THE ROLE OF MOBILE FORENSICS IN ACQUIRING THE DIGITAL EVIDENCE ARTEFACT OF IOT-BASED APPLICATIONS

By
Ts Dr Nurul Hidayah Binti Ab Rahman
Lecturer
Faculty of Computer Science and Information Technology
Universiti Tun Hussein Onn Malaysia

Outline

- Introduction
  - IoT and Digital Forensics
  - Introduction to study
- Study Background
- Experimental setup
- Results and Discussion
- Conclusion and future work

Introduction

Digital Forensics

- include the collection and acquisition, analysis, interpretation and reporting of digital evidence that involves the usage of digital devices capable of storing electronic information connected to unlawful acts.

Internet of Things

- ecosystem encompasses interconnected systems of cyber-physical devices equipped with embedded IoT functionalities (e.g. sensors and actuators) that have the ability to generate, collect, exchange and store data via networking and communication infrastructure (Gubbi et al. (2013); Hossain et al. (2015); Stankovic (2014)).

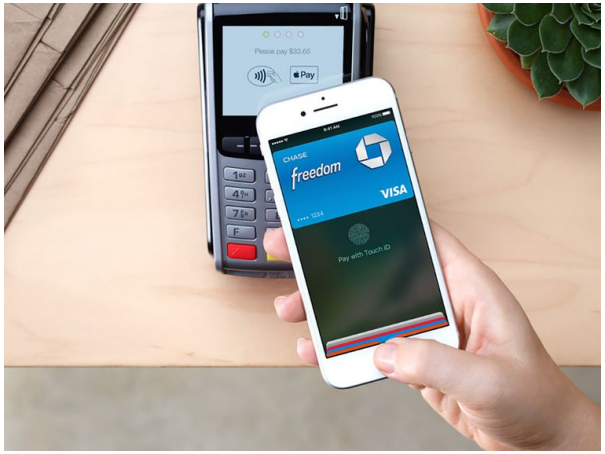
The role of smartphones in the IoT

IoT and digital evidence

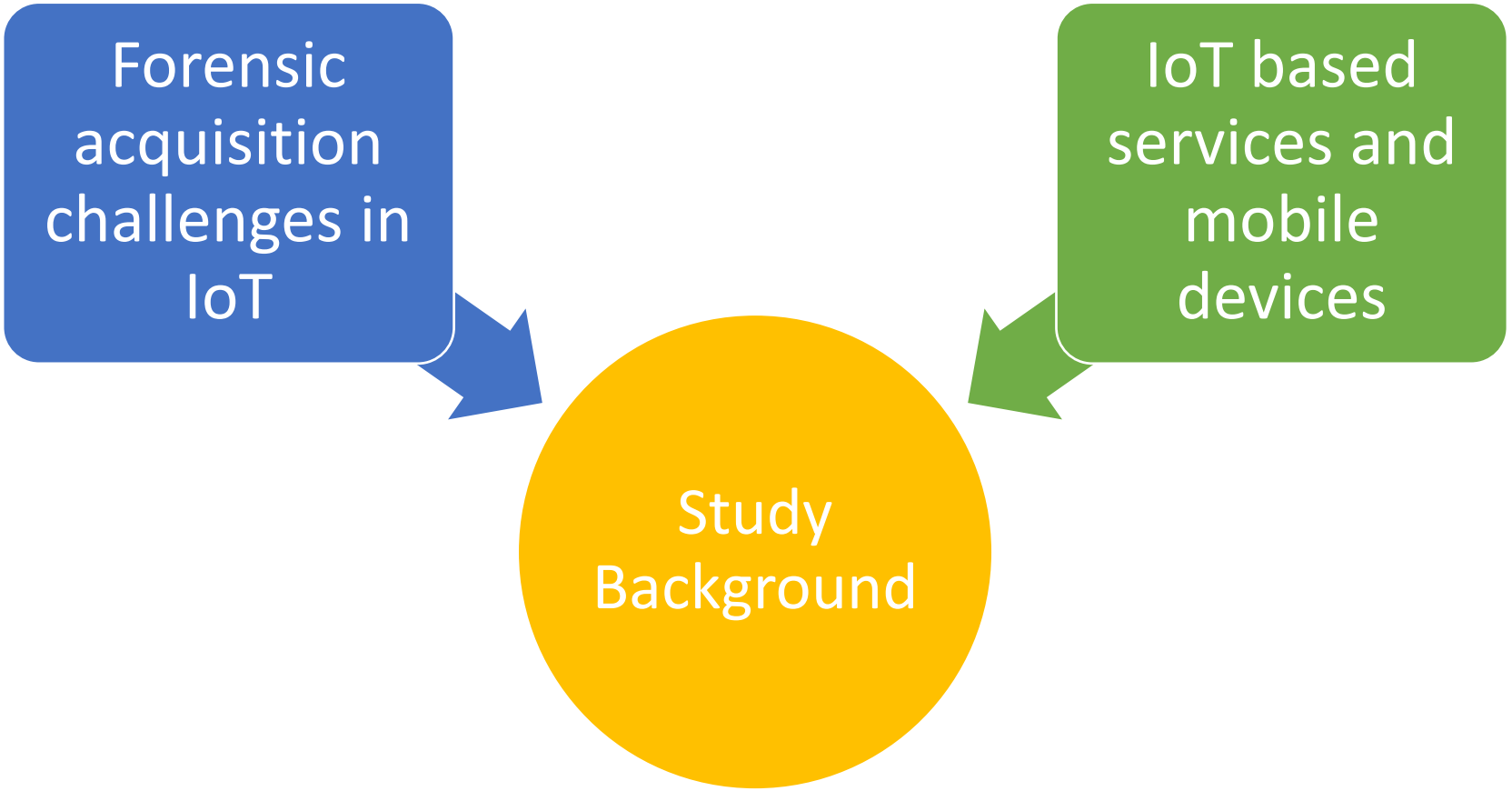
- The huge amount of data generated by and resides on both IoT devices and servers would present significant evidentiary values connected to cyber-criminal activities.
- Forensic acquisitions - the initial stage in digital forensics phases that involves creating a copy of data (i.e. forensic image) within a defined set.

