An Example of Mobile Forensics

Kelvin Hilton

K319

k.c.hilton@staffs.ac.uk

www.soc.staffs.ac.uk/kch1

Objectives

- The sources of evidence
  - The subscriber
  - The mobile station
  - The network

Introduction

Some GSM Facts

- Nearly 1 billion subscribers worldwide
- Estimated that worldwide mobile phone fraud will reach $40 billion dollars
- US Law enforcement agents have found that 80% of drug dealers arrested in US using cloned mobile phones
- Ironically, Pablo Escobar the top Columbian drug dealer was tracked down by monitoring his mobile phone activity
- Two aspects relevant to a Forensic Analyst
  - Has the phone been used for a criminal act?
  - Can the phone be use to secure a conviction?

Some GSM Facts

- How many GSM handset manufacturers are there?
- The European Telecommunication Standards Institute (ETSI) regulates the GSM standard (all 4000 pages of it!)
- Any equipment used on a GSM network has to have approval by the ETSI
- All MS's are independent from any network

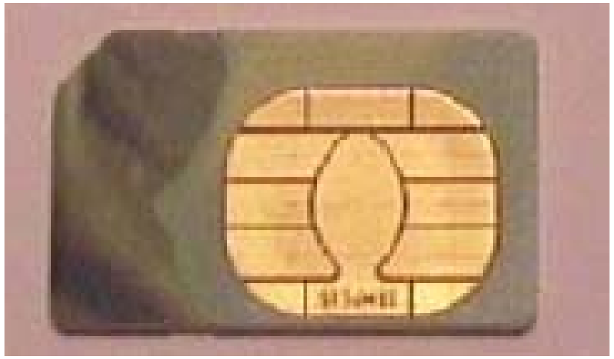
Need to Understand

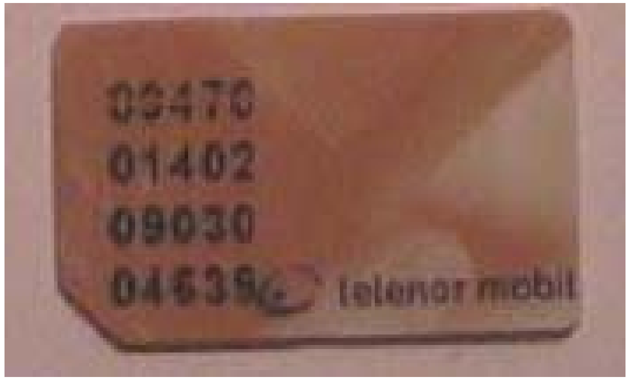
- How do we separate the subscriber and the equipment identities?
- What evidence can be obtained from the network entities?
  - Mobile Station
  - The Subscriber Identity Module (SIM)
  - The core network
- What tools can be used to extract the data without prejudice?
- The separation between the subscriber as a and the equipment as network entities
- How to present the evidence

The Subscriber

How to Identify a Subscriber

- Every mobile subscriber is issued with a smart card called a Subscriber Identity Module (SIM)
- As physical evidence the SIM provides details printed on the surface of;
  - Name of the Network Provider
  - Unique ID Number





Electronic Access to the SIM

- Every SIM can be protected by a Personal Identification Number (PIN)
  - Set at point of manufacture
  - Can be changed by the Subscriber
  - Four digit code
  - Usually 3 attempts before phone is blocked
- Bypassing the PIN requires the Pin Unblocking Key (PUK)
  - 8 digit code
  - Set by manufacturer
  - Maximum 10 attempts before phone is peefore phone is permanently blocked

