Abertay University

Advanced Digital Forensics Unit 2

Michael Awoyemi

CMP416 Advanced Digital Forensics

2024/25

Contents

1 INTRODUCTION

1.1 BACKGROUND

This report comprehensively explains the digital forensic investigation of a smart city network that has experienced unauthorised access. To address a network forensic incident effectively, gathering comprehensive information about several key aspects of the event is crucial. This includes determining exactly what occurred, pinpointing the timing of the incident, understanding the methods used by the perpetrator, identifying which devices were compromised, and detailing the actions taken in response to the breach. Answering these questions will not only resolve the immediate issue but will work towards identifying the individual or group responsible for the malicious activity.

The structure of the report is designed to thoroughly investigate these elements. The structure is shown in Figure 1. Identification, Preservation, Analysis, Documentation and finally Presentation of evidence. Following the well-known Digital Forensic Investigation Process, all the incidents will be identified and preserved accordingly using hash values to prevent accidental or voluntary tampering of evidence. After analysing the findings, the final steps of the investigation are documentation and presentation tailored to different audiences.

Each section of this report will delve into the specifics of the incident, providing a complete picture of the circumstances surrounding it. The forthcoming sections will elaborate on the significance of each component, outlining why these particular details are essential for a comprehensive analysis and for developing effective mitigation strategies moving forward. This structured approach will ensure that all necessary facets of the incident are covered and will enhance the understanding of the threat landscape.

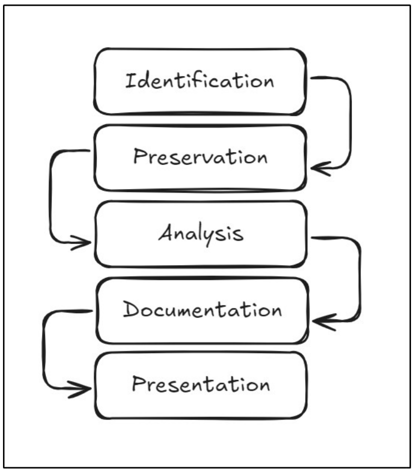

Figure 1

1.2 AIM

This report examines a security breach that occurred within a diverse smart city network. The findings will assist the company in addressing key questions including the nature of the incident, the timing and location of the breach, the methods used to exploit the network, and potential individuals or entities responsible for the event.

2 DATA ACQUISITION

The first step in this process involves identifying and cataloguing all connected devices within the premises and preserving them in their current state, either compromised or not. Each device will be thoroughly examined to gather critical information that may shed light on how the unauthorised access occurred. A copy of the information retrieved will be created to be worked on and prevent any form of tampering with the originals which can be verified using hash values.

This part of the investigation will focus on analysing all network ports and services associated with the devices. This includes assessing device configurations and identifying any vulnerabilities to evaluate the overall security effectiveness of the network infrastructure.

Additionally, external network communications will be monitored closely. This aspect is crucial, as attackers often use these channels to exfiltrate sensitive information or introduce malware into the network. By inspecting outgoing and incoming data flows, it can better understand the dynamics of the breach and establish any potential links to malicious activities.

2.1 ENUMERATION

To effectively contain a cyberattack, it is essential to first identify which Internet of Things (IoT) devices may have been compromised. This process begins with a comprehensive examination of all network devices using specialised scanning tools such as Nmap, along with other network analysis applications. These tools allow for a detailed scan of each device connected to the network. During the scanning process, various critical aspects are assessed, including the status of network ports and the services running on them. By evaluating the open ports, investigators can gain insights into potential vulnerabilities. For instance, if an uncommon port is discovered to be active, it raises immediate red flags, signalling that an unauthorised service may be operating.

In addition to monitoring port status, these scans also reveal the specific services and their versions running on each device. If a service is detected as outdated or should not be operating on a particular device such as a protocol typical of more robust systems appearing on a less capable IoT device this could indicate that the device has been compromised.

Through this meticulous scanning and analysis, security teams can pinpoint compromised devices, understand the nature of the threat, and implement appropriate containment strategies to mitigate further risks to the network and its connected devices.

2.2 LOGS

Logs play a crucial role in aiding forensic teams during investigations. They provide valuable insights from various sources such as router logs, Intrusion Detection System (IDS) logs, Intrusion Prevention System (IPS) logs, and firewall logs. By meticulously analysing this data using forensics timeline reconstruction tools, investigators can reconstruct events to understand what transpired during a security incident. These logs facilitate the examination of both internal and external communications, enabling the identification of specific IP addresses, accessed web pages, log-in attempts, email exchanges and downloaded files that may reveal how an attacker interacts with affected devices. Digital evidence is also inherently unstable; crucial information such as RAM contents, system logs, or temporary files can be lost if not preserved promptly.

