Insure IoT Forensics

University: University of Nebraska at Omaha
Members: Elisabeth Henderson, Ashley Leedom, Amber Makovicka, Ronald Ramirez, & Nathan Wood

Executive Summary

The Internet of Things (IoT) intersects with every aspect of modern life from industry to agriculture, education to entertainment, and medicine to law enforcement. With the ubiquity of IoT devices, it is imperative that forensic investigators can reliably gather data and maintain its integrity throughout the course of an investigation. Currently, there exists no defined and accepted standard for IoT forensic investigations. This can be attributed in part to the heterogeneous nature of IoT. Nearly every class of IoT device integrates its own hardware and software, data storage techniques, and network solutions differently. Even devices from the same category can vary in design and functionality. For example, Google and Amazon both produce home assistants. However, Google Home operates best as an in-house search engine while the Amazon Echo facilitates convenient online shopping. The nature and purpose of the device will also have an effect on the data that can be gathered; wearables and smart appliances will not generate the same types or volume of data. The data these devices gather and generate may be stored locally or on the cloud, compounding the complexity of the data acquisition process.

IoT forensics is still an emerging field due in part to the aforementioned reasons. This makes introducing evidence gathered from IoT devices in court difficult as investigators cannot point to best practices and precedent to show their evidence is sound. Many of the existing frameworks for forensics and IoT forensics are very similar to one another. They focus on a few core principles and differences from traditional forensics to IoT forensics. As a result, we've decided to focus more on the practical application of IoT forensics with hands on experiments, and have shifted away from developing our own framework.

Project Goals

- Review state of the art research and standards concerning IoT forensic and traditional digital forensics.
- Compare and contrast IoT forensic techniques with those of traditional digital forensics standards.
- Identify the driving factors of the slow maturation of IoT forensic standards and possible solutions.
- Apply recommended standards gathered from IoT forensic literature in hands-on experiments to test their effectiveness across multiple IoT devices.
- Provide educated recommendations on developing and establishing IoT forensic standards, research, and areas that merit further study.

Project Methodology

We started our project by conducting a review of the current literature and standards related to IoT forensic data acquisition. Additionally, we examined traditional digital forensics techniques and compared and contrasted them to current IoT forensics standards. The review provided insight on the current state of IoT forensics and which allowed us to identify outstanding issues in the field.

We examined and selected technical procedures to use and reference as we moved into the hands-on portion of our project. We referred to the processes and procedures presented in the Computer Forensics Technical Procedure Manual (North Carolina State Bureau of Investigation) as well as the Forensic Examination of Digital Evidence: A Guide for Law Enforcement (US Department of Justice).

The second half of our project focused on hands-on experimentation with IoT devices. This allowed us to fully understand the forensic and data acquisition processes. Lastly, using the knowledge we gained from the literature review and hands-on application, we will present our research, and refinements to IoT forensics moving forward.

Results / Findings

We discovered that many of the existing frameworks for digital and IoT forensics bear similiarities and share a few core principles. We decided to focus more on the practical application of IoT forensics with hands on experimentation and shift away from developing our own framework. Below we've summarized the results of our literature review and hands on experiments.

Literature review

We chose to focus our research in four categories: digital forensic frameworks, IoT forensic frameworks, the difficulties in establishing IoT forensic frameworks, and IoT data acquisition.

- Our research into digital forensic frameworks culminated in selecting A Comprehensive and Harmonized Digital Forensic Investigation Process Model as our de facto digital forensic framework.
    - Research Methodology: We examined and selected technical procedures to use and reference as we moved into the hands-on portion of our project. We referred to the processes and procedures presented in the Computer Forensics Technical Procedure Manual (North Carolina State Bureau of Investigation) and the Forensic Examination of Digital Evidence: A Guide for Law Enforcement (US Department of Justice).
    - Research and Framework Selection: We examined multiple digital forensics frameworks from over the years and analyzed their applicability to our project. We determined that the Comprehensive and Harmonized framework proposed by Valgarevic and Venter was the most suitable for our needs. We also referred to the recommendations presented by ACPO and NIST.
- IoT forensics is far less developed than traditional digital forensics, with minimal work available that defines prospective frameworks. In IoT forensics, instead of proposing traditional frameworks, researchers develop specific technology that addresses the various needs of a digital investigation. Emphasis is placed on gathering forensic data from IoT-based infrastructures and designing applications that can store, interpret, and report on the assembled evidence.
    - IoT Framework Selection: The Generic Digital Forensic Investigation Framework for the Internet of Things (DFIF-IoT) consists of three process blocks: proactive processes, IoT forensics processes, and reactive processes. Proactive processes

represent activities that prepare an organization to undergo a forensic investigation. This module encompasses incident scenario definitions, evidence source identification, planning incident detection, potential digital evidence collection, and digital preservation. IoT forensics processes represent all the IoT-based aspects and infrastructures from which digital evidence can be acquired. Reactive processes represent the digital forensic investigation itself and are triggered after an incident has been detected. There are three stages in this module: initialization, acquisitive processes, and investigative processes. During initialization, investigators follow established protocol for commencement of a digital forensic investigation. During the acquisitive processes, evidence is collected from data sources, transported, and stored securely. Finally, the investigative processes involve analyzing, interpreting, and reporting the gathered evidence.
    - DFIF-IoT Considerations: DFIF-IoT is purposely vague to account for the various applications of IoT devices in an organization. However, it does provide a stable foundation for the field to build off of in coming years.