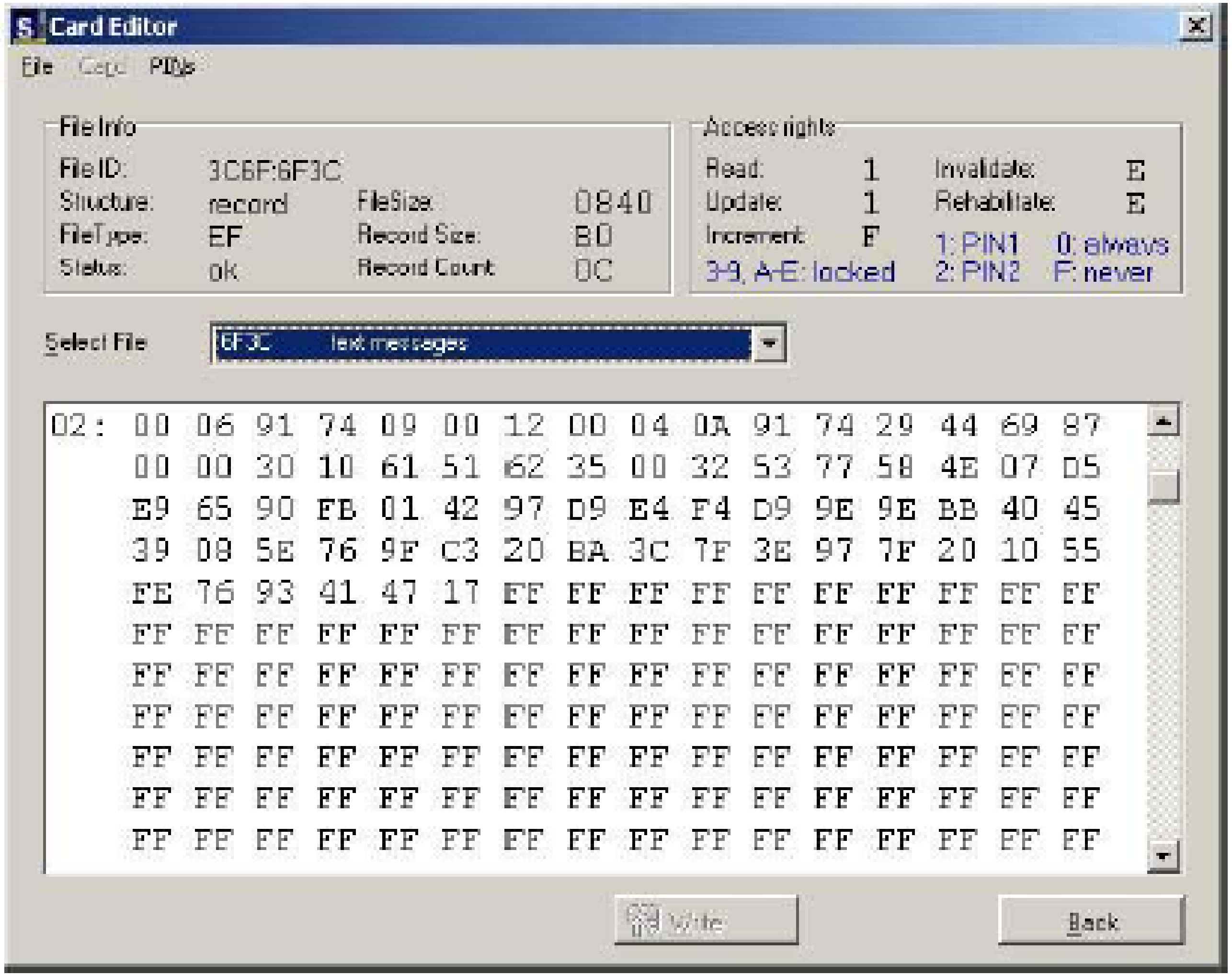
What Can Be Extracted From A SIM?

- As SIM is a smart card it has
  - A processor
  - Non-volatile memory
- Processor is used for providing access to the data and security
- GSM standard 1111 specifies the physical and logical properties of access mechanism for the SIM
- To access the data need;
  - Standard smart card reader
  - SIM access Software
- Data stored in binary files

What Can Be Extracted From A SIM?

