Investigation Internet of Things (IoT) Device using Integrated Digital Forensics Investigation Framework (IDFIF)

Randi Rizal ¹, Missi Hikmatyar¹
¹Department of Informatics, Universitas Perjuangan, Tasikmalaya, Indonesia

Abstract. The Internet of Things (IoT) in the Industrial Revolution 4.0 refers to networks of objects, objects, or devices that are connected on a large scale connected to the Internet. These objects, become smart, feel the environment and collect and exchange data with other objects. Devices on the internet of things are interconnected with other devices for the purpose of securely exchanging data. This new technology appears in various fields of human life. Therefore there are many new challenges for forensic investigators in finding digital evidence on these IoT devices. A digital forensic researcher will face many challenges to gather evidence from infected components on an Internet of Things (IoT) device and also face difficulties in analyzing the evidence. In this study, there will be an investigation of network forensic attacks on the Internet of Things (IoT) devices using the IDFIF method.

1. Introduction

The current progress of digitalization and Internet connectivity, more leads to the development of new designs and prototypes that are full of creativity, namely the Internet of Things (IoT). Internet of Things (IoT) is a long-term investment by converting objects from traditional to intelligent by utilizing the basic technology that processes the Machine-to-Machine (M2M) and Radio Frequency Identification (RFID) devices [1]. The main goal in the use of Internet of Things (IoT) is to exchange data between devices and applications safely. In recent years the Internet of Things (IoT) has become very popular and implemented in various fields of life. A growing number of devices that are connected to the internet include many different capabilities [2]. Internet of Things (IoT) include personal computers, laptops, smartphones, tablets and other devices [4]. These devices are interconnected and share the same network to communicate with each other. All of these devices are connected to the internet with various conditions to analyze the situation and work accordingly. Connected devices are also programmed to make decisions automatically or properly inform users so that users can make the best decisions. The network between various connected devices can bring many advancements in application technology and services that can benefit development in various fields of human needs, one of which is in the business field. Many devices are connected to the internet to share local information with cyberspace. Some IoT elements such as RFID (Radio Frequency Identification), WSN (Wireless Sensor Network), WPAN (Wireless Personal Area Network), WBAN (Wireless Body Area Network), HAN (Home Area Network), NAN (Neighborhood Area Network), M2M (Machine to Machine), CC (Cloud Computing), and DC (Data Center) have influence in life such as the IoT sensing process. According to analysis reports, many devices connected to the Internet of Things (IoT) attract hackers to solve network security mechanisms in the Internet of Things (IoT) device [3]. To investigate such attacks, it is necessary to apply the parameters
of the digital forensic Internet of Things (IoT) parameter [5] called Forensic IoT [1]. Digital forensic investigations on the Internet of Things (IoT) devices are very challenging and diverse, traditional forensic models do not fit into the current Internet of Things (IoT) environment. Many large devices will also bring new challenges to data and network management. A number of Internet of Things (IoT) devices will generate large data making it difficult for researchers to analyze data [6].

2. Methodology

2.1. Arduino Bluetooth Configuration Scheme

Preparing the Arduino package which is the main package needed in the system, the package used is the Arduino driver package that can be installed directly. The Arduino configuration with Bluetooth Hc-05.

![Figure 1. Bluetooth Arduino Configuration Scheme with](image)

Some configurations on Arduino connect Arduino to a computer, carrying out serial communication such as sending and receiving sensor data via a serial terminal on the Arduino IDE via the USB Connector. Power Jack: Input voltage to activate Arduino, IC ATMEGA 328p: ATMel microcontroller IC with Arduino bootloader. Digital I/O is used for digital input and output, at pin 3, 5, 6, 9, 10, 11 has a sign (~) which indicates that the pin other than having Digital I/O facilities also has PWM (Pulse Width Modulation) the output value range is 8 bits or an equivalent value between 0-255. Next is Analog Input which is used for sensor data input, potentiometer, and other analog input devices. Then Power is used to take the power of 5V, 3.3V, GND.