For a more comprehensive analysis, tools like Wireshark can be employed to monitor current and past incoming and outgoing traffic across the network. This powerful network protocol analyser allows forensic experts to capture and visualise packet data, making it easier to detect anomalies in traffic patterns. Additionally, implementing an IDS such as Snort can enhance threat detection capabilities. Snort can be configured to process the packet capture (pcap) files retrieved from Wireshark, and custom rules can be developed to pinpoint irregular or malicious activity more swiftly.

Moreover, understanding the points of access exploited by an attacker can guide the examiner in creating a statistical flow analysis and the implementation of a honeypot.

2.3 STATISTICAL FLOW ANALYSIS

Statistical Flow Analysis is a pivotal technique in digital forensics, especially when Intrusion Detection Systems (IDS) or Intrusion Prevention Systems (IPS) are unavailable. It examines network traffic metadata such as IP addresses, port usage, and data volumes to identify compromised devices and malicious activities. By focusing on flow patterns rather than payloads, it remains lightweight, scalable, and effective, even in encrypted environments.

This method addresses critical forensic questions, including the “When” (timeline of attacks), “Who” (compromised hosts), and “How” (methods used). Indicators of compromise include unusual traffic volumes, non-standard port usage, and communication with known malicious systems. For example, a compromised host may exhibit abnormally high traffic during data exfiltration or connect to suspicious IPs linked to command-and-control (C2) servers. Statistical analysis can also detect time-based anomalies, such as activity outside working hours, and reveal data leakage by correlating large outbound traffic volumes with suspected breaches.

Visualisation tools like EtherApe enhance the process by graphically mapping traffic patterns. These tools highlight hotspots of abnormal activity, illustrate lateral movement within networks, and pinpoint devices exchanging large volumes of data. Such visual insights simplify anomaly detection and help trace attacker behaviours across a compromised network. Flow analysis also supports behavioural profiling, uncovering patterns such as periods of inactivity, entertainment usage, or internal data-sharing relationships. Cross-referencing flow data with threat intelligence enables investigators to confirm or refute findings and refine security measures.

2.4 HONEYPOTS

Once the presence of a malicious attacker has been confirmed, digital forensics inspectors can employ a sophisticated virtual database-type honeypot designed to mimic a treasure of sensitive or potentially harmful information. A honeypot serves as a decoy system designed to attract and study potential intruders, allowing security teams to gather intelligence on attack methods and strategies without putting critical systems at risk. This proactive approach not only helps in understanding threats but also strengthens overall network security. This honeypot might include fabricated data such as user passwords, accessible port information, proprietary secret recipes, or even fictitious user profiles. The primary purpose of a honeypot is to engage the attacker by capturing real-time data on their techniques and methodologies, thus providing valuable insights into their behaviours and strategies.

To achieve this, the honeypot must be engineered to be intriguing and appealing to the attacker. When they conduct their scans in search of privilege escalation, they should encounter this enticing environment, prompting them to explore and attempt to extract information from it. The design of the honeypot is crucial; it needs to simulate an authentic system, complete with various vulnerabilities that attackers typically target. Inside this honeypot, all data must be deliberately crafted to be non-sensitive and entirely fictitious. This precaution helps mitigate any potential risks, ensuring that even if an attacker accesses the honeypot, they will encounter only benign information that cannot cause real harm. Through the monitoring of interactions within the honeypot, forensics teams can analyse the tactics employed by the attackers and better understand their intentions, ultimately leading to improved security measures and strategies to defend against future intrusions.

2.5 BEHAVIOUR

The actions of attackers often reveal their core motivations, which can be financial, political, or ideological. For example, those driven by financial gain may create payment trails, like cryptocurrency transactions, that offer clues for investigators. On the other hand, hacktivists who target significant symbols might deliberately leave behind signatures or messages that correspond with their mission, providing essential insights into their tactics and goals. Grasping these psychological and behavioural aspects can assist investigators in predicting the attacker’s subsequent actions and discovering concealed evidence.

3 CRITICAL EVALUATION

Digital forensic investigations involve intricate processes that encounter numerous challenges throughout, from gathering evidence to analysis and reporting. These challenges arise due to various technical, procedural, and legal issues, which, if not properly addressed, can jeopardise the integrity of the investigation. Nonetheless, the use of innovative approaches, flexibility, and advanced forensic techniques can help alleviate these obstacles. The amounts of data generated by modern networks can easily overwhelm forensic investigators. The diversity of file types, encrypted communications, and cloud systems makes it difficult to isolate pertinent evidence. Additionally, the rising use of Internet of Things (IoT) devices introduces a wide array of data sources with different logging standards. Establishing a clear chain of custody for digital evidence is critical but challenging in high-stress situations. Any disruption in this chain can result in evidence being deemed inadmissible in court.