- Currently no standardized IoT forensic framework exists. Complications include the wide variety of IoT devices, each with their own uses, makes, models, operating systems, and storage capabilities. Additionally, many of these devices do not store their data locally, but rather offload the data to the cloud which adds another level of complexity to creating a standard.

    - Data Extraction: IoT devices have many different storage methods. They might use a cloud service or write to a local hub running a service rather than storing data on the actual IoT devices. Devices also may not include traditional interfaces for gathering data stored on IoT devices.
    - Chain of Custody: Keeping a well document Chain of Custody is a vital process during a forensics investigation. However, with the diversity of IoT devices maintaining the documentation to uphold integrity could be difficult.
    - Evidence Handling: Digital evidence can be easily modified which could potentially overwrite important data. Traditional digital devices typically only have one location of storage which is not the case in IoT device. The environment of IoT is much more volatile, making data extraction more difficult.
    - Evidence Identification: Due to the variety of IoT devices and storage processes, identifying the data needed during an investigation can be challenging. Lack of forensic documentation and tools to collect the data once it has been identified can also be a nightmare for investigators.

- We identified four data acquisition techniques we would attempt on our own devices. These included using FTK, Bluetooth-based data extraction, network data extraction, and acquiring application data from a mobile device.

    - Data Acquisition Results: These techniques were employed in our hands on experiments, which are detailed below.

Hands on research

Our hands on experimentation focused on several IoT devices, including a Google Home Mini, Garmin Vivosmart HR+, and Metawear CPRO.

- Our first experiment utilized the Google Home Mini.

    - We wanted to observe its network traffic and view any logs available on the cloud platform. Unfortunately, the network traffic is encrypted and not human readable. However, the cloud platform has logs available to developers and law enforcement.
    - Another approach we took when analyzing the Google Home Mini involved a network monitoring tool developed by Princeton called IoT Inspector. This tool creates graphs from the data it observes, allowing us to see what the Google Home Mini interacts with such as advertisements domains. This tool is excellent when used in a research capacity but does not provide much actionable data for forensic analysts.

- Our second experiment utilized Ubertooth One, a tool for sniffing Bluetooth traffic.

    - Sniffing was done between an Android phone and two IoT devices, a MetaWear CPRO, and a Garmin Vivosmart HR+. We were able to capture and analyze this traffic in Wireshark.
    - The Metawear CPRO sent its packets in plaintext, however, the traffic was difficult to decipher. We were able to identify several commands sent from the phone to the device. This includes on and off signals for each LED light color and the initialization of the connection.
    - Unfortunately, the Garmin used encryption. We attempted to break the encryption using Crackle, however, we were unsuccessful.

- Our final experiment utilized a more traditional approach using FTK Imager, XRY, and Autopsy.

    - We attempted to connect each device to FTK Imager, but only the Garmin was recognized. While we were not expecting any device to be recognized, we were able to gather a lot of data from the Garmin. We identified the exact GPS route a user took during a workout as well as general health records.
    - We used XRY to create an image of the Android phone that had been connected to each IoT device. In examining the image of the phone, we were able to pull some of the data that had been generated by the IoT devices. From the Garmin, this data included daily summaries of user activity, individual workout information, and user profile information. The Metawear yielded files containing sensor data. The only evidence we could recover from the Google Home Mini were the connection confirmation and events created with voice commands.

Conclusion and Recommendations

The field of IoT forensics is evolving at a rapid pace despite its relatively young age. Due to the inherent diversity present in IoT devices and infrastructure, a standard forensic framework has yet to be developed. Instead, technology and software are being used to fulfill the requirements of a digital investigation. Unfortunately, they often have to be installed and operating before an incident occurs to be of any use. Unlike traditional digital forensics, IoT forensics requires investigators to be proficient in many forensic fields, primarily cloud, mobile, and network forensics.

Upon concluding our experiments, we found that the best means of acquiring forensically-relevant data from IoT devices is to use a more traditional approach. This entails gathering information directly from the device via the creation and examination of an image. When that is not possible, other disciplines of forensics can be utilized, such as mobile and cloud forensics.

Since the principle barrier to the creation of an IoT forensic framework standard is the mass diversity between the hardware and storage capabilities of IoT devices, we recommend introducing production standards in the field. This would allow toolkits to be created that can support multiple devices of a similar creed.

Due to the amount of data that gets offloaded from IoT devices to the cloud, legislation and procedures must be enacted that enable authorized investigators to gain access to that data. Investigators, of course, must possess a warrant or subpoena. Security should not be compromised for the sake of convenience.

The wide variety of IoT device types and data gathering capabilities means it may be difficult for investigators to identify which devices bear forensically-relevant information. Organizations should introduce publicly-available libraries tjat detail the general information that is stored on their devices (assuming internal storage does exist on that device). This information can help investigators target devices that will likely hold relevant information for an investigation.