IOP Conference Series: Materials Science and Engineering

PAPER • **OPEN ACCESS**

IoT forensic: Optimizing Raspberry Pi for investigation on the smart home network

To cite this article: N Widiyasono *et al* 2019 *IOP Conf. Ser.: Mater. Sci. Eng.* **550** 012019

View the article online for updates and enhancements.

This content was downloaded from IP address 118.171.222.70 on 07/11/2019 at 05:59

IOP Conf. Series: Materials Science and Engineering **550** (2019) 012019 doi:10.1088/1757-899X/550/1/012019

IoT forensic: Optimizing Raspberry Pi for investigation on the smart home network

N Widiyasono[1], I K G D Putra[2] , I A D Giriantari[3] and M Sudarma[4]

[1] Siliwangi University, Siliwangi Street, Tasikmalaya 46115, Indonesia
[2,3,4] Udayana University, PB Sudirman Street, Denpasar 80234, Indonesia

Email: nur.widiyasono@unsil.ac.id

Abstract. Cybercrimes can occur by utilizing existing technology, and any such crime leaves a trace on the system, i.e. data digital evidence. Therefore, it takes a scientific way to analyze the digital evidence on the forensic of such cybercrime. Raspberry Pi is one of the systems that can be developed and functioned as a device used for investigation on the network. The device can capture data on layer 5 (session layer) and investigation process using NIST (National Institute of Standard Technology) method. Raspberry utilization is not only in the process of capturing the data alone but can be used for Mobile Wireless Hacking. Like the two blades of the device has a benefit according to the needs of its users. This device can be further developed for the investigative process by mobile law enforcers, by making some modifications so that they can be taken wherever they go. The contribution of this research is developing this tool for investigation process on network service where after system able to do wireless hacking then data collection at layer 5 is done automatically during the specified timeframe, then the system will auto shutdown by itself, besides modification of battery as energy source so that this tool can be used in mobile.

1. Introduction

Cybercrime is a term that refers to criminal activity with a network computer as a tool, target, or place of crime, such as fraud (online auction, check, car credit, identity, child pornography) so that cybercrime can be defined as a crime that uses the computer illegally. Cybercrime activities have electronic evidence that is electronic and requires forensic management to be analyzed. Digital Forensic is this case isa management of cybercrime.

Cybercrime is done through the internet network media, criminals perform the action by using weaknesses of the system and Internet network infrastructure to get important information. Forensic management and handling attacks on Internet networks are called Network Forensics. Network Forensics is an activity carried out to collect digital data evidence and analyze cyber crimes committed by perpetrators and present the report in the trial.

Certain IoT application services are connected to cloud computing or IoT ecosystems connected through existing networks to enable security holes. IoT benefits for the industry are very large but have the potential for unique security challenges given the growing cybersecurity threats and will affect the implementation of IoT. Enhancing IoT security systems and developing effective digital forensics techniques for investigating sources of attack and obtaining digital evidence data is important so that they can be used in the trial process. The heterogeneity of IoT devices and the absence of standardization become IoT Forensics challenges, besides requiring special applications that have the ability to collect

Content from this work may be used under the terms of the Creative Commons Attribution 3.0 licence. Any further distribution of this work must maintain attribution to the author(s) and the title of the work, journal citation and DOI.
Published under licence by IOP Publishing Ltd

digital data evidence. Application capabilities are several stages of the investigation process such as data collection, examination, analysis and reporting [1]

Interoperability and IoT connectivity standards as well as IoT security, privacy, availability and resilience issues have been conducted, although IoT security issues are still open to review, and studies of digital forensics to investigate cybercrime on IoT are also more important [2].

IoT can connect humans with various services, sensors, and other objects. IoT is currently used in several applications such as smart transportation, smart healthy and smart sensor networks [3]. IoT development leads to cloud-based services and is a business opportunity that increases the number of smart devices [4]. The IoT environment has challenges to security issues including privacy, access control, data storage, and communication security [5]. Caution Investigations are also directed at the use of devices, sensors, and every byte connected to the IoT ecosystem. This problem causes the growth and spread of vulnerable and insecure IoT devices [6]. Conventional user-based security architecture is not used on IoT networks [7]. so in carrying out the ecosystem investigation phase IoT requires special tools, techniques, and procedures such as to secure IoT networks, collect data, maintain data and analyze digital data evidence.

IoT devices are designed to work passively and independently [8], thus requiring a broad search process, even though they can be found, but for digital forensics there is no way to do digital evidence data collection and documentation [9], in addition to methods for imaging IoT devices Forensics is so limited that it ignores ethical considerations to find evidence of devices running in a multi-tenancy environment [10].

