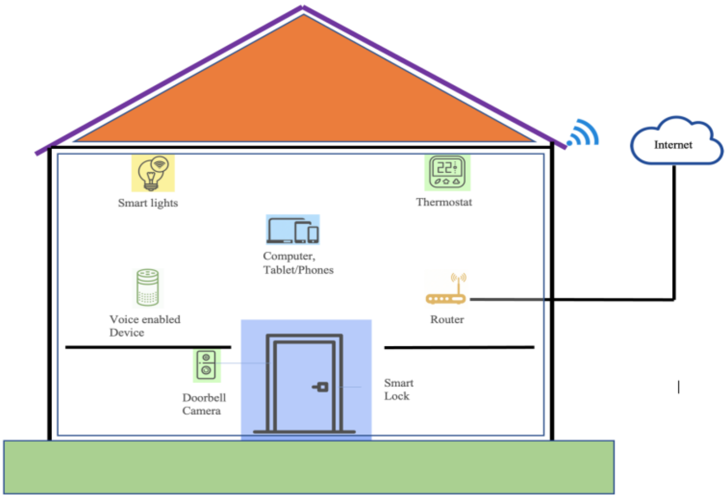


Figure 1: Smart Home Illustration

Canopus49, CC BY-SA 3.0 <https://creativecommons.org/licenses/by-sa/3.0>, via Wikimedia Commons

Existing risk assessment methods are not adequate for dynamic systems, such as IoT [5]. The risk assessment methods are not sufficiently designed for smart homes of today. This could lead to serious situations to personal security and property.

The nature of how an attacker gathers various types of intelligence about the users' devices and documentation and then uses that information to map the attack surfaces is explained in [6]. There are two types of attack surfaces, namely Hardware-based and Software-based.

The Hardware-based surfaces include embedded devices and hardware that include both internal and external components, which are prone to attack. The external attack vectors include areas, such as IO ports, power buttons, headphone jacks, camera, etc., which an attacker attaches onto a device to exploit internal device resources. Internal attack vectors include integrated circuits, circuit components, software, ICs and memory/ROM.

The software-based surfaces include the software, which controls the operation of an IoT device, including firmware, operating systems, and applications. Attackers target firmware, operating systems, and applications to gain access to command and control essential for attack objectives. Example: when a memory related buffer overflow occurs, an attacker can inject a unique code into the host program to take control.

One of the main aims of studying the attack surface is to understand the security threats faced by IoT devices. It helps to understand how an attacker targets the host (local and public network) and deploys the attack and what information is targeted. Table 1 shows the attack surface for the different types of networks [7].

Table 1: Attack Surfaces

Local Network Attack	Public Network Attack
Device to Device	User to IoT services
Device to controller	Service to service
Controller to gateway	Application to service
User to gateway	IoT device to service

IoT devices communicate via various network protocols, such as HTTP, Long range wide area network (LoRaWan), Bluetooth, and ZigBee and use various data protocols, such as MQTT, CoAP, AMQP, M2M, XMPP, etc. [8]. Since IoT devices communicate with various protocols, such as Low Energy Bluetooth, NFC, WIFI, LAN etc. they offer a large attack surface for an attacker to exploit vulnerabilities and intercept or manipulate data [5]. The IoT devices can face Cyberattacks at various levels, such as access control and authentication level or even at a network gateway level between local and public network [6].

Essentially, IoT devices contain sensors, actuators, or both. Sensors acquire data, and actuators control the data or act on the data [13].

- Sensors monitor IoTs and provide data about the 'Thing', such as temperature, light intensity, or battery level. Popular IoT sensor devices include home hub devices such as Amazon's Alexa Echo, Apple's HomeKit and Google Home as well as smartphones.
- Actuators control IoTs via hardware inside the device, such as controls in a Smart Thermostat, a dimmer switch in a smart bulb or the gear motors in a robot vacuum cleaner. The actuators represent the physical interface to the IoT that makes it "go" whether it be to turn on the heat, dim the lights, or send the robotic vacuum cleaner to the charging station. Popular IoT actuator devices include the Doorbell camera (Ring, Nest, etc.), Smart electric outlets and the Nest thermostat.

Eavesdropping is also a concern at the application layer due to IoT devices communicating with each other and to the cloud via the network. Due to insecure pairing, weak authentication, and poor protocol such as lack of suitable cryptography Bluetooth Low Energy(BLE) devices according to [9] are subject to eavesdropping, pin hacking, Man-In-The-Middle attacks. Security vulnerabilities causes personal data to be stolen, unlocking smart locks, misinterpretation of the messages exchanged, battery drain of IoT devices, etc

Certain other devices such as smart bulbs communicate with a hub using ZigBee protocol which is based on IEEE 802.15.4 standard.[10.] It's a low powered low-cost protocol that's popular for a lot of IoT devices. These devices communicate via the network and sometimes add a CORS header which includes 'Access-Control-Allow-Origin: *'. This along with weak authentication can cause external web server to intercept communication to create an information leakage possibility.

There are various ways a cyber hacker could gain unauthorized access of data or systems of users. There are various ways to classify the threats and vulnerabilities that IoT devices face, however, below are some typical ways an attacker can compromise IoT devices in a home environment.

