Advances in Computational Sciences and Technology
ISSN 0973-6107 Volume 10, Number 5 (2017) pp. 1285-1293

http://www.ripublication.com

IoT Evidence Acquisition – Issues and Challenges

Parag H. Rughani

Ph. D.
Assistant Professor, Institute of Forensic Science
Gujarat Forensic Sciences University
E-mail: parag.rughani@gmail.com

Abstract

As the world is moving to Internet of Things, the attackers too. Increasing use of IoT devices in various segments has been instrumental in attracting attackers for possible use of this latest and less controlled technology in committing crimes. Though, academia, industry and research fraternity is busy in strengthening security of IoT components, they are still not able to keep pace with offenders. As it is not possible to completely eliminate crimes, there is always need of forensics, and IoT is also not an exception. Time is not far when the crimes will be IoT centric and will need to be investigated forensically. This paper is an attempt to identify issues and challenges involved in Evidence Acquisition of IoT components from a crime scene. The outcome of the work done can be essentially helpful to forensic investigators in understanding and overcoming these issues in overcoming crucial evidences from and IoT crime scene.

Keywords: IoT Forensics, IoT Crimes, Evidence Acquisition, Internet of Things, IoT Attacks, IoT Crime Investigation.

1. INTRODUCTION

Internet of Things is one of the latest technologies which has initiated a new era in the field of computer and networking. The network of networks of computer ruled the world for almost few decades but now it is IoT which has started dominating in all segments. Bradley J. et. al.[1] in their white paper mentioned that Internet of Everything will create public-sector opportunities worth $4.6 trillion, while Gartner, Inc. forecasts that connected things will be in use worldwide will reach 20.8 billion by 2020 [2].

One can imagine how crucial it will be to make sure that these devices will not be compromised. As it is very well known that large number of researchers and security experts are not able to secure Internet fully, while the Internet of computers is existing from years. This is a huge task ahead to secure Internet of Things, which is an emerging technology and there are no uniform implementations.

Lack of standards and guidelines is one of the reasons behind improper implementation of IoT concepts. Considering expertise and pace by which attackers are adopting and targeting new technologies, one cannot ignore possibilities to see more attacks on IoT implementations in near future.

ForeScout IoT Enterprise Risk Report clearly suggests that by 2018, two thirds of enterprises will experience IoT security breaches. Following figure is detailed predictions of the report published by ForeScout [3].

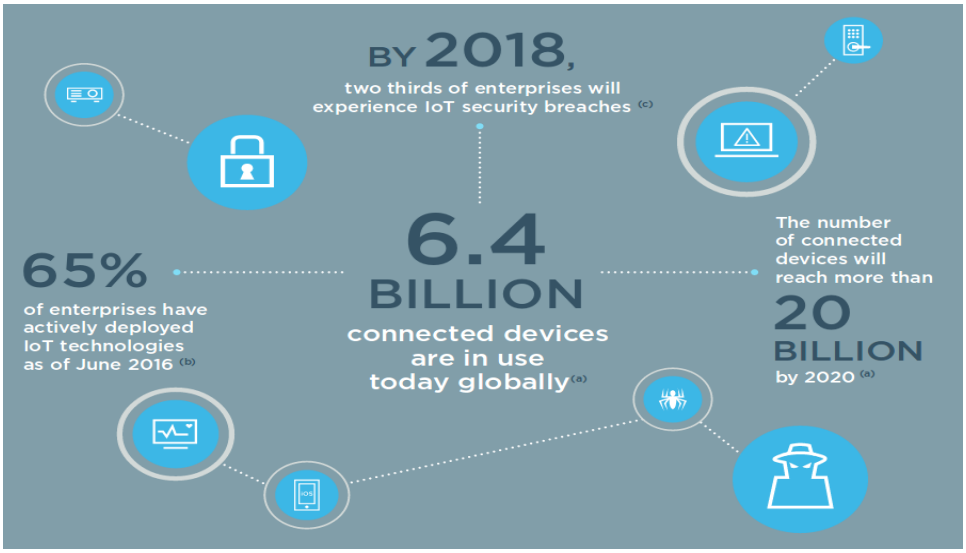

Figure 1.1 ForeScout IoT Enterprise Risk Report

It is necessary to accept possibilities of IoT related crimes and prepare necessary standards, guidelines and procedures to assist investigation of IoT crimes. IoT forensics is therefore one of the most important aspect that needs to be addressed along with IoT security. Researchers, Manufacturers and Developers are in hurry to implement smart technologies at all levels, but this urgency is leading to vulnerable systems. More emphasis is given on user friendliness and accessibility compared to security. The pace by which the smart technologies are being introduced is enthusiastic, however, if we cannot secure them then they will become prone to all

sorts of attacks. These attacks may be worse and dangerous than current attacks on Internet of Computers, only reason behind this is access to anything through Internet in IoT world.

