

|  |
| --- |
| **Unit 2 Summary Report**  *.*  **Myles Daniels 2104397**  CMP416: Advanced Digital Forensics  2024/25 |

*Note that Information contained in this document is for educational purposes.*

Contents

[1 Introduction 1](#_Toc184785952)

[1.1 Introduction 1](#_Toc184785953)

[1.2 Background 1](#_Toc184785954)

[1.3 Tasks to perform 2](#_Toc184785955)

[2 Procedure 3](#_Toc184785956)

[2.1 General procedure 3](#_Toc184785957)

[2.2 Data that would need to be collected and tools used 4](#_Toc184785958)

[3 Evaluation 5](#_Toc184785959)

[3.1 Evaluation of potential challenges 5](#_Toc184785960)

[3.2 Reflection on possible impediments 5](#_Toc184785961)

[3.3 Summary 5](#_Toc184785962)

[References 6](#_Toc184785963)

[Appendices 7](#_Toc184785964)

[Appendix 1 Home network diagram. source: MakeUseOf. (n.d.) *Home Network Setup Diagrams*. Available at: https://www.makeuseof.com/home-network-setup-diagrams/ (Accessed: 9 December 2024). 7](#_Toc184785965)

# Introduction

## Introduction

In the digital age the rapid rise of wireless networks have allowed our society to develop a number of different ways to enhance efficiency in our everyday lives from our shopping to our travels and even to the buildings we call homes. Many different companies and organizations have developed products and accompanying software to solve problems that up until a decade ago we didn’t think were issues such as being able to control your heating remotely in case of cold weather or back from a trip abroad one of the main pioneers of a device like this is the Centrica/British Gas owned hive. Such devices can even solve the reverse problem such as if you away from your home but worried about your homes security many devices can be bought which allow you to keep an eye on your front door and your house, pioneers by Amazons Ring, many companies now offer such products as well for affordable prices alongside many other products such as smart tv’s including chrome sticks/firesticks, lightbulbs which can be turned off/on and changed colour from the comfort of your phone and smart plug sockets which like light bulbs can also be turned off and on from mobile applications.

All of these devices however come with a huge danger much like most aspects of our interconnected world we take a lot of it for granted, malicious actors have been known to prey on these devices and not even the companies themselves are completely above board with amazon recently agreeing to pay $6.5 million to the US Federal Trade Commission over their employees spying on customers through their own ring cameras.[3] the scenario this report is based on is a cautionary tale in IOT security and should serve as a warning to those who install such systems in the future.

## Background

In this report we will be covering the multiple layers of the proposed investigation as part of an incident that has taken place in a smart city network, a smart city is defined as a: “a municipality that uses information and communication technologies (IOT) to increase operational efficiency, share information with the public and improve both the quality of government services and citizen welfare.”[1]. This particular city is made up of different local IOT (internet of things) which are defined as: “IoT devices are **nonstandard computing hardware** -- such as sensors, actuators or appliances -- that connect wirelessly to a network and can transmit data.” [2]

These interconnected networks that include devices such as smart thermometer, home security cameras, speakers and so forth all controlled centrally by a security team responsible for monitoring and controlling data access with all local areas being given their own individual links and basic security defences such as a firewall that is managed from the central location. Within this smart city a single house has experienced a catastrophic breach in security and the source needs to be identified so the breach can be sealed mitigation can be deploying in order to reduce or prevent the risk of such an incident reoccurring.

The incident in question is that a single home in which a smart home in the city has had problems with its own individual network in which a malicious intruder has gained access over a number of days to most if not all IOT devices within the local network, they began by manipulating connected speakers and escalated from there what makes this a serious breach though is that even after basic security measures were applied such as resetting passwords the intruder was still able to have control over the devices and expand further into the local network which escalated to the intruder taking control of cameras and speaking to the houses occupants and most serious of all taking control of the smart thermostat and increasing the temperature to 85\*C Fahrenheit. Which after all other devices being disconnected leaves us with the current situation.

## Tasks to perform

With us being brought up to speed on the current situation there are a number of problems that need to be addressed immediately the first being to identify the cause of the attack and subsequent breach, with the network currently being disconnected it will be a challenge however multiple techniques and tools do exist to extract such data, the next issue will be to identify the scale of the breach to see if it is just confined to this one network or if is just the symptom of a larger problem especially if local password changes were not enough to prevent it. Finally, mitigations need to be drawn up in order to minimise the risk of recurrence and hopefully prevent its reoccurring. This process can be seen in the flowchart below.

A diagram of a flowchart

Description automatically generated

# Procedure

## General procedure

To begin with an inventory would have to be made of all smart devices within the household how they are connected to the main network and possibly interview the occupant of the household in order to gather additional information related to the timeline of events especially for any information that may have been missed from the initial briefing such as if the occupant accessed any websites recently, received and opened any suspect emails or downloaded anything recently even if it was part of firmware update additionally a complete listen of all active and connected devices to check what the intruder had access to and maybe even a device that they used to gain access to the network but didn’t manipulate in an obvious way like the others. The next step would be to check both the configuration of all the devices on the network check whether the homeowner has tampered with the device in any way alongside confirming that all standard security measures in place especially if factory default device passwords are still in place.