Cyber attackers often erase traces of their activities through anti-forensic techniques like data wiping or encryption. Tools like Volatility and Rekall are designed for preserving and analysing volatile memory, allowing investigators to extract essential information from RAM after the system has been powered down. Implementing live forensics during incident responses ensures that ephemeral data is captured on time. Cybercriminals may also use advanced techniques such as polymorphic malware (an evolving malware strain that frequently mutates its features to evade detection from traditional security solutions), rootkits, and steganography to evade detection and forensic investigation. These techniques require equally advanced tools and expertise to uncover.

IoT devices frequently utilise proprietary communication protocols that are either not fully documented or standardised, complicating the analysis of captured network traffic or system logs. This lack of standardisation makes it difficult to decipher communication patterns, especially when encryption or obfuscation techniques are used. The prevalent use of encryption for in-transit data such as SSL/TLS further complicates network traffic analysis. While encryption is crucial for secure communication, it can mask evidence of malicious behaviour

Additionally, investigations often cross multiple countries, creating jurisdictional challenges. Data privacy regulations, like GDPR, limit how evidence can be collected and handled, potentially causing conflicts between legal compliance and investigation objectives. International cooperation helps navigate jurisdictional issues. Forensic investigators must collaborate closely with legal experts to ensure adherence to data privacy laws while maintaining investigative integrity.

Furthermore, a zero-day may occur. This attack exploits a vulnerability in software or hardware that has not yet been identified or disclosed by the vendor or security community. These attacks are particularly dangerous as they are hard to detect. Conventional security measures, such as antivirus programs or IDS, depend on known vulnerabilities and attack signatures. As zero-day vulnerabilities are unknown, these defences often fail to recognise or stop the attack, allowing the attacker to remain undetected for prolonged periods while exploiting the vulnerability to steal data or gain unauthorised access. The challenge for digital forensic investigators is that zero-day attacks typically leave behind little evidence of compromise, making them difficult to trace. Investigators may not recognise these attacks until the vulnerability is discovered elsewhere, often long after the damage is done. Behavioural analysis and anomaly detection can help mitigate this issue.

Advanced forensic tools and automation are essential to tackle challenges in digital forensics, particularly within complex environments like IoT networks and cloud infrastructures. Utilising artificial intelligence (AI) and machine learning (ML) can greatly enhance the efficiency of investigations. These technologies can swiftly process grand amounts of data, identify anomalies, and detect suspicious patterns that would take human analysts much longer to uncover. By automating repetitive tasks, such as log analysis or detecting traffic patterns, AI and ML enable forensic investigators to concentrate on more critical facets of the investigation, thereby enhancing the speed and accuracy of the process. Moreover, the emergence of cloud computing and IoT environments requires the adaptation of new forensic methodologies. Traditional forensic techniques must evolve to address the unique characteristics of these platforms. For instance, forensic-as-a-service (FaaS) platforms offer centralised solutions to support investigators.

4 REFLECTIVE COMPONENT

Malicious individuals utilise various sophisticated strategies to infiltrate IoT networks to avoid detection, which complicates forensic investigations. These strategies include exploiting vulnerabilities in IoT protocols, intentionally obscuring data, and implementing advanced evasion methods. Each of these approaches presents distinct challenges that investigators must address to effectively identify, analyse, and mitigate security breaches.

A key challenge comes from the improper use of IoT protocols like MQTT, CoAP, or UPnP, which prioritise efficiency over security. Cybercriminals take advantage of these protocols to circumvent security measures, establish backdoors, and maintain persistent access to the network. For example, attackers might utilise protocols such as HTTP or DNS to manipulate and simulate legitimate traffic, blending seamlessly with normal network activities. This makes it hard for investigators to differentiate between regular device operations and malicious actions. Such tactics obscure evidence and complicate the tracing of attackers' activities within the network. To tackle this, investigators need to use advanced protocol analysis tools and behaviour-based monitoring applications that can identify protocol usage anomalies.

Data obfuscation is another common tactic hackers use to conceal their actions. This can include encrypting command-and-control communications, embedding malicious data in legitimate traffic or files through steganography, or altering device logs to hide signs of unauthorised access. For instance, an attacker may modify or erase logs from compromised devices to create the impression that a breach did not occur. These methods significantly impede forensic investigations, as critical evidence may be missing or heavily disguised. To counteract these techniques, investigators may adopt innovative strategies such as memory forensics to reveal decrypted data stored in RAM and utilise secure, immutable log repositories that capture and preserve logs in real time, even when devices are compromised.