1. **DDoS attacks** – Large number of request flood the IoT devices resulting in Denial of Service and the devices to go down. This results in downtime and potential financial losses to companies [11].
2. **Man-In-the-Middle** – These occurs when hackers breach the communication between two different systems and can secretly intercept and listen on data that's being transmitted. They can then send and receive data to both parties and can cause further damage based on the data received such as login credentials etc. Example an email that asks for login to bank account, however the man in middle will receive the login credentials after login instead of request going to the bank [12].
3. **Worm/Viruses** – Malware can be introduced into IoT devices when we download data and can then compromise the device and then further communicate with other neighboring devices in the IoT network [13].
4. **Botnets** – Web criminals frequently rent access to crime machines called 'botnets' to mask their true location online. Botnets allow hackers to bounce their Internet traffic through a myriad of infected systems that are usually untraceable [14].
5. **Eavesdropping/Data Theft** – IoT devices such as Camera, audio devices, Microphones etc. can be intercepted and used to listen in on data being transmitted. results in privacy loss and concerns [15].
6. **Social Attacks/Phishing** – Cybercriminals try to access sensitive information from social engineering route or using phishing emails convincing people to give out their confidential information such as bank accounts, personal information, home address, SSN, Credit Card numbers, order history etc. [16].
7. **Ransomware** – Once a IoT device is compromised the information obtained could then be used for blackmail and get ransom for keeping it private. In other instances, the users data such as files, pictures, videos can be encrypted and only released after payment of ransom [14].

Cisco Cyber Defense Lab v4 [17] explores various scenarios and tools for scanning vulnerabilities and simulate attacks. The learnings from this lab include how once hackers have made their way into a host network, they can execute the following techniques to further compromise systems:

- **Port Scanning**: Scan all available ports to search for openings and compromise.
- **Pivoting**: Route traffic from a hacker's computer to the host network computers
- **Data Exfiltration**: Once worms and trojans are placed and systems are compromised, then data is exfiltrated onto the hacker's computer from the host computer.

Explored in this study were various tools that could be used to examine the threats and vulnerabilities that exist in a Smart Home network. An existing Smart Home environment was tested against currently existing Cyberthreats by running various forensic tools and the data obtained was interpreted, based on various parameters to check the overall health of the devices and home network. The results provide various mechanisms that one could use to verify and implement to realize a safe smart home environment and help protect from cyber-attacks.

METHODS:

Tools Used

Cisco StealthWatch Management Console (SMC)

Cisco provides tools for comprehensive monitoring of various devices [18]. The Stealthwatch Management Console (SMC) [18] dashboard typically shows a list of network devices feeding NetFlow to the Stealthwatch Collector, and the Stealthwatch Sensor that turns raw traffic into NetFlow. Also, an additional list of devices can be viewed by clicking on the + button next to each section to expand the list. The various tools offered by Cisco for Cybersecurity detection and prevention are listed in Table 2:

Table 2: Cisco Tools

Cisco Tools
Cisco StealthWatch Management Console (SMC)
Cisco Email Security Appliance (ESA)
Cisco Identity Management Services
Cisco Tetration

Other tools included in the study are as follows:

1. **Nmap Scanner**, version 7.92 scans various ports and services on a computer network by sending packets and analyzing the results. This includes host discovery, port scanning, version detection, etc. [19].
2. **TcpDump**, version 4.99.1 command line-based network data analyzer. It reads the data being transmitted by the IoT device [20].
3. **Nessus Scanner,** version 10.2.0 for Mac is a Remote scanning tool that scans computers and raises alerts if it discovers vulnerabilities [21].
4. **Shodan** search engine for Internet of Things (IoT) [22]. This tool is able to locate IoT devices exposed to the internet insecurely.
5. **Wireshark**, version 3.6.6 Network protocol analyzer used to monitor network traffic that is flowing and analyze any abnormalities [23].
6. **Charles Proxy**, version 4.6.2. HTTP Proxy/Monitor tool that enables developer to view all HTTP/SSL/HTTPS traffic between machine and Internet [24].

Most of the tools selected are industry standard and opensource in nature and can be generalized to most other environments where similar results are used for decision making.

In computers a port is connection between peripherals and serves as an interface between which data is shared. Port scanning is a means of checking which ports are open on a given network and how they receive or send data. It is also a process which sends packets to specific ports on a host and analyze responses to identify vulnerabilities [26].

RESULTS AND DISCUSSION

Nmap is a popular scanning tool [19]. It was run on a local computer router with -T4 -a -v options. The results indicate that Port 80, 443 and 53 are open, which are per expectation. Port 80 is the default HTTP port for data communications which is widely used and universally. Port 443 is the secure port which is used for passing encrypted data. DNS uses port 53 which is generally open on firewalls and routers to transmit DNS queries.

Nothing out of ordinary was observed from the Nmap scan results.

```
Kirans-MBP:~ kiranvokkarne$ nmap -T4 -A -v 192.168.1.2
Starting Nmap 7.92 ( https://nmap.org ) at 2022-07-27 17:11 PDT
NSE: Loaded 155 scripts for scanning.
NSE: Script Pre-scanning.
Initiating NSE at 17:11
Completed NSE at 17:11, 0.00s elapsed
Initiating NSE at 17:11
Completed NSE at 17:11, 0.00s elapsed
Initiating NSE at 17:11
Completed NSE at 17:11, 0.00s elapsed
Initiating Ping Scan at 17:11
Scanning 192.168.1.2 [2 ports]
Completed Ping Scan at 17:11, 0.00s elapsed (1 total hosts)
Initiating Parallel DNS resolution of 1 host. at 17:11
Completed Parallel DNS resolution of 1 host. at 17:11, 0.01s elapsed
Initiating Connect Scan at 17:11
Scanning Kirans-MBP.lan (192.168.1.2) [1000 ports]
Completed Connect Scan at 17:11, 0.04s elapsed (1000 total ports)
Initiating Service scan at 17:11
NSE: Script scanning 192.168.1.2.
Initiating NSE at 17:11
Completed NSE at 17:11, 0.00s elapsed
Initiating NSE at 17:11
Completed NSE at 17:11, 0.00s elapsed
Initiating NSE at 17:11
Completed NSE at 17:11, 0.00s elapsed
Nmap scan report for Kirans-MBP.lan (192.168.1.2)
Host is up (0.000084s latency).
All 1000 scanned ports on Kirans-MBP.lan (192.168.1.2) are in ignored states.
```

```
Not shown: 1000 closed tcp ports (conn-refused)
NSE: Script Post-scanning.
Initiating NSE at 17:11
Completed NSE at 17:11, 0.00s elapsed
Initiating NSE at 17:11
Completed NSE at 17:11, 0.00s elapsed
Initiating NSE at 17:11
Completed NSE at 17:11, 0.00s elapsed
Read data files from: /usr/local/bin/../share/nmap
Service detection performed. Please report any incorrect results at https://nmap.org/submit/ .
Nmap done: 1 IP address (1 host up) scanned in 0.82 seconds
```