The next step would be to looking to network traffic data throughout the local network and see if the intruder has attempted to try and get out of the local network or if the intruder got into the network via the central management system. The next part is to look at network data specifically all network traffic logs between the various devices in the local network and any probing attempts made towards the central control room, the ideal place to start would be the main personal router as this device would be the ideal target for any attacker as controlling the router would allow them access to the whole network as it manages all the different connections that allow the devices to communicate with the central control room or for the local homeowner to use an example setup is shown in appendix one. The way such data would be collected would be through collecting traffic logs from the router by a number of methods, in the offline state certain professional tools such as Splunk[4] or Logstash could be used to gather the logs generated also the central control rooms logs could also be accessed pertaining to the individual firewall for this household additionally there may be a chance that services such as Wireshark could have been used by the central control room as part of their monitoring process, if so these logs would be useful in gathering the necessary information which would be related to abnormal data such as suspicious connections or unknown ip addresses and any and all abnormal data transfers.

The next step would be individual log analysis which would entail collecting such data from all of the smart devices that exist within the network in particular the affected devices which are the home speakers, all security cameras and the thermostat in these logs we would need to look for any types of unauthorized access that includes random temperature changes for the thermostat, access attempts and connections to the microphones and speakers and any authorised data streams passed through the speakers especially as the occupant reported loud disturbing music being played through them Finally we would have to grab firewall and other monitoring logs from the central security monitoring station in order to map the intruders movements throughout the network itself and also deploy vulnerability scanning tools as well in order to uncover any unknown vulnerabilities that may exist within the network including those that the attacker may have used to gain access to the home network.

## Data that would need to be collected and tools used

Whilst this initial investigation process is a good start, we need to define in detail the data that would need to be collected and tools that may have to be used throughout all steps of the investigation including router, device and central control room logs. To begin with the first type of data that would be acquired would be from the router logs and would entail us gathering information about device connections including but not limited to MAC addresses, IP addresses and assignments and DNS requests among others also due to the fact that the administrator reset the password and the attacks continued we would need to look for any unauthorised changes such as SSID changes and any unscheduled firmware updates.

The next type of data that would need to be collected from the IOT device logs would be to uncover any commands executed on the devices especially in relation to the thermostat as its still set to the temperature the intruder set it to and assuming that attempts have been made to rectify the setting, the intruder must have permanently set meaning they would have an advanced level of access and control alongside logs from the other known infected devices such as the speakers and security cameras alongside this from any of the logs that are retrieved from the central control room we should look for user actions related to this household any alerts their monitoring systems may have brought up indicating the presence of malware on their network, if this is found we would need to collect samples of it if possible for analysis in order to determine its type and possible origin.

To collect these types of data we would need to assemble an arsenal of tools for the task ahead. To start off with we would need a number of network analysis tools in order to capture network traffic within the network even for a brief window to give a better understanding of what has transpired, in order to do this Wireshark would be needed, Wireshark is the main tool in most digital forensic arsenals due to its range of abilities and how easy it is to capture network data. We would also need to acquire any cache or meta data that would be stored on the IOT devices and in order to do this we would need a tool like Autopsy[5] which would allow the examination of the device file systems, stored data and cache in order to retrieve anything that may be useful, another tool use for general log gathering and analysis is Splunk alongside a vulnerability scanning tool such as Nessus which can provide a comprehensive report and scaling of any vulnerabilities found across the network and finally if any malware is found over the course of the investigation there are a number of malware analysis tools out there chief among them IDA pro which can be use to reverse engineer the code used which can give very telling information about its origin or creator.

# Evaluation

## Evaluation of potential challenges

Though there is a good set plan for both an investigation, the data that is required to be collected and tools that will be used there are always unknowns in any investigation. On of the major limitations to an investigation is the volatility of any data acquired as logs especially from the IOT devices such as the speakers, cameras and thermostat tend to be limited due to their size and memory available and a major part of this investigation relies on the Central control room having accurate network monitoring logs with those captured after the network was disconnected are next to useless however centralisation of all device logs across the entire smart city network. Another issue that may arise during the investigation is the issues surrounding the multiple different types of IOT smart devices that may exist within the households with each of them having different protocols and baseline security standards that may have been the cause of the network intrusion in the first place however this would be a low risk as we already know the current device inventory and hopefully all configurations are custom according to the needs of the occupant and the smart network.

