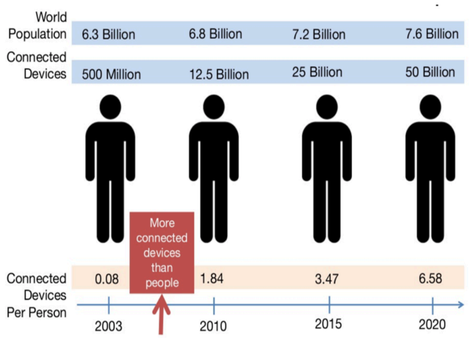
IoT Digital Forensics of Nest Ecosystem

Gokila Dorai, Department of Computer Science, Florida State University

Dr. Shiva Houshmand, Department of Computer Science, Southern Illinois University

INTRODUCTION

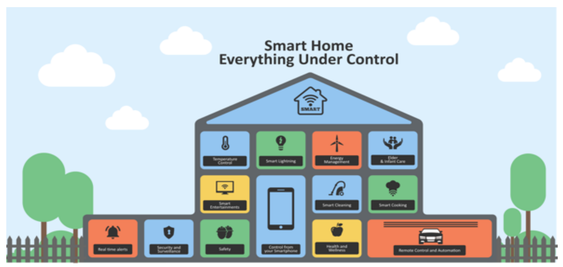
In the current world, we have a huge number of devices connected to the internet. Gartner's prediction [7] estimates that close to 21 billion devices that rely on IoT would have been connected by 2020. Home monitoring systems, personal health gears, numerous wearable devices, cars, appliances are some example of growing field of internet of things (IoT). Through sensors, connectivity, people and processes, the smart system of internet of things exchange enormous amount of data and potentially hold valuable information for investigators. Our contribution in this paper is the forensic analysis of Nest mobile application installed in iPhone devices which is used to control Nest devices such as, the thermostat, indoor and outdoor cameras. The information contained within the Nest app can prove invaluable to law enforcement in the investigation of crimes. The primary goal of this paper is to identify, extract and document artifacts created by Nest app on iOS devices. The artifacts are extracted from iTunes backup files. We also classify these artifacts in a forensically sound manner to provide useful insights to forensic investigators. The following figure is from Cisco IBSG, April 2011:



OBJECTIVES

Our objective was to investigate the following on several IoT devices in a *smart home* setting:

- What kind of data can be collected from IoT devices?
- Can new types of data and traces from these devices be utilized for digital forensic purposes?
- If so, how can we collect and analyze them efficiently?
- How can IoT devices aid forensic investigators with their cases?



FORENSIC ANALYSIS

- What happened?
- When did it happen?
- How did it happen?
- Who and/or What did it?

MATERIALS & METHODS

The devices used for this study are the 2nd generation Nest Learning Thermostat, Nest Indoor camera and Nest outdoor camera. The devices are equipped with 802.11 radios as well as 802.15.4 radios. The device setup is performed with the use of the mobile Nest iOS application. Through the application, users are asked to provide the SSID and password of their home network. This allows the devices to communicate with the Nest services. Unlike other home automation platforms, in the Nest ecosystem there is no central hub responsible for coordination of the devices. The devices can access the internet directly through the home's Wi-Fi router. Additionally, the Nest Protect devices are capable of communicating with each other, regardless of the presence of a Wi-Fi network, using the Nest Interconnect feature.

Data was collected from iOS devices using iTunes backup system without encryption. On detailed analysis, useful information regarding user activities in a home environment were collected.