Nmap advanced flags -sp was also used to scan on those ports. A netstat of the local network was also executed on a local MacBook and the results discussed in section titled Results & Discussions.

```
Kirans-MBP:nmap kiranvokkarne$ netstat -ap TCP
Active Internet connections (including servers)
Proto Recv-Q Send-Q  Local Address          Foreign Address        (state)
tcp4       0      0  kirans-mbp.lan.58432   192.168.1.229.8009     SYN_SENT
tcp4       0      0  kirans-mbp.lan.58431   52.109.0.24.https      ESTABLISHED
tcp4       0      0  kirans-mbp.lan.58427   151.101.129.69.https   ESTABLISHED
tcp6       0      0  2603-8000-753f-e.58426 lax31s19-in-x01..https ESTABLISHED
tcp4       0      0  kirans-mbp.lan.58425   151.101.193.69.https   ESTABLISHED
tcp4       0      0  kirans-mbp.lan.58424   stackoverflow.co.https ESTABLISHED
tcp4       0    110  kirans-mbp.lan.58423   192.168.1.229.8009     FIN_WAIT_1
tcp4       0      0  kirans-mbp.lan.58422   146.75.92.193.https    ESTABLISHED
tcp4       0      0  kirans-mbp.lan.58420   151.101.1.69.https     ESTABLISHED
tcp6       0      0  2603-8000-753f-e.58379 lax17s02-in-x04..https ESTABLISHED
tcp4       0      0  kirans-mbp.lan.58356   49.246.178.107.b.https ESTABLISHED
```

A **TcpDump** [20] tool is a data network and packet analyzer program that runs on a command line interface. A TcpDump [20] tool was next used to check the data being transmitted with a local scan:

```
bash-3.2# tcpdump host 192.168.1.2
tcpdump: data link type PKTAP
tcpdump: verbose output suppressed, use -v or -vv for full protocol decode
listening on pktap, link-type PKTAP (Apple DLT_PKTAP), capture size 262144 bytes
10:22:43.289311 IP ec2-50-16-7-188.compute-1.amazonaws.com.https > kirans-mbp.lan.51122: Flags [.], ack
4123527583, win 14, options [nop,nop,TS val 2494669361 ecr 1337857706], length 0
10:22:43.289372 IP kirans-mbp.lan.51122 > ec2-50-16-7-188.compute-1.amazonaws.com.https: Flags [.], ack 1, win
2048, options [nop,nop,TS val 1337878107 ecr 2491696798], length 0
….
10:22:44.136322 IP google-home-mini.lan.32149 > kirans-mbp.lan.50595: Flags [P.], seq 1:111, ack 110, win 277, options
[nop,nop,TS val 2010715 ecr 716626740], length 110
…
19 packets captured
34 packets received by filter
0 packets dropped by kernel
```

The local MacBook scan revealed some Google Home traffic, therefore advanced search was performed -A and -AA flags

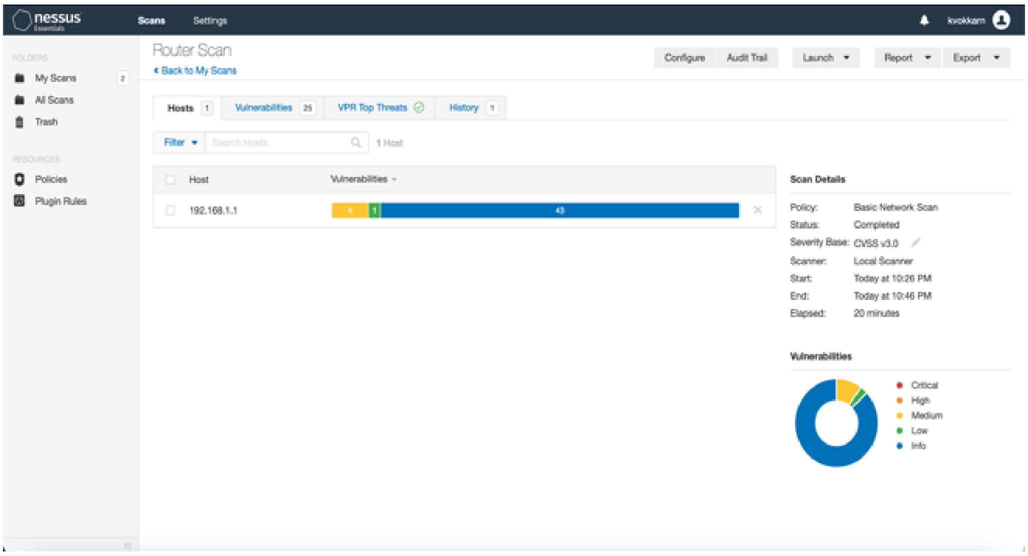
Next, the Internet Router at home was also scanned

```
bash-3.2# tcpdump host 192.168.1.1 -A
tcpdump: data link type PKTAP
tcpdump: verbose output suppressed, use -v or -vv for full protocol decode
listening on pktap, link-type PKTAP (Apple DLT_PKTAP), capture size 262144 bytes
10:31:00.756303 ARP, Request who-has 192.168.1.179 tell sac2v1k.lan, length 28
.......[;H}@...........[;H}@..............
10:31:01.780254 ARP, Request who-has 192.168.1.179 tell sac2v1k.lan, length 28
```

```
.......[;H}@...........[;H}@..............
10:31:02.599650 ARP, Request who-has 192.168.1.179 tell sac2v1k.lan, length 28
.......[;H}@...........[;H}@..............
10:31:03.828457 ARP, Request who-has 192.168.1.179 tell sac2v1k.lan, length 28
.......[;H}@...........[;H}@..............
```

A **Nessus** [21] scan tool which is used to find vulnerabilities and developed by Tenable was used to perform a scan as shown on Figure 2 on the Internet router to detect any threats and vulnerabilities.