However data gathering and data validity won’t be the only area where there may be obstacles during the course of this investigation actually tracking down the suspect would be another issue altogether mainly due to the fact that most attacks tend to hide their true identity for obvious reasons and achieve this through a number of means including vpns(virtual Private networks)[6], virtual machine platforms such as VM-workstation and other forms of proxies alongside regular encryption methods and with each layer added this can increase the chance of them not being traced back at all however there are some techniques to get around issues like this such as pattern recognition where continuous encrypted dataflows can be followed and once suspect links have been identified these flows can be correlated with metadata and hopefully identify the potential attacker. Finally physical access would be an issue especially with trying to extract data however as the smart network is managed centrally this would be no issue.

## Reflection on possible impediments by intruder

Whilst there may be technical challenges during the course of this investigation it is nothing compared to the ways the intruder may try to disrupt the investigation or cover their tracks as they exploited the network. A key way they do that is through Protocol misuse where they may exploit standard internet protocols that exist in the network in order to hide their activities within regular traffic so that when logs are pulled it is hard to distinguish between regular traffic and the intruders movements however certain tools such as Wireshark could be able to sort through this subterfuge, another way they may attempt to throw investigators off is by data fragmentation which can be used to mask malware payloads and commands and would make any attempt at a forensic reconstruction very difficult however through the same kind of tools such as Wireshark you could attempt to build the picture of the payloads and commands and hopefully work towards reconstructing them.

Another form of subterfuge and a more concerning one is Log tampering where if the intruder has a higher authentication level of control such as gaining administrator privileges they may be able to access all logs across a network with a view to either delete them to destroy any valuable evidence or modify them to mask their intrusion and allow them to remain in the network this issue is extremely important to our scenario as the attack continued even after it was initially detected which would indicate that the intruder has a greater level of privilege within the network that would allow them to evade basic security remedies finally we come to another way the intruder can and has attempted to disrupt our investigation by lateral movements i.e. jumping between devices in the household network as the attacker has jumped from device to device the scope of this investigation has widened to the point where there are concerns whether this intrusion is just limited to this network alone, however monitoring of traffic between devices alongside network segmentation would allow us to turn their own subterfuge against them.

## Summary

This proposed investigation has uncovered an alarming breech of security within this smart city network the scale of the devices affected in this network and the severity of the breech itself by which the intruder was able to circumvent initial security remedies suggest a deeper problem and this intruder having a deeper level of access into the system than previously briefed on whilst this scenario hasn’t presented us with any useable data it is safe to assume that the cause of this incident is due to a woeful breech in the Smart City IOT device and network security and I firmly believe that the attack isn’t just limited to this network alone mainly due to the attacker seemingly having a high level of privilege across this household network something which can only be gained from the central control room, therefore I would suggest that if this investigation was to take place it be a large scale resource intensive one covering the entire smart city network in order to locate the vulnerabilities the intruder has exploited to gain entry, any and all vulnerabilities that are rated CVSS critical or high and a complete review of all current technical security polices that exist in the smart city network.

# References

**For URLs, Blogs:**

**[1] Holland, M., 2024. *Smart city*. TechTarget. Available at:** [**https://www.techtarget.com/iotagenda/definition/smart-city**](https://www.techtarget.com/iotagenda/definition/smart-city) **(Accessed: 8 December 2024)**

**[2] TechTarget 2024, *What is an IoT device?*, IoT Agenda (Accessed: 8 December 2024),** [**https://www.techtarget.com/iotagenda/definition/IoT-device**](https://www.techtarget.com/iotagenda/definition/IoT-device)**.**

**[3]** **Malwarebytes 2024, *Ring agrees to pay $5.6 million after cameras were used to spy on customers*, (Accessed: 8 December 2024)** [**https://www.malwarebytes.com/blog/news/2024/04/ring-agrees-to-pay-5-6-million-after-cameras-were-used-to-spy-on-customers**](https://www.malwarebytes.com/blog/news/2024/04/ring-agrees-to-pay-5-6-million-after-cameras-were-used-to-spy-on-customers)**.**

**[4] Splunk. (n.d.) *What is Splunk & What Does It Do?* Available at:** [**https://www.splunk.com/en\_us/blog/learn/what-splunk-does.html**](https://www.splunk.com/en_us/blog/learn/what-splunk-does.html) **(Accessed: 8 December 2024).**

**[5] Autopsy. (n.d.) *Autopsy: Open Source Digital Forensics*. Available at:** [**https://www.autopsy.com/**](https://www.autopsy.com/) **(Accessed: 10 December 2024).**

**[6] NordVPN. (n.d.) *What is a VPN? Virtual Private Network Meaning*. Available at:** [**https://nordvpn.com/what-is-a-vpn/**](https://nordvpn.com/what-is-a-vpn/) **(Accessed: 11 December 2024).**

# Appendices

## Appendix 1 Home network diagram. source: MakeUseOf. (n.d.) *Home Network Setup Diagrams*. Available at: <https://www.makeuseof.com/home-network-setup-diagrams/> (Accessed: 9 December 2024).