This paper discuss important aspects related to evidence acquisition from IoT crime scene, which is the most important step of forensics. Following sections explain IoT, IoT Security, Forensics and IoT evidence acquisition issues and challenges followed by conclusion.

2. INTERNET OF THINGS

Various authors defined Internet of Things based on their perception, Atzori et. al.[4] conceptualized IoT in 3 paradigms, Internet - oriented, things oriented and semantic - oriented. Similarly, IEEE P2413 – an IEEE project for IoT also considers IoT architecture as a three-layered architecture consisting of 1) Applications, 2) Networking and Data Communications and 3) sensing layers [5]. While Gubbi J. et. al.[6] defined IoT as "Interconnection of sensing and actuating devices providing the ability to share information across platforms through a unified framework, developing a common operating picture for enabling innovative applications."

However, the basic idea of IoT is to connect everything through Internet for the purpose of sharing information, resources and services. Embedded systems, M2M, and similar concepts were initiated but did not long last, but with era of IoT they have been reintroduced. It will not be a proper justification to say that IoT has evolved recently, it was there in different forms but now has picked up pace with evolution in the speed of Internet. So, in general terms we can say that Internet of Things basically is a network of existing components like, sensors, apps, clouds and many more to allow communication between non-living things and make them smart.

IoT as being an evolving concept, no standard architecture is adopted uniformly, however, many researchers proposed various architectures to illustrate possible way of implementing it. Khan R. et. al.[7] discussed a generic architecture with five layers, which consists Perception, Network, Middleware, Application and Business as bottom-to-top layers.

While, purpose of this work is to assist forensic investigators in IoT evidence acquisition, I have decided to consider a general architecture with 3 layers as shown in following figure, which can give an idea about which evidences can be found from which layer.

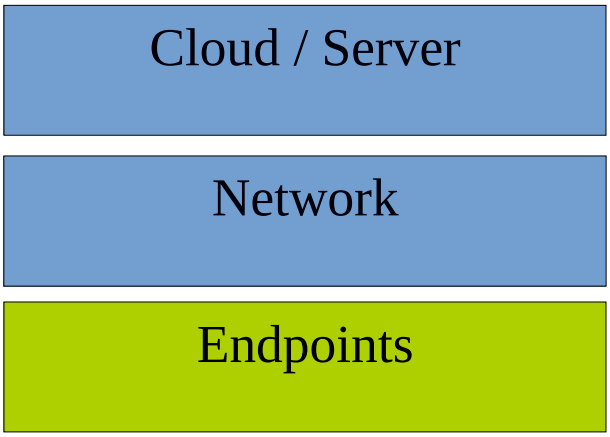

Figure 2.1 IoT Architecture

The above figure shows a simple and generalized architecture of IoT, which is directly or indirectly followed by all the IoT implementations. The bottom layer consists of endpoints, which could be anything ranging from sensors, micro-controllers, RFID tags, smartphones, computers, or anything which is required and is the end point of the network. The middle layer here is necessary for allowing endpoints to communicate and share information with each other and even for preserving information on a cloud storage. The top layer may be optional in few cases but in most of the scenarios it will be needed to preserve information for future use.

3. IoT SECURITY

While it is necessary to make non-living things smart enough to handle certain process by themselves or at least to inform concerned authorities in case of any abnormal situation occurs, but it is equally important to secure these smart things. The concept of smart phone, smart car, smart home, smart office, smart enterprise, etc. is the need of the hour but not at the cost of security of the people and information used by these so called smart devices and premises.

Since, the research fraternity is conscious about security of IoT, many authors have contributed in this paradigm. Xu, T. et. al. [8] proposed propsed a hardware based security mechanism for IoT, while Farooq, M. U. et. al. [9] discussed various challenges involved in security at various layers of IoT. Zhang Z, et. al. [10] on other hand discussed challenges related to IoT security. Riahi, A. et. al. [11] suggested a systemic and cognitive approach for IoT security.

Though, a lot of work has been done in this regard, it is still not sufficient to keep IoT world secure. In fact it is not even possible to do so, because even if sufficient techniques are adopted one can not prevent attacks caused by the mistakes of end

users or mis-configurations. Also, the way criminals are focused, collaborated and equipped they are always one step ahead then the security experts. We can never ignore possibilities of security breaches resulting into crimes in this world including digital and IoT world. The IoT crimes are bound to happen and we need to address them to solve. There is acute need of forensic investigators who can understand and solve IoT related crimes which may happen in the future. We may educate forensic investigators to equip themselves to handle possible future IoT crimes with their advanced skills and available tools.