EXPECTED RESULTS

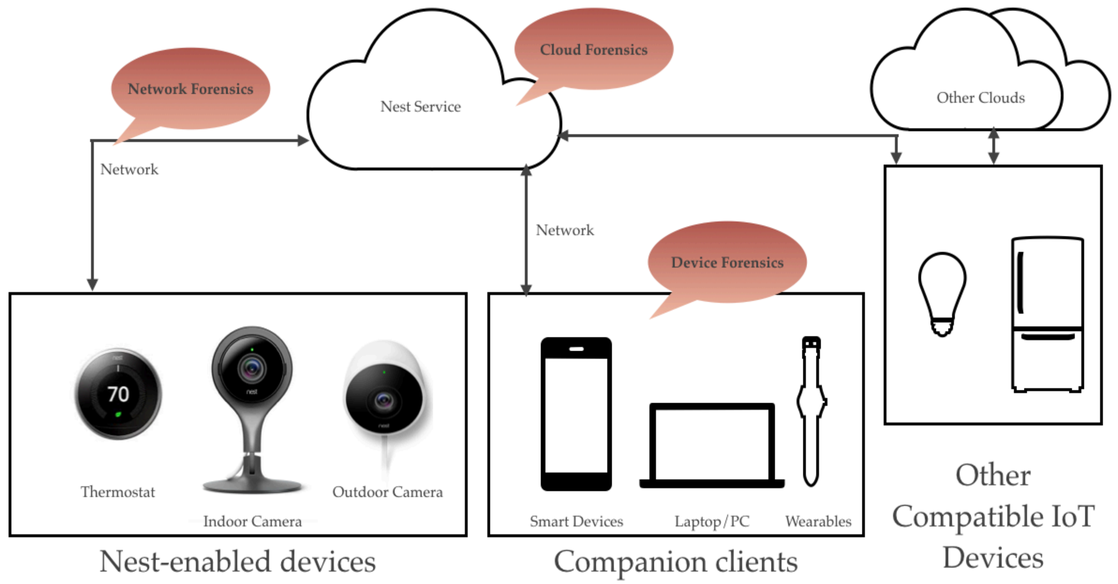
We recovered the following information by performing mobile device backup analysis:

- User adjustments to thermostats
- Thermostat Schedules
- Entry/Exit of a person from home
- Sounds heard at a given time
- User Settings
- Location Settings
- Timeline series

CHALLENGES

- IoT can be inappropriately used as a platform for illegal activities or storage of files used for espionage purposes.
- The fast pace at which IoT devices are manufactured, securing these devices from attacks is becoming a challenge.
- Internet of things can be infected with malware, could be hacked, they can have back-doors for attackers to intrude and, they can be tampered.
- Data diffusion across various components.
- IoT device manufacturer tends to use their own proprietary protocol for data and communication.
- Lack of standardized IoT forensic tools.
- Lack of stable international policies to acquire cloud data with mutual agreement.

Forensic Ecosystem of Nest-enabled Devices



FUTURE WORK

Cloud forensics of Nest internet of things is essential for identifying user behaviors, because most meaningful data are only saved on the cloud side. However, acquiring data from the cloud has two fundamental limitations in that it requires valid user credentials (usually a set of ID and password), and it is practically impossible to respond to a situation in which users try to delete data from the cloud. Analyzing client companions will help us in handling this limitation. Therefore, our future work might focus on this.

CONCLUSION

The number of connected IoT devices is going to grow rapidly. Hence, automated forensic analysis of any component in an IoT ecosystem is highly essential. Also, sensors are limited to the physical information they register and the implementation of the detection algorithm. Many sensor readings are tunable. That being said, the users of such data and models should be aware of the existence of false positives and false negatives. They should take proper steps to detect and minimize false results from IoT devices. And hence, investigators of any case involving IoT forensics must be aware of such false results.

REFERENCES

1. B. Copos, K. Levitt, M. Bishop, J. Rowe, Is Anybody Home? Inferring Activity From Smart Home Network Traffic, in: Security and Privacy Workshops (SPW), 2016 IEEE, IEEE, 245–251, 2016.

2. S. Zawoad, R. Hasan, FAIoT: Towards Building a Forensics Aware Eco-System for the Internet of Things, in: Services Computing (SCC), 2015 IEEE International Conference on, IEEE, 279–284, 2015.

3. S. Perumal, N. M. Norwawi, V. Raman, Internet of Things (IoT) digital forensic investigation model: Top-down forensic approach methodology, in: Digital Information Processing and Communications (ICDIPC), 2015 Fifth International Conference on, IEEE, 19–23, 2015.

4. V. R. Kebande, I. Ray, A generic digital forensic investigation framework for internet of things (iot), in: Future Internet of Things and Cloud (FiCloud), 2016 IEEE 4th International Conference on, IEEE, 356–362, 2016.

5. H. Chung, J. Park, S. Lee, Digital forensic approaches for Amazon Alexa ecosystem, Digital Investigation 22 (2017) S15–S25.

6. A. Mylonas, V. Meletiadis, B. Tsoumas, L. Mitrou, D. Gritzalis, Smartphone forensics: A proactive investigation scheme for evidence acquisition, Information Security and Privacy Research (2012) 249–260.

7. Gartner's article on "8.4 Billion Connected Things", https://www.gartner.com/newsroom/id/3598917

ACKNOWLEDGEMENTS

Our special thanks to Dr. Sudhir Aggarwal, Florida State University for guiding me through this work.