As seen in Figure 2 the vulnerabilities on the router scan are identified as shown with color coding as high, medium, low and info. The various vulnerabilities that were flagged and will be discussed and handled in the results section.



Host	Vulnerabilities
192.168.1.1	4 1 43

Scan Details

Policy: Basic Network Scan
Status: Completed
Severity Base: CVSS v3.0
Scanner: Local Scanner
Start: Today at 10:26 PM
End: Today at 10:46 PM
Elapsed: 20 minutes

Vulnerabilities

Figure 2: Nessus scan profile [15]

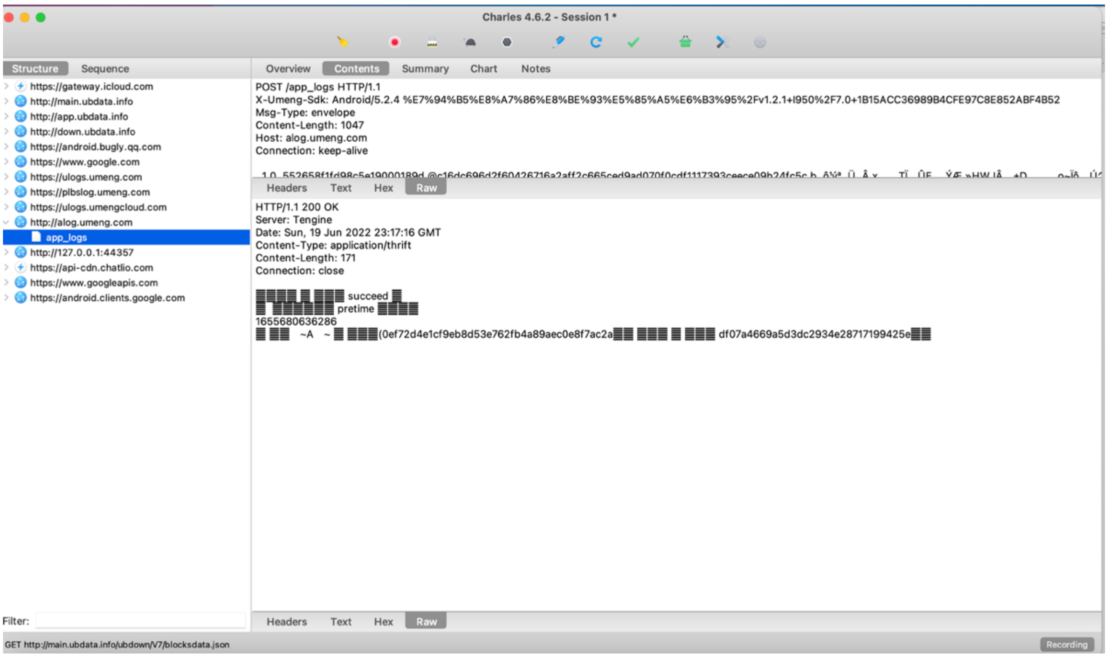
Likewise, **Shodan** [22] is another web-based tool that’s used to identify exposed IoT devices on the internet. Devices can be searched by location or other filter parameters such as below:

-https port:443 – This query will bring up a list of servers running port 443.
-netcam – This query would bring up a list of netcam devices.
-title: “OutlookWeb Access" port:443,80 – This query will provide a list of sites hosting Microsoft OWA.
-webcamxp country:SE: This search would bring up a list of webcams in Sweden.

Masscan [25] is another fast port scanning tool and has a GUI interface for scanning like Nmap. Port 80-8000 were scanned.

The next step was to run a **Wireshark** [23] an open-source packet analyzer to scan the network to get a comprehensive look of the data being transmitted between the various devices in the network with a EAPOL packet scan. A DNS/HTTPS scan was also performed.

Finally, an Android TV box was setup in the home network with **Charles Proxy** [24] a cross platform proxy debugging tool to monitor the traffic between the Android TV box and router to look for any suspicious activity in the proxy traffic. Figure 3 below shows scan results of various HTTP endpoints the Android TV box is hitting on the Internet, assessment of scan will be discussed in the results section.



```
https://gateway.icloud.com
http://main.ubdata.info
http://app.ubdata.info
http://down.ubdata.info
https://android.bugly.qq.com
https://www.google.com
https://ulogs.umeng.com
https://plbslog.umeng.com
https://ulogs.umengcloud.com
http://alog.umeng.com
    app_logs
http://127.0.0.1:44357
https://api-cdn.chatlio.com
https://www.googleapis.com
https://android.clients.google.com
```

```
POST /app_logs HTTP/1.1
X-Umeng-Sdk: Android/5.2.4 %E7%94%B5%E8%A7%86%E8%BE%93%E5%85%A5%E6%B3%95%2Fv1.2.1+l950%2F7.0+1B15ACC36989B4CFE97C8E852ABF4B52
Msg-Type: envelope
Content-Length: 1047
Host: alog.umeng.com
Connection: keep-alive

 1.0  552658f1fd98c5e19000189d @c16dc696d2f60426716a2aff2c665ced9ad070f0cdf1117393ceece09b24fc5c b
```