4. FORENSICS

Forensics – use of scientific tools and techniques in solving crimes – exists from many years. Digital forensics a branch was needed to deal with digital crimes after criminals and offenders started exploiting digital components and media like computers, mobile phones and Internet. The digital forensics or the forensics itself can be seen as a step-by-step process for solving a crime. Many authors have defined this process by dividing into multiple phases. Altheide C. and Carvey H. [12] in their book "Digital Forensics with Open Source Tools" broken down digital forensics process in three categories as shown below:

Figure 4.1 Forensics Steps

The acquisition step here includes identification and acquisition of important evidences from a digital crime scene, and this is core of this paper. The second phase deals with analysis of evidences acquired from the crime scene to understand how, when and by whom the crime was committed. The outcome of the analysis reports including other documentation comprises the presentation phase. This phase ends with presenting complete analysis report in front of the court.

Dr. Edmond Locard (1877-1966) gave principle of exchange [13]: "Any action of an individual, and obviously the violent action constituting a crime, cannot occur without leaving a trace." in 1934. This rule was defined in context with conventional crimes, but it is proved correct in digital world also. The same rule is equally applicable in the Internet of Things.

It has been seen in digital crimes that whenever any object [Computer, mobile, storage media, etc.] interacts with any other object, significant information is exchanged and preserved. This principle of exchange is the key aspect in solving a crime.

Considering case of IoT, the things which are connected to the network and are

involved in sharing information in any form equally fulfill requirements of principle of exchange, especially when used for malicious activities or with malicious intentions.

5. ISSUES AND CHALLENGES INVOLVED IN IOT EVIDENCE ACQUISITION

As evidence acquisition is a key point in forensics process, if it is not handled well, the investigators may exclude some necessary and important evidences during their acquisition or may collect unnecessary evidences, which may mislead overall analysis and investigation process. To address this issues this section discusses various challenges to help the investigator in identifying and acquiring important and required evidences from the IoT crime scene. As per oxford dictionary [14] crime scene is the place where an offense has been committed and forensic evidence may be gathered.

Before identifying and acquiring any evidence one must remember that volatile memory also contain useful information and should not be missed in case if it is available. This applies to all the three layers of IoT architecture. Details on volatile memory acquisition from computers are explained by Ligh, M. H. et. al. [15] in their book “Art of Memory Forensics”.

When we talk about digital crimes, most of the times we generally find and acquire Computers, Mobile / Smart phones, Storage media, electronics gadgets, etc. from the digital crime scene. A detailed guideline to identify and acquire evidences from digital crime scene is already published by NIST [16]. But so far there is not specific guideline available specifically for IoT crime scenes.

The evidence acquisition process in this section is based on previously defined IoT architecture in figure 2.1 of this paper. Since, sufficient work is done in network and cloud / server forensics, the emphasis in this paper is given to only bottom layer consisting of Endpoints. The endpoints are the most commonly encountered components from a crime scene. Some of the challenges of IoT crime scenes are discussed below.

The major challenge in IoT crime scene is visibility of the evidences, there are chances that one may not see any endpoint at the crime scene or opposite to that one may find thousands of sensors lying on a crime scene. Since, it is possible to implant or embed sensors in any device or even in human body, it may not be possible for the forensic investigator to identify and locate the endpoints at the crime scene. As it may not be possible to check each and every corner and person present at the crime scene to discover endpoints, the best way a forensic investigator can do is to collect and analyze logs from network devices to identify number of sensors connected in the

network under investigation. These logs may also provide additional information about location and / or last time when sensor was active.

Another challenge in this step of forensic investigation is to document the topology of the network of the endpoints, as we are connecting things in the IoT and that too through the Internet, the possibilities are always there that a sensor found on the crime scene is sending information to a home appliance residing at an unknown location. Again, it is not possible to traverse through all the sensors and components to prepare a network diagram. The best thing which can help in this situation is again related to network log analysis, however, many times it may not be possible to get a complete picture of IoT implementation for the suspect network, especially if network device has logs only since it restarted.