- Ideally an Analyst would download an image of the contents and compute a hash value of the contents as a means of validating originality of content
- At present files are downloaded *traditionally*
  - Software
    - Sim Manager Pro
    - ChipIt
    - SimScan
  - Cards4Labs only available to Law Enforcement Agencies
    - Produces a text report of content rather than downloading

An Example of Raw SIM Data



File Info

File ID: 3C6F:6F3C
Structure: record FileSize: 0840
FileType: EF Record Size: B0
Status: ok Record Count: 0C

Access rights

Read: 1 Invalidate: E
Update: 1 Rehabilitate: E
Increment: F
1: PIN1 0: always
2: PIN2 F: never
3-9, A-E: locked

Select File: 6F3C text messages

```
02:  00 06 91 74 09 00 12 00 04 0A 91 74 29 44 69 87
     00 00 30 10 61 51 62 35 00 32 53 77 58 4E 07 D5
     E9 65 90 FB 01 42 97 D9 E4 F4 D9 9E 9E BB 40 45
     39 08 5E 76 9F C3 20 BA 3C 7F 3E 97 7F 20 10 55
     FE 76 93 41 47 17 FF FF FF FF FF FF FF FF FF FF
     FF FF FF FF FF FF FF FF FF FF FF FF FF FF FF FF
     FF FF FF FF FF FF FF FF FF FF FF FF FF FF FF FF
     FF FF FF FF FF FF FF FF FF FF FF FF FF FF FF FF
     FF FF FF FF FF FF FF FF FF FF FF FF FF FF FF FF
     FF FF FF FF FF FF FF FF FF FF FF FF FF FF FF FF
     FF FF FF FF FF FF FF FF FF FF FF FF FF FF FF FF
```

** Sample extracted using Sim Manager Pro (www.txsystems.com)*

What Can Be Extracted From A SIM?

- 29 files stored on a SIM
- Most have evidentiary value
  - However, most provide network rather than subscriber data
  - Most network data is not visible to the user of the SIM via the MS
  - Validity of network data can easily be corroborated via network operator
- We shall concentrate on the user data files

Location Information File

File	Purpose	Size
LOCI	Location Information	11 bytes

- The bytes 5-9 of the LOCI contain the network Location Area Identifier (LAI) code
- Network Operator specific
- This data is retained when the MS is powered down
- Updated as MS moves from one location to another
- Analyst can determine which location the MS was present in when last used
- Location Areas can contain many cells
- LOCI DOES NOT DETAIL WHICH CELL!
- Cell data not stored on SIM

Serial Number

File	Purpose	Size
ICCID	Serial Number	10 bytes

- Integrated Circuit Card Identifier
- Corresponds to the number printed on the surface of the SIM
- Identifies the SIM

Subscriber Identifier

File	Purpose	Size
IMSI	Subscriber ID	9 bytes

- International Mobile Subscriber Identity
- As stored in the HLR/VLR's on the networks
- Unique ID for every subscription on the Operator's network

Phone Number

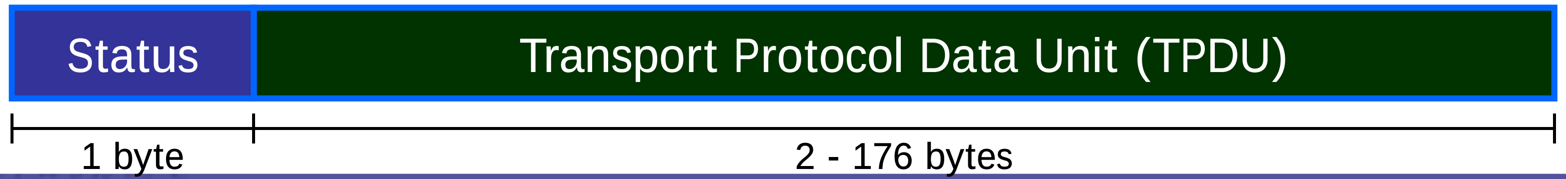
File	Purpose	Size
MSISDN	Phone Number	variable