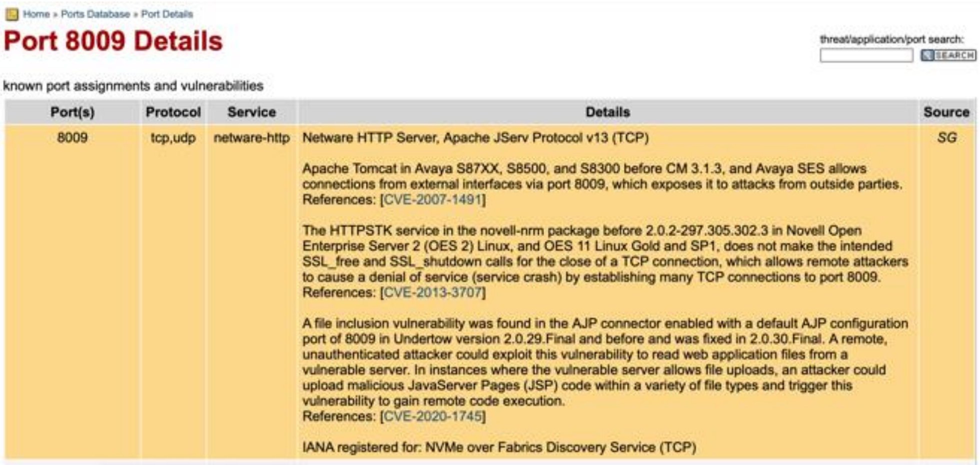
```
HTTP/1.1 200 OK
Server: Tengine
Date: Sun, 19 Jun 2022 23:17:16 GMT
Content-Type: application/thrift
Content-Length: 171
Connection: close

████ █ ███ succeed █
█ ██████ pretime ████
1655680636286
█ ██  ~A  ~ █ ███(0ef72d4e1cf9eb8d53e762fb4a89aec0e8f7ac2a██ ███ █ ███ df07a4669a5d3dc2934e28717199425e██
```

```
GET http://main.ubdata.info/ubdown/V7/blocksdata.json
```

Figure 3: Charles Proxy Scan [24]

Netstat results in Figure 4 indicate that ‘netware-http services’ was using port 8009. Upon further investigation it appears according to speedguide.net “a file inclusion vulnerability was found in the AJP connector enabled with a default AJP configuration port of 8009 in ---


Home » Ports Database » Port Details
threat/application/port search:
SEARCH

Port 8009 Details

known port assignments and vulnerabilities

Port(s)	Protocol	Service	Details	Source
8009	tcp,udp	netware-http	Netware HTTP Server, Apache JServ Protocol v13 (TCP) Apache Tomcat in Avaya S87XX, S8500, and S8300 before CM 3.1.3, and Avaya SES allows connections from external interfaces via port 8009, which exposes it to attacks from outside parties. References: [CVE-2007-1491] The HTTPSTK service in the novell-nrm package before 2.0.2-297.305.302.3 in Novell Open Enterprise Server 2 (OES 2) Linux, and OES 11 Linux Gold and SP1, does not make the intended SSL_free and SSL_shutdown calls for the close of a TCP connection, which allows remote attackers to cause a denial of service (service crash) by establishing many TCP connections to port 8009. References: [CVE-2013-3707] A file inclusion vulnerability was found in the AJP connector enabled with a default AJP configuration port of 8009 in Undertow version 2.0.29.Final and before and was fixed in 2.0.30.Final. A remote, unauthenticated attacker could exploit this vulnerability to read web application files from a vulnerable server. In instances where the vulnerable server allows file uploads, an attacker could upload malicious JavaServer Pages (JSP) code within a variety of file types and trigger this vulnerability to gain remote code execution. References: [CVE-2020-1745] IANA registered for: NVMe over Fabrics Discovery Service (TCP)	SG

Figure 4: Netstat results report

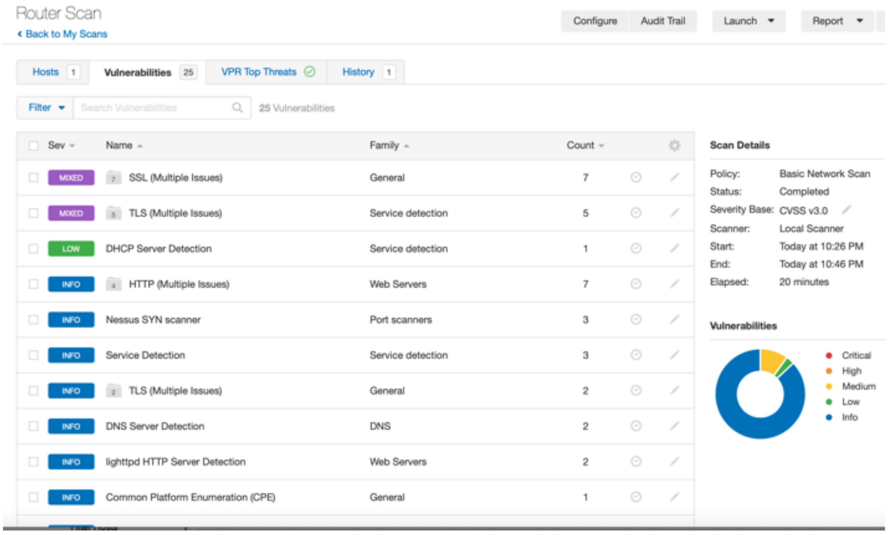
TcpDump [20] tool revealed that the router is constantly talking to 192.168.1.179, so a check was performed to find whom the IP address belonged to:

```
Nmap scan report for 192.168.1.179
Host is up (0.0058s latency).
All 1000 scanned ports on 192.168.1.179 are in ignored states.
Not shown: 1000 closed tcp ports (reset)
MAC Address: 00:26:EC:02:F8:00 (Legrand Home Systems)

Nmap done: 1 IP address (1 host up) scanned in 0.44 seconds
```

This revealed that 192.168.1.179 belongs to the Legrand Smart Home Hub. This is the hub that’s used to setup Smart Lights and Smart Switches in the home. It was also observed that the data packets being sent were some sort of pings which seemed normal. The Smart hub seems to be constantly sending keep alive heartbeats to the devices that are connected to it. The TcpDump also detected traffic coming from Google Home devices, however this was also deemed normal traffic.