Smart home infrastructure usually uses local area networks including shared access points with routers to connect to existing devices, in addition to using smart plugs. The smart plug has several functions, such as the wireless signal strength is much stronger, reduces cable problems, controls several smart devices at the same time with a touch of a button [11]

IoT Forensic is a digital forensic activity conducted to gather digital data evidence within the Internet of Things (IoT) device. The process of collecting digital data evidence requires tools such as raspberry pi but by default raspberry pi requires installation and configuration in advance that is adding the operating system *Kali-Linux RPI, Wireshark, Ethercap, Aircrack-ng,* and programming, besides those devices are not can be done in mobile so that require change to intake of power source in the form of battery. Therefore, this research aims to develop an optimized raspberry Pi for investigation on the smart home network.

2. Method

Process flow stages of research can be described in figure 1.

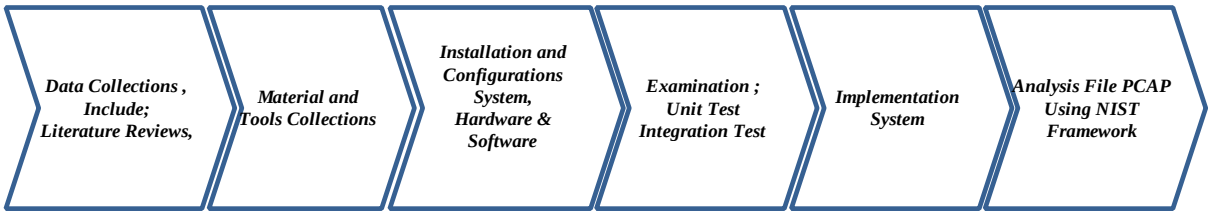


Figure 1. Research process flow.

The necessary data collection on theories relating to this research such as Raspberry Pi, networking, digital evidence, data acquisition and how the system is built, with literature study techniques that collect the necessary data from journals, books, internet, articles, as well as discussions with counselors during the consultation process.

The collection of tools and materials is any collection of necessary materials that support such as hardware and software. The following of hardware and software required are shown in Table 1.

Table 1. The hardware and software needed for the development of Raspberry Pi.

No	Hardware / Software	Function
1	*Raspberry Pi 3 B*	Device for system control
2	MicroSD 16GB	As Storage Operating System, coding and other data.
3	*USB Wireless Adapter* (*TP-Link TL-WN722N*)	Media for wireless access
4	*USB Drive / Flash disk*	External storage for (.pcap)
5	5v power supply adapter	Power source
6	*Box Casing*	Packing all hardware
7	*LED (red, yellow, green, orange)*	Set the system work process
8	4 Resistors 330 Ω	Electric current inhibitor to led
9	4 pieces Keys: 1 Large keypad, 3 Small keys	Device point indicator indicator
10	Cable Jumper	Raspberry Pi connector with LED and button
11	Image Kali Linux Rpi (.img)	Operating System for Raspberry Pi special Forensic / Cracking
12	Bash Script	Script or coding to control the system
13	Python	Script for controlling Raspberry Pi to network access point, LED, and Button
14	Aircrack-ng and crunch	Tools for cracking passwords
15	Ettercap (Text version)	Tool for sniffing
16	MD5 & SHA Checksum Utility	Tool for hash testing on pcap files
17	Wireshark	Tools to perform pcap file analysis

Installation stages and system configuration was prepared to illustrate the workings of the system before designing the design of hardware and software.

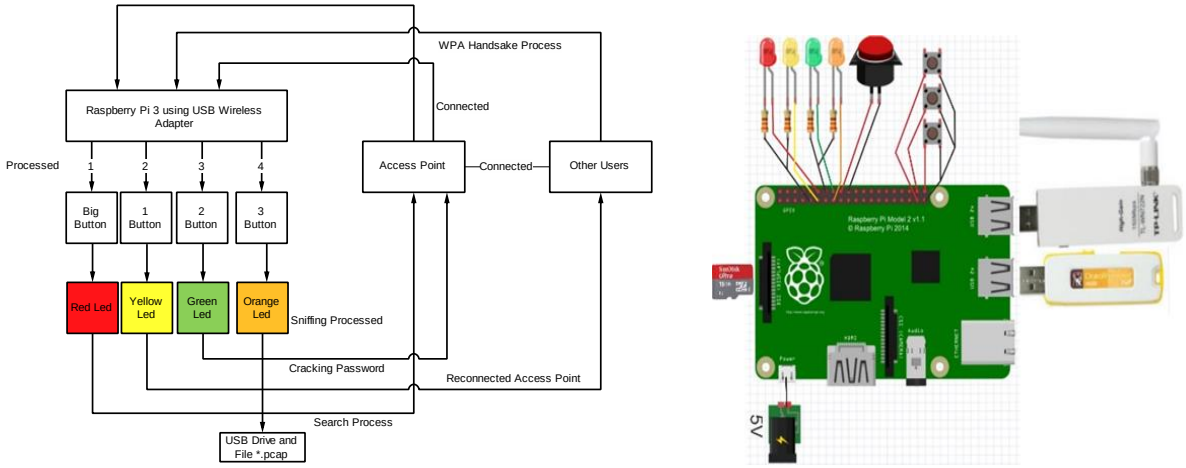


Figure 2. System block diagram.

