

Forensic Investigation on IoT Devices & Components



Deric Vincen V.P

Enroll No. 032200300003013

Introduction

The Internet of Things (IoT) is rapidly transforming our world, connecting a vast array of devices to the internet. While this offers numerous benefits, it also presents new challenges for cybersecurity and forensic investigations. This presentation will delve into the complexities of forensic investigations on IoT devices and explore the techniques and tools available for extracting evidence.



Investigative Layers



- **Device Layer:** This layer focuses on acquiring data directly from the device's storage, such as memory dumps and file system analysis.
- **Network Layer:** This layer involves capturing and analyzing network traffic associated with the device, including communication logs and data transfers.
- **Cloud Layer:** This layer examines data stored in the cloud by the device's manufacturer or service provider.

Forensic Techniques

- **Physical acquisition:** This involves directly extracting data from the device's memory using specialized tools.
- **Logical acquisition:** This involves collecting data from the device's operating system and file system.
- **Network analysis:** This involves capturing and analyzing network traffic associated with the device.
- **Cloud analysis:** This involves analyzing data stored in the cloud by the device's manufacturer or service provider.
- **Malware analysis:** This involves analyzing malware found on the device to understand its functionality and potential impacts.

Forensic Tools

- **Universal Forensic Extractor (UFE):** A versatile tool used for acquiring data from various devices, including IoT devices.
- **Magnet Axiom:** Another popular option, Axiom offers comprehensive data acquisition and analysis capabilities for diverse devices, including some IoT models. It boasts user-friendly interfaces and advanced features like data carving and decryption.
- **CloudForensics:** As IoT data often resides in the cloud, tools like CloudForensics become crucial. They enable investigators to acquire, analyze, and present cloud-based evidence from various platforms like Google Drive and Dropbox.
- **The Sleuth Kit:** A free and open-source digital forensics toolkit used for acquiring and analyzing data from various devices.


Evidence Preservation

Decorative geometric shapes on the left side of the slide, including a large dark teal hexagon, a smaller teal hexagon above it, and two overlapping hexagons (one teal, one light green) at the bottom.

- Document the chain of custody: Maintain a detailed record of who handled the evidence and when.
- Use write-blockers: Prevent accidental modifications to the device's data.
- Create forensic images: Create a digital copy of the device's storage for analysis.
- Store evidence securely: Store evidence in a secure location with controlled access.

Challenges of IoT Forensics




- **Device diversity:** The vast range of IoT devices with varying hardware, software, and operating systems presents a significant challenge for investigators.
 - **Limited storage:** Many IoT devices have limited storage capacity, making it difficult to collect and preserve all potentially relevant evidence.
 - **Security vulnerabilities:** Many IoT devices are not designed with security in mind, making them susceptible to attack and data manipulation.
 - **Lack of standardization:** The lack of standardized forensic procedures and tools for IoT devices creates additional challenges.
- 

Case Study

In late 2016 in France, telecom company OVH was hit by a distributed denial-of-service (DDoS) attack. Experts were struck by how the assault was 100 times larger than similar threats. The following month, over 175,000 websites suffered, as Dyn, a managed DNS (Domain Name System) provider, was hit by another powerful DDoS attack. Much of the eastern United States and some of Europe suffered a significant drop in Internet quality.





The Mirai botnet was unlike other malware because it attacked IoT devices instead of computers. IoT, of course, is a fancy name for devices that carry sensors and software, allowing them to communicate with other devices and systems. Mirai infected vulnerable consumer devices like smart cameras. It also weaponized Realtek-based routers.

Mirai scanned the Internet for targets and breached their security by trying default username and password combinations. It didn't take long for Mirai to infect hundreds of thousands of IoT devices in countries worldwide and gain significant power. Mirai's attack in 2016 against OVH peaked at a startling 1TBps.

Conclusion

Forensic investigations of IoT devices require specialized skills, advanced tools, and a deep understanding of the unique challenges involved. By employing proper techniques, utilizing relevant tools, and maintaining a meticulous chain of custody, investigators can play a crucial role in fighting cybercrime and ensuring justice in cases involving IoT devices.



Thank You