Nessus [22] scan from Figure 5a and Figure 5b indicates multiple vulnerabilities that were identified as part of scan:

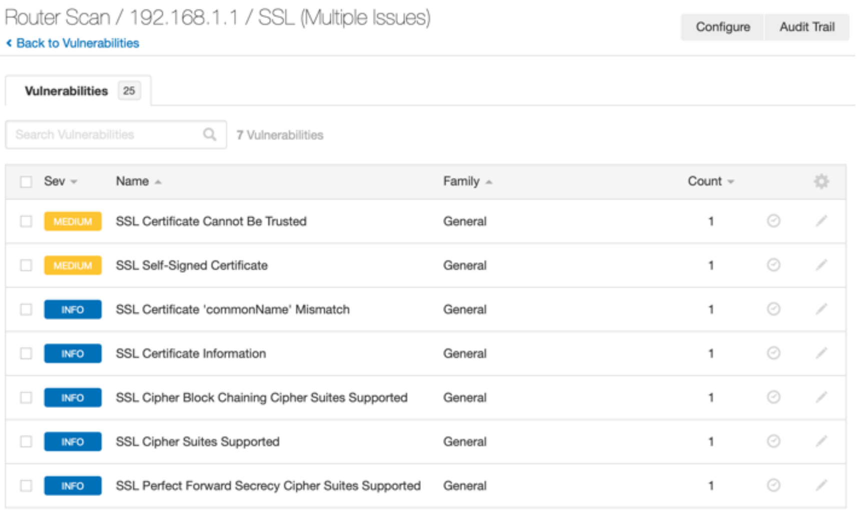


Sev	Name	Family	Count
MIXED	SSL (Multiple Issues)	General	7
MIXED	TLS (Multiple Issues)	Service detection	5
LOW	DHCP Server Detection	Service detection	1
INFO	HTTP (Multiple Issues)	Web Servers	7
INFO	Nessus SYN scanner	Port scanners	3
INFO	Service Detection	Service detection	3
INFO	TLS (Multiple Issues)	General	2
INFO	DNS Server Detection	DNS	2
INFO	lighttpd HTTP Server Detection	Web Servers	2
INFO	Common Platform Enumeration (CPE)	General	1

Scan Details

Policy:	Basic Network Scan
Status:	Completed
Severity Base:	CVSS v3.0
Scanner:	Local Scanner
Start:	Today at 10:26 PM
End:	Today at 10:46 PM
Elapsed:	20 minutes

Figure 5a: Nessus scan [22] results



Sev	Name	Family	Count
MEDIUM	SSL Certificate Cannot Be Trusted	General	1
MEDIUM	SSL Self-Signed Certificate	General	1
INFO	SSL Certificate 'commonName' Mismatch	General	1
INFO	SSL Certificate Information	General	1
INFO	SSL Cipher Block Chaining Cipher Suites Supported	General	1
INFO	SSL Cipher Suites Supported	General	1
INFO	SSL Perfect Forward Secrecy Cipher Suites Supported	General	1

Figure 5b: Nessus scan [22] results

The vulnerabilities identified were as follows:

- SSL Certification cannot be trusted – indicates certificate installation was not properly completed on the server or website.
- SSL Certificate is self-signed – users may see a warning message indicating data cannot be fully trusted
- TLS multiple issues detected – Can potentially have Poodle, Breach, Heartbleed, and other attack vulnerabilities
- DHCP server vulnerability detected – Can provide sensitive information about the network to outsiders

Each of these vulnerabilities were assessed to determine the nature of threats and any resolutions available to overcome the issues. The results flagged by the tool seem precise as pointed out by the scan and definitely can help bring down the threat level and aspire confidence that the smart home setup is fairly secure.

The Shodan scan showed vulnerabilities in the webcam and doorbell cam connected to the home and how it could be exploited. This was corrected with multi factor authentication and can further be improved by installing a VPN to block IoT devices from showing in the Shodan scan.

The Masscan and Wireshark results showed no vulnerabilities in the immediate network, but further devices may need to be scanned for comprehensive coverage.

The Charles Proxy logs did not indicate anything suspicious. The logs were analyzed for both HTTP and SSL traffic and main observation was that the box is connected with its corresponding CDN api-cdn.chatlio.com for getting video playlist manifest and video segments for playback. The other endpoints being accessed by the device are to just capture/write logs such as ulogs.umeng.com and ulogs.umegcloud.com.

The scientific hypotheses and tests in this study can be reproduced and testable and hold good for any given smart home environment.

The entire results are summarized in the scan matrix in Table 3.

Table 3: Tools Scanning Results Summary

Tool Used	Device	Traffic/ Vulnerabilities /Threats	Port Scanned/ Threats	Result
Nmap scan	MacBook, Internet Router	Port scanning no threats detected	1000+ ports scanned 80, 443, 53 port open	Safe no issues detected
Netstat scan	MacBook	File Inclusion Vulnerability	tcp/udp 8009 port	Vulnerability observed and port was closed
TcpDump scan	MacBook	Google Home Traffic	google-home-mini.lan.32149	No issues detected
TcpDump scan	Internet Router	Legrand Smart Home Hub	192.168.1.179 traffic detected	Normal Pings to router
Nessus scan	Internet Router	SSL Multiple Issues TLS Multiple Issues	SSL Certificate cannot be trusted/Self signed certificate, DHCP Server running	SSL and TLS vulnerabilities identified and resolved
Shodan scan	Netcam, Webcam	Webcam, doorbell camera	443(HTTPS), 80(HTTP), 554(RTSP), 22 (SSH)	Vulnerabilities identified
Massscan	Port scan router & MacBook	Port scanning no threats detected	80-8000	HTTP SSL
Wireshark monitoring	All Devices	EAPOL packets scan DNS/HTTP scan	SSL traffic HTTP traffic	No issues discovered
Charles Proxy Tool	Android TV Device	CDN traffic Application logs	HTTP/HTTPS traffic	Normal traffic and data observed

It's observed from the results summary in Table 3 that 'IoT Security' is heavily dependent on certain independent variables such as 'Number of Devices' since more the number of devices more are the chances of a cyber-attack and open ports available for that can be exploited. Also, the 'IoT Architecture' being used can play an important part as it will determine how efficient the devices are and to what extent they offer protection against snooping and intrusions.