Next challenge in acquisition is to decide whether to create an image of an endpoint or to acquire it physically. In case of computer crimes, the standard practice is to create a working copy / image of the storage media and seal the actual media to avoid accidental alteration in the actual evidence. However, one needs to think a lot in case of IoT crime scenes. Since, the endpoints in IoT crime scenes – excluding computers and smartphones – stores minimal or no information, it is very difficult to create an image of those endpoints. In case if a component stores some information then also it should be technically possible to create image of that device. The suggested way is to create image from available sources.

Another challenge in evidence acquisition is to maintain integrity of the evidences collected. Most frequently used technique for computers and phones is to calculate hash and maintain chain-of-custody to assure integrity. However, chain-of-custody is a feasible solution here, the question arise about calculating hash at the time of creating image. The problem here is lack of available tools that can prevent accidental changes in the endpoint.

Further, Many times these endpoints remain passive and are activated on specific incident to raise an alert or to perform a task. It would be very difficult to know when and how the sensor communicate. One can think about reverse – engineering the controller which is programmed to manage overall functionality of the endpoints.

Last but not the least is mobility of the IoT endpoints. If we take example of smart watch, smart shoes, smart chips, components of smart home, smart cars, drones, etc. then it is very much possible to mobilize them at any location. Until and unless they are actively connected to the network, they are not traceable. It may not be possible to visualize these scattered endpoints which can play a major role in forensic investigation.

6. CONCLUSION

As discussed in previous section, there are notable issues and challenges in the IoT evidence acquisition process – first step of IoT forensics. If not addressed in timely manner, these issues and challenges may lead to incomplete or incorrect forensic investigation of IoT crimes, which may give a benefit to criminals as they can be escaped very easily based on lack of evidences or false positives / negatives. These issues need an immediate attention from all the concerned domain experts to make sure IoT gets implemented properly, remain secure and if required it should be possible to solve the IoT crimes for safer and better IoT world.

REFERENCES

[1] Bradley J. , Reberger C. , Dixit A. and Gupta V., Internet of Everything: A $4.6 Trillion Public-Sector Opportunity, - White Paper in Cisco and/or its affiliates, 2013.

[2] Rob van der Meulen, Gartner Says 6.4 Billion Connected "Things" Will Be in Use in 2016, Up 30 Percent From 2015, Press Release, 2015.

[3] Michael DeCesare, ForeScout IoT Enterprise Risk Report, 2016

[4] L. Atzori, A. Iera, G. Morabito, The Internet of Things: A survey, Comput Netw. 54 (2010) 2787 – 2805

[5] Minerva R, Biru A and Rotondi D, Towards a definition of the Internet of Things (IoT), IEEE Internet Initiative, 2015.

[6] Gubbi, J., Buyya, R., Marusic, S., & Palaniswami, M. (2013). Internet of Things (IoT): A vision, architectural elements, and future directions. *Future generation computer systems*, *29*(7), 1645-1660.

[7] Khan, R., Khan, S. U., Zaheer, R., & Khan, S. (2012, December). Future internet: the internet of things architecture, possible applications and key challenges. In *Frontiers of Information Technology (FIT), 2012 10th International Conference on* (pp. 257-260). IEEE.

[8] Xu, T., Wendt, J. B., & Potkonjak, M. (2014, November). Security of IoT systems: Design challenges and opportunities. In *Proceedings of the 2014 IEEE/ACM International Conference on Computer-Aided Design* (pp. 417-423). IEEE Press.

[9] Farooq, M. U., Waseem, M., Khairi, A., & Mazhar, S. (2015). A critical analysis on the security concerns of internet of things (IoT). *International Journal of Computer Applications*, *111*(7).

[10] Zhang, Z. K., Cho, M. C. Y., Wang, C. W., Hsu, C. W., Chen, C. K., & Shieh,

S. (2014, November). IoT security: ongoing challenges and research opportunities. In *Service-Oriented Computing and Applications (SOCA), 2014 IEEE 7th International Conference on* (pp. 230-234). IEEE.

[11] Riahi, A., Natalizio, E., Challal, Y., Mitton, N., & Iera, A. (2014, February). A systemic and cognitive approach for IoT security. In *Computing, Networking and Communications (ICNC), 2014 International Conference on* (pp. 183-188). IEEE.

[12] Altheide C. and Carvey H., Digital Forensics with Open Source Tools, 2011

[13] Locard E. Police and scienifiques methods (1934) , page 8

[14] https://en.oxforddictionaries.com/definition/crime_scene

[15] Ligh, M. H., Case, A., Levy, J., & Walters, A. (2014). *The art of memory forensics: detecting malware and threats in windows, linux, and Mac memory*. John Wiley & Sons.

[16] Crime Scene Investigation A Guide for Law Enforcement, NIST, 2013