- Mobile Station International ISDN number

Text Message Data (SMS)

File	Purpose	Size
SMS	The text messages	n * 176 bytes
SMSP	Message parameters	variable
SMSS	Status of the message	variable

- Short Message Service is a popular communication method
- Most SIM’s have 12 slots for storing messages
  - Modern MS’s allow storage on the device as well
- Each SMS SIM slot is configured as;



Text Message Data (SMS) - Status

- Status byte values

Value	Interpretation
00000000	Unused
00000001	Mobile terminated message, read
00000011	Mobile terminated message, unread
00000101	Mobile originated message, sent
00000111	Mobile originated message, not sent

- When user deletes a message only the status flag is changed
  - Therefore, providing the message has not been overwritten any message in a slot can be recovered and translated using software

Text Message Data (SMS) - TPDU

- The TPDU consists of the following elements:
  - The ISDN number of the SMS service center
  - The ISDN number of the sender (or recipient, depending on status) of the message
  - Date and time (in seconds) the message was received by the SMS service center, this referrs to the time of the clock at the SMS service center
  - Phonebook number on the MS (ie Inbox, Outbox)
  - The message itself
    - Encoding varies between manufacturers
    - Most common is 7-bit packed as defined by the GSM standard
    - Message is optimised for streaming onto the SIM
    - Unused bytes contain FF hex value

Dialled Numbers

File	Purpose	Size
AND	Short Dialled Numbers	variable

- Most SIMs have up to 100 slots for storing phone numbers
- Binary encoded name/number pair
- When number is deleted the slot is filled with FF hex value so deleted numbers cannot be retrieved forensically
- Slots are allocated in sequence
  - Therefore can forensically analyse if a number between two numbers has been deleted

Dialled Numbers

File	Purpose	Size
LND	Last Dialled Numbers	variable

- SIMs can store up to five of the last dialled numbers
- Binary encoded format
- Most MS manufacturers do not use this feature preferring to implement this feature on the MS calling logs
- NOTE: The SIM does not store received call data

Threats to SIM Data

- Knowledgeable criminals will be aware of the properties of the SIM and thus manipulate them
- Greater threat is that of cloning SIM data for illicit use
  - Two key pieces of data
    - IMSI
    - The data encryption key (Ki)
  - IMSI can be obtained;
    - Directly from the SIM using a scanning software
    - Eaves-dropping on the networks for unencrypted transmission of the IMSI
      - EG at Airports when a roamer registers on a visiting network
  - Ki cannot normally be obtained directly as it is derived from an encryption algorithm stored on the SIM
    - However, if the encryption algorithm is weak then it is possible to feed numbers

Threats to SIM Data

- GSM SIM's can be cloned because authentication protocol has flaw
  - COMP128 is the algorithm used by most operators
  - Problem is that the algorithm is a published standard and it leaks information at every attempt to connect. With sufficient number of challenges to the SIM card enough info can be gathered to deduce the secret key for the SIM
  - Approximately 150000 queries required takes about 8-11 hours with a suitable smartcard reader
  - Called a chosen-plaintext attack
- SimScan software can obtain the Ki electronically but at the risk of damaging the SIM

- Obtaining blank SIMs
  - Cannot reprogram IMSI or Ki data on a SIM card obtained through any other means than direct from the manufacturer

The Equipment

Generic Properties

- All MS’s have to GSM standards on how they access and communicate with the network and SIM card
- Every MS has a unique ID called the International Mobile Equipment Identity (IMEI)
- Everything else is manufacturer dependent
  - File system
  - Features
  - Interface
  - Etc.
- Have to request the SIM PIN if activated
- May have optional MS PIN
  - No way of bypassing the MS PIN without specialist hardware provided by manufacturer

Accessing MS Data

- Stored in flash memory
- Forensic Investigator must ensure the retrieval of data without alteration!
  - Imaging
    - As most MS's now have flash upgradeable Operating Systems, etc. this is usually a straightforward process
    - However, manufacturer's reluctant to provide access to the tools to achieve this
    - Independent tools known as **Flashers** are available for most mainstream MS's but have no recognised legal status
  - Data suites
    - Provided by manufacturers
    - Allow access to SMS/MMS, call registers, phonebooks, etc. as stored on phone
    - Cannot access memory directly
  - Photographing screens!