Attackers also implement sophisticated evasion techniques, including IP spoofing to mask their identity, or using lateral movement within the network to access sensitive information without triggering alarms. In IoT environments, cybercriminals may compromise devices to navigate to other devices or systems within smart city infrastructures. These techniques complicate the tracing of the attackers' true origin and the complete understanding of the breach's scope. As a result, investigators need to utilise tools like network mapping software (like Nmap) to visualise communication paths and intrusion detection systems such as Snort to identify unusual traffic patterns that may indicate unauthorised movement or communication.

In addition to disguising their operations, malicious hackers often rely on anonymity tools like Tor or VPNs to obscure their location and identity. These tools make it exceptionally challenging for investigators to trace attacks back to their origins, especially when the evidence leads to anonymised endpoints or proxy servers. This problem is worsened by jurisdictional issues, as attacks may cross multiple countries with differing cybersecurity regulations and cooperation frameworks. To counter these methods, investigators can analyse metadata and timestamps across various devices, collaborating with internet service providers or international cybersecurity networks to identify patterns that penetrate the layers of anonymity.

Lastly, attackers may attempt to overwhelm forensic systems by generating excessive logs or traffic, a tactic known as log flooding or data poisoning. In smart city networks with a grand number of connected devices, this strategy can obscure critical evidence amidst a flood of irrelevant or fabricated data, increasing the likelihood of missing crucial patterns. To combat such tactics, AI-based systems can prioritise anomalies and highlight high-risk events. Furthermore, investigators can archive older logs for later analysis to ensure that significant data is not overlooked.

5 CONCLUSION

In summary, this report comprehensively outlines the essential steps for investigating an IoT security breach within a smart city network. The investigation process, which ranges from identifying vulnerabilities to gathering and analysing evidence, highlights the intricate nature of implementing a thorough and systematic forensic approach to security incidents in connected IoT environments.

The final stages of presentation and reporting in the digital forensics investigation are crucial for effectively interpreting and communicating evidence. Following the detection of the breach and the collection of pertinent data, the analysis phase requires advanced tools and methodologies to recreate the attack scenario. In this instance, employing network traffic analysis, log examination, and device memory forensics is vital for identifying the attacker's entry point, recognising exploited vulnerabilities, and understanding the breach's extent. By maintaining forensic integrity at every stage, investigators can confirm the evidence's reliability and significance.

The final phase of the investigation is reporting, which involves not only recording findings but also offering practical recommendations derived from the analysis. This report highlighted the challenges presented by vulnerabilities to IoT, such as inadequate protocol security, encryption weaknesses, and obfuscation techniques utilised by attackers. It has also highlighted the necessity of continuous monitoring, secure data collection, and centralised log management to uphold a robust forensic framework for smart city networks.

Ultimately, forensic investigations reveal not only the technical aspects of breaches but also provide strategic solutions to mitigate future incidents, aiding the primary goal of securing smart city infrastructures. By following forensic best practices and using advanced tools, the investigation can effectively deliver insights into the specific attack as well as recommendations for enhancing the security of IoT networks in smart cities.

REFERENCES

GeeksforGeeks, n.d. Challenges in Digital Forensics. [online] Available at: https://www.geeksforgeeks.org/challenges-in-digital-forensics [Accessed 1 December 2024].

BlackBerry, n.d. Polymorphic Malware: Ransomware Protection Solutions. [online] Available at: https://www.blackberry.com/us/en/solutions/endpoint-security/ransomware-protection/polymorphic-malware [Accessed 1 Dec. 2024].

CrowdStrike, n.d. Data Obfuscation. [online] Available at: https://www.crowdstrike.com/en-us/cybersecurity-101/data-protection/data-obfuscation [Accessed 1 December 2024].

Forensic Science International: Digital Investigation, n.d. [online] Available at: https://www.sciencedirect.com/journal/forensic-science-international-digital-investigation [Accessed 1 December 2024].

IEEE, 2022. Network Traffic Obfuscation and Automated Internet Censorship. In: 2022 10th International Symposium on Digital Forensics and Security (ISDFS), 27-28 June 2022, Istanbul, Turkey. New York: IEEE, pp. 1-10. Available at: https://ieeexplore.ieee.org/iel8/6287639/10380310/10623179.pdf [Accessed 5 December 2024].

CrowdStrike, n.d. What is a Honeypot in Cybersecurity? [online] Available at: https://www.crowdstrike.com/en-us/cybersecurity-101/exposure-management/honeypots [Accessed 7 December 2024].