Configuration is also done on Bluetooth HC-05 devices. When configuring Bluetooth, the Bluetooth position is not associated with an Arduino device that uses wireless. The default Bluetooth setting is Baudrate: 9600bps, Name Bray with Code: 1234. Any changes to the above configuration will be saved even when the power is turned off. All commands sent to Bluetooth do not have to be newline characters. Furthermore, the procedure to do that Bluetooth configuration is to connect Bluetooth to the PC, the LED must blink, open the Arduino IDE software, select the correct COM port that is connected to Bluetooth.

2.2. Scenario of Attack IoT Device

Stage of scenario attacks on the Internet of Things (IoT) devices to implement network forensics on the Internet of Things (IoT) devices. System simulation aims to conduct Bluetooth forensic testing of the Internet of Things (IoT) network of devices in detecting attacks. Simulation is done using the LOIC tool used to detect attacks. Training starts with sending IP packets on the target and the port will be attacked. The following is an example of an attack system simulation against an Internet of Things (IoT) device:
3. Result
Investigation of Internet of Things (IoT) devices uses the Integrated Digital Forensics Investigation Framework (IDFIF) [7] method with the following results:

Figure 3. Integrated Digital Forensics Investigation Framework (IDFIF)
3.1. Preparation
An initial phase was covering preparations to conduct an investigation of start doing evidence handling process to making the report. There are several stages to the main stage of preparation, notification, authorization, and preparation.

3.1.1. Notification. Notified of violations of law to law enforcement. This stage is the process of receipt a report related to the occurrence of a case.

3.1.2. Authorization. The step for the right of access to evidence and the law status of the investigation activity.

3.1.3. Preparation. Prepared the availability of tools and personnel. Equipment that was brought to the investigative process is hardware tools and software tools. Preparing a first responder who will do if the crime scene.

3.2. Proactive Process
A prompt action against a offence area so that witness is not contaminated and manipulated digitally. There Six phases exist in proactive main stages are:

3.2.1. Safing the area. Did a procedure to ensure the offence area (the scene). And shield from contamination so that the integrity is maintained.

3.2.2. Documenting the Scene. Processing a crime scene, searching for the origin of the woodpecker events searching for connections and network communications and document the crime area by opinion a picture every detail of the area.

3.2.3. Incident Sparking. An first analysis of the method of events that happened looked at the potential evidence at the scene.

3.2.4. Proactive Preservation. Direct action against the evidence to maintain its integrity. There five subphases in this phase are:

- Plugin Portable Power Supply, a resource in the process of securing electronic evidence that is being alive.
- Communication Shielding, Protection against electronic evidence to avoid contamination.
- Non-volatile Evidence, securing digital evidence that is non-volatile.
- Protection, protection of the data phase includes the resistance that attacks containment, and recovery is the return of such systems.
- Monitoring, the stage for a real investigation to investigate the network by performing a search for traces on the network and seeking potential data used as evidence

3.2.5. Proactive analysis. Analysis of direct action to get the initial hypothesis on the investigation. There three subphases in this phase are:

- Strategy Approach, Strategy or method in the collection. Determine the strategy or technique that according to the case.
- Detection of Incident/Crime that detects and confirm a violation of the law.
- Capturing, capturing of data contained in the network and capture activity happening on the network.
3.2.6. Preliminary report. Manufacturer of the initial report on the investigation at this stage of proactive

3.3. Reactive Process
The main stage is that continued action on the investigation. In this reactive stages, the investigation process traditionally. The reactive process is a continuation of proactive measures to optimize the process of investigation. There six phases in the reactive process are:

3.3.1. Identification. Is to identify the evidence, the search for potential evidence. Digital evidence that identified as a result of capturing the data activity on the network.

3.3.2. Collection & Acquisition. A collection stage and the stage of acquisition of electronic evidence. Collecting electronic evidence and acquire digital evidence.

3.3.3. Preservation. Keep the integrity of the artifacts using a chain of custody and hashing functions. There three subphases in this phase are:

- Seize, is foreclosing on the artifacts as well as the labeling of finding items.
- Transportation, transfer of evidence from the crime scene to the laboratory.
- Storage, storage of electronic evidence in the storage of evidence and data capturing results in a database.