Global Positioning System (GPS) devices and navigation apps can be used in a court as evidence for road accident cases.

The role of mobile forensics



- Using MaybankPay (mobile payment app) as a case study.
- The role of mobile forensics in facilitating forensic acquisition in the Internet of Things environment.


Forensic acquisition challenges in IoT
IoT based services and mobile devices
Study Background

Forensic acquisition challenges in IoT

- IoT devices :
  - IoT devices comprise various types of devices such as smartphones, wearable devices, and smart televisions.
  - The devices consist of diversity in data formats, interface, protocols, and file systems that would complicate the acquisitions processes as the existing procedures of conventional devices may not fit-for purpose.

Forensic acquisition challenges in IoT

- IoT infrastructure
  - encompasses various computing infrastructures such as distributed, cloud and mobile computing.
  - Digital evidence is therefore may exist and can be acquired from various potential sources across the infrastructure.
  - Involves different digital forensics practices
    - for instance network, cloud and mobile forensics.

Potential Sources of Evidence Artefacts on IoT Ecosystem Layers

IoT ecosystem layers	Potential sources of evidence artefacts	Potential forensic acquisition methods
Things (Example: Desktops, Smartphones, Smart TV Box)	Mobile client artefacts ; hard disks, registry, activity logs	Computer forensics and mobile forensic ; cloud forensics
Communication and Network (Example: Servers, data packets)	Network logs ; Audit logs	Network forensics ; Virtual machine forensics
Computing and storage (Example: Cloud storage)	Backup tapes, Backup server ; datacenter artefacts	Computer forensics and mobile forensic ; cloud forensics
Application and Services (Example: Web-based apps, mobile apps)	System files artefacts, browser artefacts ; accessed files, database files	Computer forensics and mobile forensic ; cloud forensics ; browser forensics

Other related work

- Researchers have also examined evidence of interest in IoT devices and showed varied evidence types were recovered.
  - Smart watch: Baggili et al. [8] recovered evidence artefacts from smart watches such as calendar, contacts, and fitness data.
  - Smart home technology: Badenshop et al. [26] have undertaken the extraction and analysis of non-volatile memory of the Z-Wave transceiver and identified key artefacts such as Home ID, pairing log, and protocol information table.
  - A digital evidence taxonomy model: Razak et al. [27] demonstrated digital evidence taxonomy model for mobile health IoT-based applications can be acquired from three layers that are mobile devices, browser and network.