Accessing MS Data

- Stored in flash memory
- Forensic Investigator must ensure the retrieval of data without alteration!
  - Imaging
    - As most MS’s now have flash upgradeable Operating Systems, etc. this is usually a straightforward process
    - However, manufacturer’s reluctant to provide access to the tools to achieve this
    - Independent tools known as **Flashers** are available for most mainstream MS’s but have no recognised legal status
  - Data suites
    - Provided by manufacturers
    - Allow access to SMS/MMS, call registers, phonebooks, etc. as stored on phone
    - Cannot access memory directly
  - Photographing screens!

MS Data

- Very much dependent on the model, may include;
  - IMEI
  - Short Dial Numbers
  - Text/Multimedia Messages
  - Settings (languge, date/time, tone/volume etc)
  - Stored Audio Recordings
  - Stored images/multimedia
  - Stored Computer Files
  - Logged incoming calls and dialled numbers
  - Stored Executable Progams (eg J2ME)
  - Stored Calendar Events
  - GPRS, WAP and Internet settings

Threats to MS Data

- Tools such as Flashers and Data Suites can be used to directly manipulate MS data
  - Common threat is removing the Service Provider Lock (SP-Lock) limiting the MS to a single networked
  - Changing the IMEI on stolen phones
    - Networks blacklist stolen IMEI’s in the EIR
    - Can also be used to avoid tracing an MS
  - Detecting changes to the IMEI
    - Compare the electronic IMEI with that printed on the inside of the device
- No scientific way to detect if flash memory has been flashed and if so why

The Network

Network Operator Data

- The Network Operators can provide detailed data on calls made/received, message traffic, data transferred and connection location/timing
- The HLR can provide;
  - Customer name and address
  - Billing name and address (if other than customer)
  - User name and address (if other than customer)
  - Billing account details
  - Telephone Number (MSISDN)
  - IMSI
  - SIM serial number (as printed on the SIM-card)
  - PIN/PUK for the SIM
  - Subscriber Services allowed
- Not necessarily for pre-pay!

The Call Data Records (CDR’s)