A regression analysis model of the above results could be computed to study the various variables involved. In this scenario the dependent variable is 'IoT Security'. We know a given IoT security model depends on various factors (independent variables) that could influence its effectiveness, The below are some of the independent variables affecting our case:

- IoT Architecture
- Device Design
- Number of Devices
- Software Updates
- Device Monitoring

Given this, a model for multiple linear regression can be built

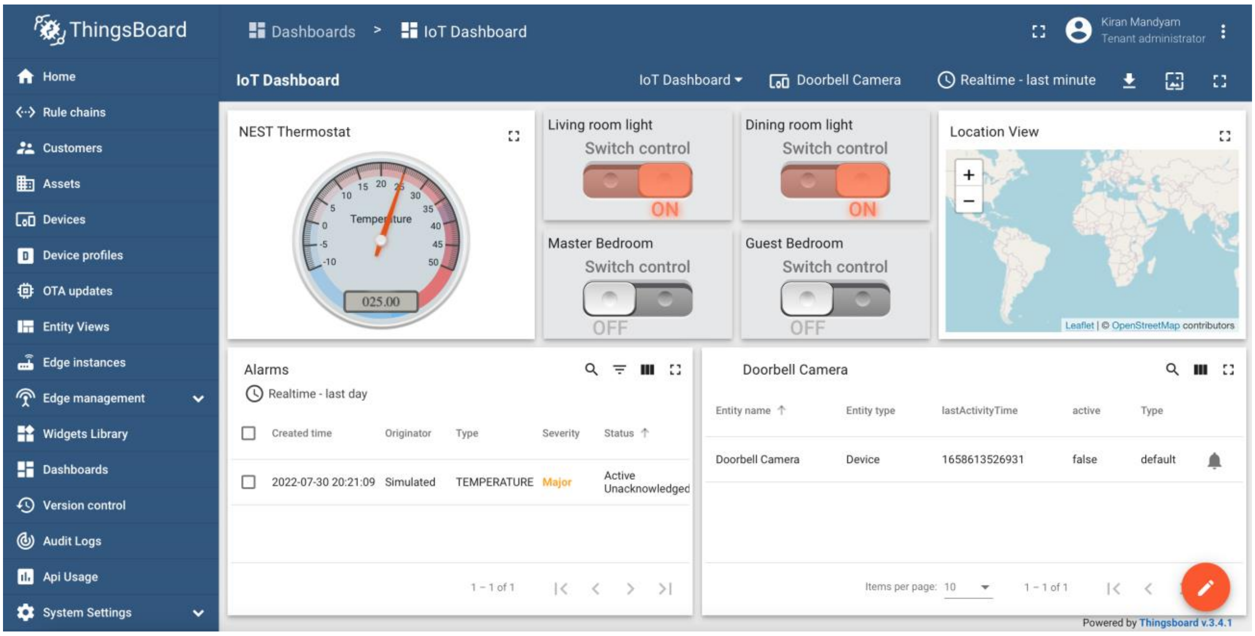
$$y = m1x1 + m2x2 + m3x3 + \dots\dots\dots + c$$

where: y is the dependent variable
x1, x2.. are the independent variables
m1, m2.. are the regression coefficients
and c is the y intercept

The ability of a strong IoT security lies in its basic architecture and how well the device is designed. There must be a security first design principal applied to each IoT device by manufactures. This will enable the devices to be more robust and reliable in withstanding intrusion attacks. Manufactures need to keep security in mind at the time of design phase itself and add features such as automatic software updates, reporting and monitoring, intrusion prevention and other features into the product upfront instead of security being an afterthought. These devices need to adhere to latest security standards and regulations so that provide the most effective protection to the consumers.

IOT DASHBOARD

As part of the study an IoT dashboard was created using ThingsBoard [27], an open source IoT platform. Fig. 6 shows the various IoT devices in the Smart home were included as widgets and monitoring enabled for analysis. These include thermostat, living room light control, dining room light control, and others.



Alarms

□	Created time	Originator	Type	Severity	Status ↑
□	2022-07-30 20:21:09	Simulated	TEMPERATURE	Major	Active Unacknowledged

Doorbell Camera

Entity name ↑	Entity type	lastActivityTime	active	Type
Doorbell Camera	Device	1658613526931	false	default

Figure 6: ThingsBoard IoT dashboard

The IoT dashboard serves both as a monitoring device for analysis of recorded content as well as live monitoring capabilities built in. Custom widgets are available to be added and configured which allows for telemetry data monitoring and visualization. Alarm was also setup of the temperature reading of the thermostat crosses a certain threshold. The doorbell camera activity was also monitored for any unusual activity or events. The dashboard also allows control and detailed monitoring of smart switches and voice enabled devices.

CONCLUSIONS

The objectivity of the results obtained, and the devices scanned show the various types of vulnerabilities that were discovered during the process of scanning and running the tools and interpreting the data. These tools collectively show the health of a home network and presence of any risks or threats. Overall, the health of the Smart Home network was observed to be fairly satisfactory and where threats or vulnerabilities were observed, they were corrected and fixed. Each typical device has characteristics of its own and hence anytime a new device is added to the network, its recommended to run a scan again.

