IoT Forensics

Paul-David Jarvis
Faculty of Science & Technology
Bournemouth University
Bournemouth, Dorset
s5115232@bournemouth.ac.uk

***Abstract*—This paper looks at "Internet of things forensics: Recent advances, taxonomy, requirements, and open challenges" and evaluates the solutions that the paper discusses and their advantages and disadvantages**

Keywords—IoT, FEMS, UFED, IOV, Trust-IoV, Open source DRone Parser, DAT, TXT

I. Main Problem

I decided to look at "Internet of things forensics: Recent advances, taxonomy, requirements, and open challenges" by Ibrar Yaqoob, Ibrahim Abaker Targio Hashem, Arif Ahmed, S.M. Ahsan Kazmi and Choong Seon Hong. The main problem that this paper attacks is the fact that Internet of Things (IoT) devices are growing in popularity and is increasing the risk of vulnerabilities in these devices and the challenges that digital forensics experts face when performing forensics on IoT devices. The paper attempts to tackle this problem by an exploration of IoT's novel factors affecting traditional computer forensics, Investigating and analysing recent studies on IoT forensics to find their strengths and weaknesses, devising a taxonomy based on forensics phases, enablers, networks, sources of evidence, investigation modes, forensics models, forensics layers, forensics tools, and forensics data processing and presents prominent use cases of IoT forensics and the key requirements for enabling IoT forensics [1].

It is extremely important to focus on this issue as technology is growing at an exponential rate and smart devices and IoT devices are on the rise. Many more cities are being smart and circular, more households are switching over to IoT technology and 127 devices are connected to the internet every second [2]. Though the growth of IoT devices in more households and cities means that they're becoming more technologically advanced and making the lifestyle of their citizens easier, sadly it also means that they become more dependent on technology and cyberattacks are on the rise. New methodologies come out by researchers attempting to adopt a variety of forensic techniques in order to investigate cyberattacks involving IoT devices.

II. Background and Related Work

The paper looked at several potentials cyberattacks in home appliances, cars, medical
implants, sensor nodes, and tag readers [1]. The paper moves onto explaining the advances made to help digital forensic experts in analysing these devices.

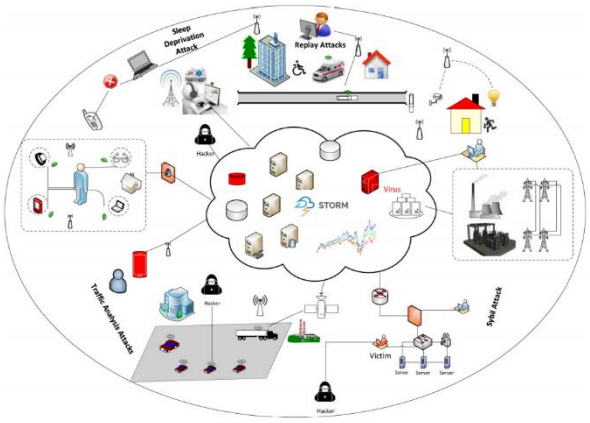

Fig. 1. The Security Concerns In an IoT-based Environment – (Yaqoob et al, 2019)

III. Forensics Edge Management System

Forensics Edge Management System (FEMS) is a system that was mentioned in this paper. It is a system that autonomously provides security and a forensic service within a home filled with IoT devices. This system and the forensic service it provides will monitor the house's network, intrusion detection and prevention and offer other benefits such as automatic detection [1] and reports to either the owner or forensics investigators depending if escalation is needed [3].

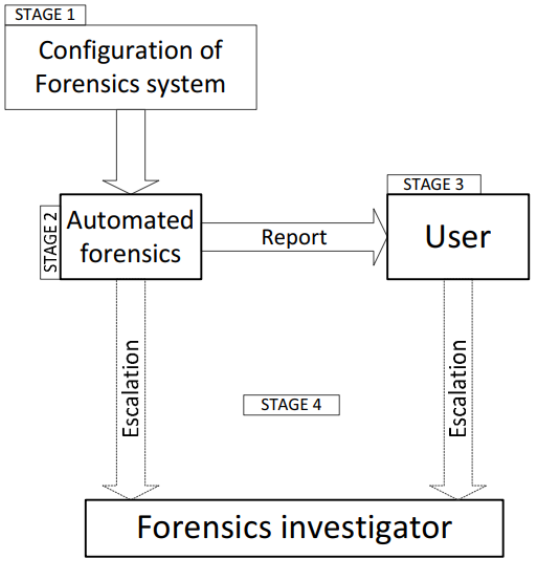

Fig. 2. Flow Diagram of FEMS – (Saint and Oriwoh, 2013)