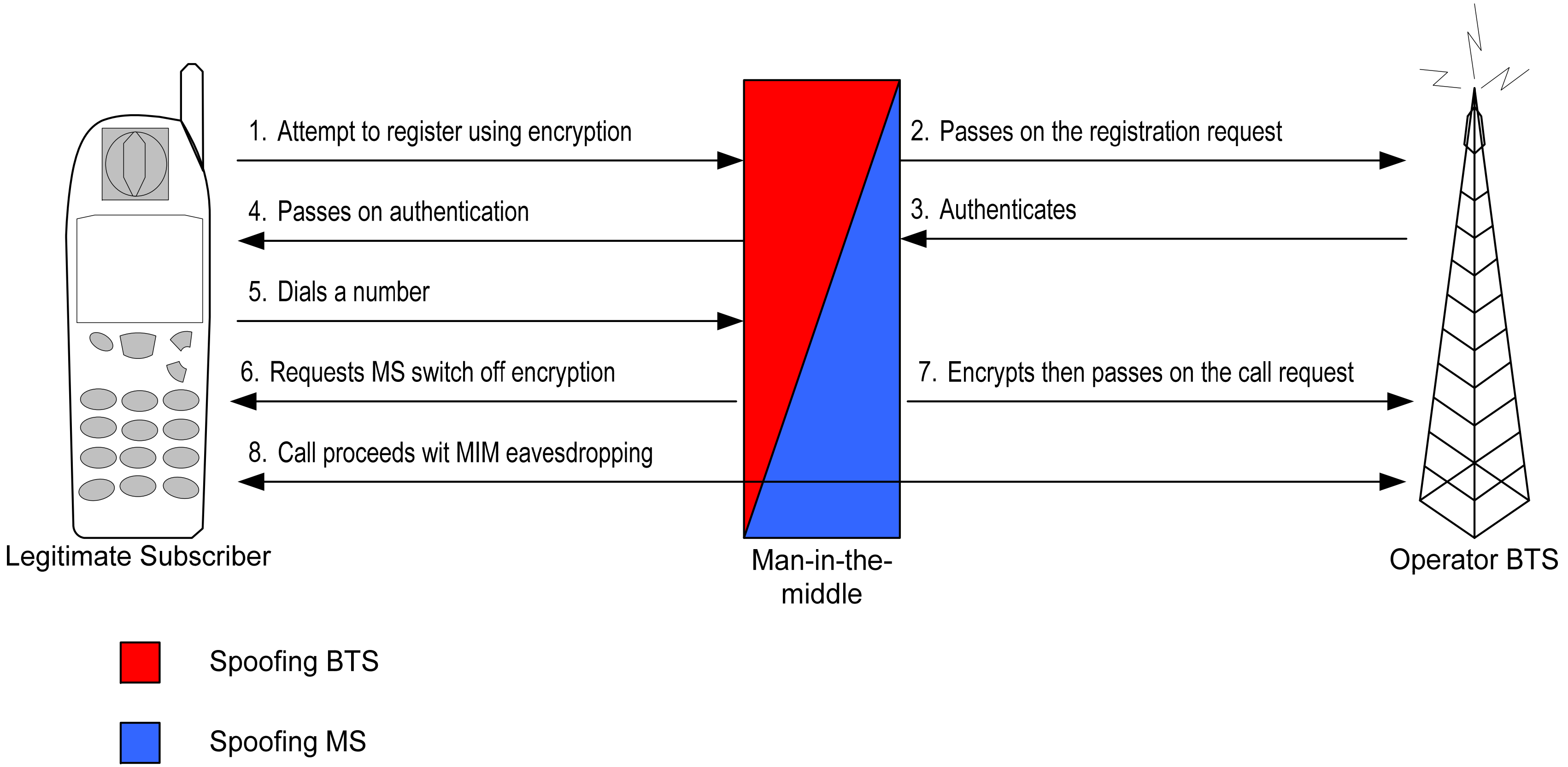
- Produced in the originating MSC transferred to the OMC
  - Every call
  - Every message
- Each CDR contains;
  - Originating MSISDN
  - Terminating MSISDN
  - Originating and terminating IMEI
  - Duration of call
  - Type of Service
  - Initial serving Base Station (BTS) (not subsequent BTSs after handover)

Tracing an MS

- BTS data can be analysed to pin point cell location (up to 35km)
  - All cells have a fixed transmission radius which may be much less than the maximum
- Upgraded GSM networks (2G+) have an extra node specifically for detecting location (legislative requirement in US)
  - Uses base station triangulation
  - 0.2 – 10km accuracy
- A persons location data is stored in the HLR for an arbitrary amount of time after an MS is switched off

Threats to Network Operator

- GSM not immune to interception
- It is possible for the network to order the MS to switch of encryption at times of high loading
  - This signal can be spoofed using a man-in-the-middle attack



1. Attempt to register using encryption
2. Passes on the registration request
3. Authenticates
4. Passes on authentication
5. Dials a number
6. Requests MS switch off encryption
7. Encrypts then passes on the call request
8. Call proceeds wit MIM eavesdropping

🟥 Spoofing BTS

🟦 Spoofing MS

Summary

- The sources of evidence
  - The subscriber
  - The mobile station
  - The network

Questions?