Figure 2 describes the overall system block diagram. Having input and output to run the process, Input is run using the buttons, and the output of a lighted LED indicates the process of the system. Raspberries act as systems that receive input, process, and output. Raspberry Pi interacts with the access point and other users get pcap files and last stored on USB Drive.

The detail of system operation are as the following: start the process by pressing big button, with the red indicator indicating that it is searching the access point, pressing the button 1 with the yellow indicator light, stopping the access point search process, another user search to perform "WPA Handshake "button, pressing button 2 with green indicator to stop other user search process, and cracking password process, if cracking process too long it can be stopped by pressing button 3, and function button 3 to do sniffing.

3. Results

The test of the system was done by implementation of the system in the field. Selection of access point and user, and WPA Handshakes. The main process that is done in the process of selecting access point and user to be targeted or target to go to stage cracking. The trial of Raspberry tool developed is done on the access point available in the environment of Siliwangi University. The test results in the form of file "*. Pcap" which then analyzed the file by using the NIST method.

Table 2. The result of system testing.

Test	Access point name	The other users connected with the same Access Point	The process of WPA Handshake with other users	Cracking Access Point password	Sniffing the Network (Access point)	Get the digital Evidence (*pcap*)
1	Wakwekwok	Yes	Yes	Yes	Yes	Yes
2	NUABi	No	No	No	No	No
3	HANAWA	Yes	Yes	Yes	Yes	Yes
4	MyPublicWifi	Yes	No	No	No	No
5	MyPublicWifi	Yes	Yes	Yes	Yes	Yes

Table 3 shows that Raspberry Pi 3 has many advantages so that it can be optimized as a tool to get digital data evidence on IoT devices.

Table 3. Comparison of Raspberry Pi3 , Windows IoT, and android things.

No	Parameter	Rasspberry Pi	Microsoft IoT	Android Things
1	Operating System	Raspbian Jessie, ARM-Based Linux OS, Raspberry Pi Media Centers, RISC OS Pi, Plan 9, Retro Gaming Suites, FreeBSD, Chromium OS, Windows 10 IoT Core, Android 7.0 Nougat, AROS: AmigaOS Remake	Windows 10 IoT	Google Brillo
2	License type	Open Source	Closed Source	Open Source
3	Programming Tools	Raspbian 8.0., BlueJ, an IDE for Java., Geany, an IDE for almost any language, Greenfoot, another IDE for Java, Mathematica, serious math on an Rpi, Node-RED - Wiring for the IoT, Python, a modern, flexible language for the Rpi, Scratch, a stepping stone to programming.	Windows Code	LeakCanary. AIDE. Vysor,Stetho, B4A, One of "Speed-Injecting" Android App Development Tools.,Android Studio. GenyMotion, Visual Studio with Xamarin, Takt, Unreal Engine, InstaBug, Eclipse, Source Tree, Fabric, Codota

4. Conclusion

The optimization has been successfully conducted to raspberry device so that it can be used to conduct a mobile investigation for a smart home environment using Access Point to connect between IoT devices. This system capable to obtain digital evidence data of PCAP extension equipped with RDP help, to access point search stage, find other users connected to same access point, WPA Hand11shakes, password cracking, password found, connect to access point, sniff, obtains "* .pcap" files and then performs the analysis and the final report makes a withdrawal.

References

[1] Harrell C 2010 *Journey Into Incident Response* available at: http://journeyintoir.blogspot.co.id/2010/10/overall-df-investigation-process.html
[2] Giaretta A S B 2016 *IEEE Trans. Inf. Forensics Secur.* **11** 665–76
[3] Zarpelão B B, Miani R S, Kawakani C T and de Alvarenga S C 2017 *J. Netw. Comput. Appl.* **84** 25–37
[4] Chifor B.-C, Bica I, Patriciu V.-V and Pop F 2017 *Future Gener. Comput. Syst.* **86** 740–49
[5] D'Orazio C J, Choo K-K R and Yang L T 2017 *IEEE Internet Things J.* **4** 524 – 535
[6] Alaba F A, Othmana M, Hashem I A T and Alotaibi F 2017 *J. Netw. Comput. Appl.* **88** 10–28
[7] Kent K, Chevalier S, Grance T and Dang H 2006 *Guide to Integrating Forensic Techniques into Incident Response* (Gaithersburg: National Institute of Standards and Technology Special Publication) p 800
[8] Wang L, Peng D and Zhang T 2015 *IJSH* **9** 173-82
[9] Ambrosin M, Anzanpour A, Conti M, Dargahi T, Moosavi S R, Rahmani A M and Liljeberg P 2016 *IEEE Micro* **36** 25–35
[10] Harbawi M and Varol A 2017 *5th International Symp. on Digital Forensic and Security (ISDFS)* (Tirgu Mures, Romania: IEEE) p 1
[11] Venčkauskas A, Damaševičius R, Jusas V, Toldinas J, Rudzika D and Drėgvaitė G 2015 A *IJESRT* **4** 460–77