A. FEMS Evaluation

The FEMS is extremely complex. I believe that the protection it supplies and the autonomously it offers is great. Knowing that IoT devices are becoming more of a regular thing day after day and knowing that not everyone who has a smart house filled with IoT devices are technological

competent so having a system that works without need from the user means that these people without a knowledge of how to digitally protect themselves is great and that they're protected. However, knowing that this system is extremely complex and is a safe bet to say that this system would need to be tested and tuned per household which potentially could be very expensive.

IV. Universal Forensic Extraction Device

The paper also touches on forensics for smartphones and how they're becoming more popular than desktop computers for criminals to exchange messages between one another. It has become very difficult to extract vital information from exploited smartphones for forensics purposes and visits a potential solution that addresses these challenges that uses a Universal Forensic Extraction Device (UFED). When a UFED is attached to a smart device it will attempt to extract passwords and pins, call history, emails, SMS, contacts and other potentially important information that can be used by digital forensics experts. [4].

Fig. 3. A Portalable UFED – (UFED | UNIVERSAL FORENSIC EXTRACTION DEVICE – unival group, 2020)

A. *Universal Forensic Extraction Device Evaluation*

The UFED seems like an incredibly useful piece of hardware. Its portability makes it extremely useful when digital forensics experts must visit on-site at the crime scene and can capture the data as soon as possible. The features it offers in terms of being able to extract information from smartphones could potentially help hundreds of people. For Example. If the UFED can extract numbers and SMS from a human trafficker's phone and potentially could expose the entire racket. However, the newer devices are very expensive with one selling for $6,000 on eBay and older models selling for roughly $100 meaning that anyone could pick one up and abuse it [5].

V. Trust-IoV

Mercedes, BMW and Tesla are all car manufacturers that have released their own version of an Internet of Vehicles (IoV) smart car. These smart cars and other huge tech companies like Google and Uber that are trying to create IoV smart cars introduces a very challenging problem. These vehicles share information to help improve road safety and traffic but now with millions of IoV cars interconnected means that malicious threat actors may find smart cars an attractive targets and launch attacks that attempt to compromise and exploit weaknesses and could potentially cause danger or death with their malicious instructions. Challenging problems for digital forensic experts could be the sheer amount of data being generated, formats of the evidence and potentially fruit from a poisonous tree considering the attacker was in the car's system meaning they could easily tamper with it.

The paper addressed this with the proposed trustworthy investigation framework called Trust-IoV. Trust-IoV will help to collect and preserve the integrity of the evidence and help maintain a secure provenance. The framework consists of a Forensics Gateway (FG) and IoV-Forensic Service (IoV-FS). The FG collects all the data from the smart vehicle itself as well as potential cloud services and smartphones. This potential evidence is then stored securely in the IoV-FS [6].

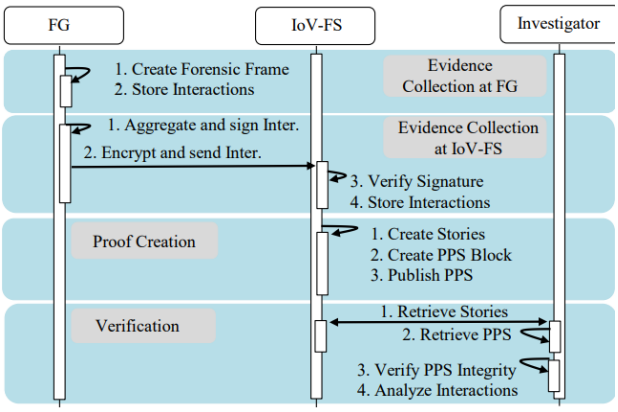

Fig. 4. The Operational Model of IoV – (Hossain, Husan and Zawoad, 2017)

1) Trust-IoV Evaluation

Knowing that IoV smart vehicles are becoming more common and knowing the risks that could potentially happen when it comes to self-driving vehicles and being hacked, Trust-IoV seems like a great forensics model to help digital forensic experts to analyse cyberattacks involving smart vehicles. Keeping the integrity of the data is one of the most important aspects when it comes to a criminal investigation so it's extremely helpful when the model and the IoV-FS helps secure the evidence.