Considerable research has been done on privacy, security, and other related topics with regard to IoT devices; however, there is still a lot to be done. This study sets the precedent in the right direction for further studies that could be done and lead to a secure environment in which an individual consumer could deploy more IoT devices into their home network. The problem is compounded due to the sheer volume of IoT devices and the abundance of newer devices emerging. Unless there are wide standardized design and compliance in place it’s hard to expect a certain standard of implementation from all the various vendors. Some may adhere to standards very closely while others may take it just as a guideline. Therefore, the future outlook seems to be quite cloudy with the onus on the users to protect themselves and here is where the various tools we used can play a part. The tools definitely give a perspective of where the user stands vis a vis their home network and smart home setup.

Limitations are generally weaknesses in the study or areas over which, one has no control over [28]. These include methods, constraints, length of a study, and responses. This project is limited to the IoT devices available as part of this study in the smart home environment. They are also dependent on the networking protocols that are supported by the available IoT devices and their vendors

REFERENCES:

[1] Nasreddine, B., & Saleh, I. (2017). *Internet of Things: Evolutions and Innovations*, ISTE Ltd. Web.

[2] IoT Analytics. (2022). State of IoT 2022, Retrieved on Jul 24, 2022, from https://iot-analytics.com/number-connected-iot-devices/

[3] Wang Xi., & Luo Ling. (2016). Research on IoT Privacy Security Risks. *International Conference on Industrial Informatics - Computing Technology, Intelligent Technology, Industrial Information Integration (ICIICII). IEEE*. pp 259–262. Doi: 10.1109/ICIICII.2016.0069

[4] Kim, S., Myungseo, P., Sehoon, L., & Jongsung, K. (2020). Smart Home Forensics - Data Analysis of IoT Devices, *Electronics (Basel)*, 9(8), pp 1215, doi: 10.3390/electronics9081215

[5] Lee, I. (2020). Internet of Things (IoT) Cybersecurity: Literature Review and IoT Cyber Risk Management. *Future Internet*, 12(9), pp 157-158. https://doi.org/10.3390/fi12090157

[6] England S. (2020). *Internet of things device cybersecurity and national security*. Utica College, MS Thesis, 62 pages; AAT 28094260

[7] James, F. (2019). IoT Cybersecurity based Smart Home Intrusion Prevention System, *3rd Cyber Security in Networking Conference (CSNet)*, pp 107-113, doi: 10.1109/CSNet47905.2019.9108938.

[8] Kelloton. (2022). Understanding the Potentials of IoT Protocols and Standards, Retrieved on Jul 26th, 2022, from https://www.kelltontech.com/kellton-tech-blog/internet-of-things-protocols-standards

[9] Barua, A., Al A., Md A., Hossain, Md., & Hossain, E. (2022). Security and Privacy Threats for Bluetooth Low Energy in IoT and Wearable Devices: A Comprehensive Survey. *IEEE open journal of the Communications* Society 3(1), pp 251–281, doi: 10.1109/OJCOMS.2022.3149732

[10] Dhanjani, N et al. (2015). *Abusing the Internet of Things : Blackouts, Freakouts, and Stakeouts.* O'Reilly

[11] CloudFare. (2022). Denial of service, Retrieved on Mar 31, 2022, from https://www.cloudflare.com/en-in/learning/ddos/glossary/denial-of-service/

[12] Veracode. (2022). Man in the Middle Attack. Retrieved on Aug 21, 2022, from https://www.veracode.com/security/man-middle-attack

[13] [13] IBM. (2022). Anatomy of a IoT malware attack. Retrieved on Aug 21, 2022, from https://developer.ibm.com/articles/iot-anatomy-iot-malware-attack/

[14] Kerbs, B. (2014). *Spam Nation*. SourceBooks, Inc.

[15] York, D. (2010). Eavesdropping and Modification. *ScienceDirect*, 3(1), pp 41-69, doi: https://doi.org/10.1016/B978-1-59749-547-9.00003-X

[16] Zafirkos, T. (2021). How Criminals Use Social Engineering to Access Sensitive Information. Retrieved on Aug 21, 2022, from https://www.networkcomputing.com/network-security/how-cybercriminals-use-social-engineering-access-sensitive-information

[17] cisco.com. (2022). Cisco Defense Clinic v4.3. Retrieved on Jul 26th, 2022, from https://dcloud-cms.cisco.com/demo_news/cyber-defense-clinic-v4-3

[18] cisco.com (2022). Cisco Secure Network Analytics Manager, Retrieved on Jul 26th, 2022, from https://www.cisco.com/c/en/us/support/security/stealthwatch-management-console/series.html

[19] nmap.org. (2022). Retrieved on Jul 26th, 2022, from https://nmap.org

[20] tcpdump.org. (2022). Retrieved on Jul 26th, 2022, from http://tcpdump.org

[21] Nessus scanner. (2022). Retrieved on Jul 26th, 2022, from http://tenable.com

[22] Shodan. (2022). Retrieved on Jul 26th, 2022, from http://shodan.io

[23] Wireshark. (2022). Retrieved on Jul 26th, 2022, from http://wireshark.org

[24] Charles Proxy. (2022). Retrieved on Jul 26th, 2022, from http://charlesproxy.com

[25] Masscan. (2022). Retrieved on Jul 26th, 2022, from https://github.com/robertdavidgraham/masscan

[26] avast.com. (2022). Retrieved on Jul 27th, 2022, from https://www.avast.com/en-us/business/resources/what-is-port-scanning#mac

[27] ThingsBoard. (2022). Retrieved on Jul 27th, 2022, from https://thingsboard.io

[28] Ross P., & Bibler Z. (2019). Limited by our limitations. *Perspect Medical Educ*. 8(4), pp 261-264. doi: 10.1007/s40037-019-00530-x