3.3.4. Examination. Processing of evidence or data to find a connection with the incident. At this stage of consideration of the data obtained from the network. There two subphases in this phase are:

- Logging file, storage and provision of information to the database data.
- Classification, Classification of the data according to criteria such data.
3.3.5. **Analysis.** A technical assessment and arranging linkages between present findings.

![Image of IoT Graph Traffic Log](Figure 6)

**Figure 6. IoT Graph Traffic Log.**

3.3.6. **Documentation.** Documented of all activities phase of the investigation from the beginning to the analysis phase.

3.4. **Presentation**

Presentation process is the last action in the current of the investigation which is the description of the results of the investigation in a report by the legal provisions and the use of common language.

| Table 1. File Log Bluetooth Traffic |
|-------------------------------------|
| **No.** | **Timestamp** | **Source IP** | **Dest. IP** | **Protocol** | **Source Port** | **Dest. Port** | **Payload** |
| 1       | 2018-04-12 08:27 | 192.168.0.222 | 192.x.x.x.127 | UDP | 59132 | 137 | 7965|2507|8617|8061|7|4663 | 6d654206275056465 |
| 2       | 2018-04-11 14:03 | 192.168.0.135 | 192.x.x.x.127 | UDP | 49775 | 137 | c3426051b11b9a8b07f022e0c |
| 3       | 2018-04-11 14:03 | 192.168.0.87 | 192.x.x.x.127 | UDP | 63293 | 137 | 552084756a20067686e64 |

3.4.1. **Conclusion.** Stage gathering up the outcome of the investigations that have been execute.

3.4.2. **Reconstruction.** The whole process of analysis and evaluation of the results of the investigation.

3.4.3. **Dissemination.** The recording means of the investigation and the entry can distribute to the other investigators who hold investigations on similar cases.

4. **Conclusion**

In this paper, we provide different aspects than those used for IoT and also use IoT devices. The author has presented a network forensic model for detecting attacks and identifying attacks. Here's more about the flooding attack and found the infected IoT Bluetooth Arduino device. Log file data with p.cap extension can be analyzed by network forensic investigation using Wireshark application. Based on the analysis that has been done, it was found that 3 IP addresses committed illegal actions, which led to overload traffic. By applying IDFIF, it can be used to detect flooding attack on IoT devices.

5. **References**

[1] Zawoad, Shams, and Ragib Hasan. "FAIoT: Towards Building a Forensics Aware Eco System for the Internet of Things." Services Computing (SCC), 2015 IEEE International Conference on. IEEE, 2015.

[2] Y. Huang and G. Li, “A semantic analysis for internet of things,” in Intelligent Computation Technology and Automation (ICICTA), 2010 International Conference on, vol. 1. IEEE, 2010, pp. 336–339.
[3] Hossain, Md Mahmud, Maziar Fotouhi, and Ragib Hasan. "Towards an Analysis of Security Issues, Challenges, and Open Problems in the Internet of Things." Services (SERVICES), 2015 IEEE World Congress on. IEEE, 2015.

[4] L. Atzori, A. Iera, and G. Morabito, “The internet of things: A survey,” Computer Networks, vol. 54, no. 15, pp. 2787–2805, 2013.

[5] R. Rizal, I. Riadi, and Y. Prayudi, “Network Forensics for Detecting Flooding Attack on Internet of Things (IoT) Device,” Int. J. Cyber-Security Digit. Forensics, vol. 7, no. 4, pp. 382–390, 2018.

[6] Oriwoh, Edewede, et al. "Internet of Things Forensics: Challenges and approaches.” Collaborative Computing: Networking, Applications and Worksharing (Collabratecom), 2013 9th International Conference Conference on. IEEE, 2013.

[7] M. Hikmatyar, Y. Prayudi, and I. Riadi, “Network Forensics Framework Development using Interactive Planning Approach,” Int. J. Comput. Appl., vol. 161, no. 10, pp. 41–48, 2017.

[8] Ruuhwan, Y. Prayudi, and I. Riadi, “Evaluation of Integrated Digital Forensics Investigation Framework for the Investigation of smartphones Using Soft System Methodology”, Int. J. Electrical and Computer Engineering (IJECE), 2017.