VI. Drone Open Source Parser

Criminals have used drone with a malicious purpose to perform certain illegal activities such as remote surveillance or to even drop bombs. The paper touches briefly on DRop, a forensic analysis tool for drones that makes it much easier to see what the drone has done. It does this by analysing a TXT file that is stored on the mobile device controlling the drone and includes data such as GPS locations, battery and flight time which can be used to link to other evidence from meta data.

Fig. 5. DJI Phantom 3 - (Phantom 3 Standard - DJI, 2021)

1) Drop Evaluation

This is a great tool to help with the forensics when it comes to drones, however because of how drones are made there is a possibility that the data and evidence can be lost if the drone is started up which creates a new TXT and DAT file or these pieces of evidence could be deleted if the drone's internal storage is full [8].

VII. Self evaluation

The problem that this paper tackles is extremely broad and successfully fixing the problem will be near to impossible due to the growth of IoT devices and IoV vehicles and the malicious threat actors that attack these devices increasing their expertise, resources and knowledge. However, fixing the main problem means fixing the problems in the specific IoT category like household IoT devices, smartphones or vehicles. There are hundreds of different solutions or models and will be more to fix and help digital forensic experts analyse the data and these solutions and models will only increase in their sophistication and become more complex as time goes on. I am unable to contemplate any model that would work better than the FEMS, UFED and Trust-IoV.

References

[1] Yaqoob, I., Hashem, I., Ahmed, A., Kazmi, S. and Hong, C., 2019. Internet of things forensics: Recent advances, taxonomy, requirements, and open challenges. Future Generation Computer Systems, [online] 92, p.Abstract. Available at: <http://www.sciencedirect.com/science/article/pii/S0167739X18315644> [Accessed 20 November 2020].

[2] Gyarmathy, K., 2020. Comprehensive Guide To Iot Statistics You Need To Know In 2020. [online] Vxchnge.com. Available at: <https://www.vxchnge.com/blog/iot-statistics> [Accessed 20 November 2020].

[3] Sant, P. and Oriwoh, E., 2013. The Forensics Edge Management System: A Concept and Design. 2013 IEEE 10th International Conference on Ubiquitous Intelligence and Computing and 2013 IEEE 10th International Conference on Autonomic and Trusted Computing, [online] Available at: <https://ieeexplore.ieee.org/document/6726257> [Accessed 20 November 2020].

[4] unival group. 2020. UFED | UNIVERSAL FORENSIC EXTRACTION DEVICE - Unival Group. [online] Available at: <https://unival-group.com/ufed-universal-forensic-extraction-device-html> [Accessed 20 November 2020].

[5] Swearingen, J., 2019. Cops' Favorite Phone Hacking Tool Is Being Sold On Ebay. [online] Intelligencer. Available at: <https://nymag.com/intelligencer/2019/02/cellebrite-phone-hacking-tool-is-being-sold-on-ebay.html#:~:text=The%20Cellebrite%20Universal%20Forensic%20Extraction,will%20run%20you%20about%20%246%2C000.> [Accessed 20 November 2020].

[6] Hossain, M., Husan, R. and Zawoad, S., 2017. Trust-IoV: A Trustworthy Forensic Investigation Framework for the Internet of Vehicles (IoV). ResearchGate, [online] p.2. Available at: <https://www.researchgate.net/publication/317179920_Trust-IoV_A_Trustworthy_Forensic_Investigation_Framework_for_the_Internet_of_Vehicles_IoV> [Accessed 20 November 2020].

[7] DJI Official. 2021. Phantom 3 Standard - DJI. [online] Available at: <https://www.dji.com/uk/phantom-3-standard> [Accessed 3 January 2021].

[8] Clark, D., Meffert, C., Baggili, I. and Breitinger, F., 2017. DROP (DRone Open source Parser) your drone: Forensic analysis of the DJI Phantom III. Digital Investigation, 22, pp.S3-S14.