IoT Based Services and Mobile Devices

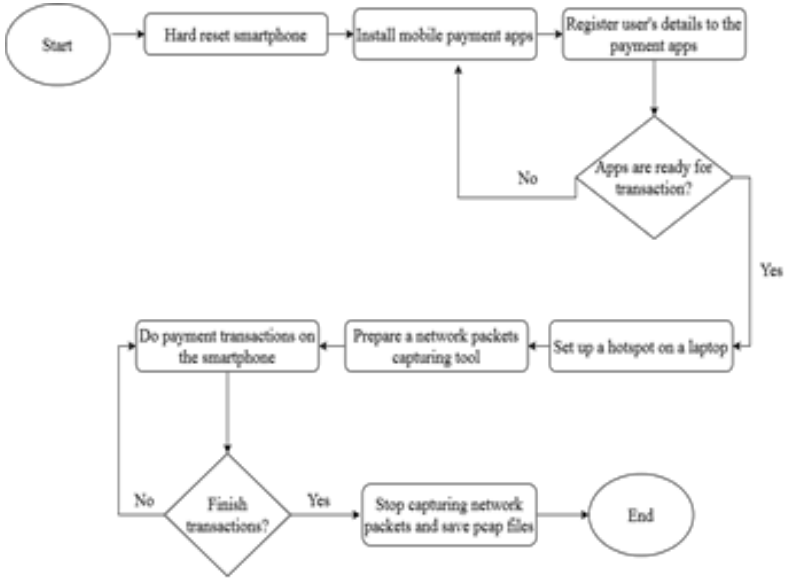
- One example of computing technology is the Near Field Communication (NFC) that can be incorporated into a mobile device which enables the plug and play of IoT connectivity infrastructure.
- NFC is derived from the existing communications technology standard, Radio Frequency Identification (RFID), as a set of standards allowing low-power wireless links to transfer small amounts of data from one device to another, securely and at very short range

Example

- **MaybankPay**
  - is a mobile wallet application (app) from the Malaysian Bank Berhad (Maybank).
  - The app enables users to enroll their credit, debit & prepaid cards in their NFC-enabled mobile devices.
  - Contactless payment - users need to tap mobile devices which act as a gateway for contactless payment onto existing Visa Paywave terminals at merchants' store.

Experimental Setup

- A series of controlled experiments were undertaken to demonstrate the role of mobile forensics in examining the recovered data remnant of IoT based application. MaybankPay, a mobile payment app in Malaysia was applied as the IoT based app and an Android smartphone acted as the IoT device. At the time of research, MaybankPay has reached more than 100 000 downloads on Google PlayStore.
- We adopted the approaches of Ab. Rahman et al. [6] as a guide of our experimental design.



Tools	Function
HTC Butterfly	An enabled NFC smartphone (Android version 4.4.2).
Magnet Acquire; Adb command	Used to acquire physical and logical images from the smartphone.
Autopsy; FTK Imager	Analyze the forensic image
Wireshark	Capture network packets
Network Miner	Analyzing network packets
mHotspot	Setting up wireless connection

Dataset

- A predefined dataset was created for our preliminary study that consists of 15 payment transactions conducted using MaybankPay.
- Four common payment simulation transactions of users on mobile payment were undertaken such as accepted transactions, rejected transactions, add card, and delete card.
- Each of the transaction was conducted with different activities to simulate real-world transactions, as consistent with previous studies such as in mobile cloud storage [6] and in mobile communication apps [11].

Result and discussion

MaybankPay apps' files and database

- represents evidence sources at Things layer of IoT

Network packets metadata

- represent evidence sources at Communication and Network layer of IoT

Examine app files and databases

- App's file: data/com.ionicframework.imxmbbmobile15570.
- App's database:/com.ionicframework.imxmbbmobile155700 /app_database/ - no artefact
- XML files: shared_prefs/InfSharedPreferences.xml/: Users' IP address, Transaction Data History (Date, refId, merchantName, tokenId, cardlast4, tokenLast4 & amount), Registered card, Application version, Mobile number

Metadata of Transactions Record

Transaction	User IP Address	Transaction History	Registered Card	App Version	Mobile No
T1	√	×	×	√	√
T2	√	√	√	√	√
T3	√	×	×	√	√
T4	√	×	×	√	√
T5	√	√	√	√	√
T6	√	×	×	√	√
T7	√	√	√	√	√
T8	√	√	√	√	√
T9	√	√	√	√	√
T10	√	√	√	√	√
T11	√	√	√	√	√
T12	√	√	√	√	√
T13	√	√	√	√	√
T14	√	×	×	√	√
T15	√	√	√	√	√

Rejected transactions (T1, T3, T4, T6 and T14) show no transaction history and registered card.

Accepted transactions present the recorded corresponding metadata of Transaction Data History that includes date, reference id, merchant name, card last 4, token last 4 and amount.

Example of Metadata from Transactions Data History

date	refid	merchantName	cardLast4	tokenLast4	amount
2...18 23:51PM	3080….00526	…-PARIT RAJA	..13	..16	MYR3.50
2...18 10:11AM	3080….11796	…-PARIT RAJA	..27	..16	MYR19.40

- Each transaction denotes its own unique reference ID value in the refid field. Therefore, it can be assumed that the value can be correlated to corresponding transaction at the servers' site, for example servers at payment service provider.

- Other fields such as timestamps, stores name, the 4 digits card and token number, and the involved cost present significant records of transaction that would facilitate forensic analysis in answering of who, what, where, when, why, which, and how a security incident took place.

Contact information

Thank You