Karel van der Lecq
karel.vanderlecq@adaptivemobile.com
Faaez Burney
Faaez.burney@adaptivemobile.com

Something has been worrying us,,,

If Mobile Network Attackers…

1. **are sophisticated/intelligent/well-paid**
2. **know they are being sometimes blocked and react to it**

- Why are we not seeing more types of new attacks over mobile core networks?

- Especially as many SS7/Diameter security & firewall deployments are not actively engaged in operational investigation & research
  - Antibiotics analogy,

- What is being missed?

Result – Project Kenobi (1) – These are the attacks we are looking for..

AdaptiveMobile **Threat Intelligence Unit** begun project to identify previously undetected suspicious activity

- Investigate new or novel behaviour from malicious sources globally
- Look for unexpected behaviour within customer and non-customer networks
- Focus on what the attackers could be doing

For this, we used our SIGIL (Signalling Intelligence Layer) Platform

Assumptions – Project Kenobi (2)

- Attackers:
  - Have expert knowledge of 3GPP standards
  - Have all GSMA documents
  - Can only do what is possible
  - Are successful
  - Know that most operators don’t actively investigate unknowns, will do ‘just enough’

Introducing Simjacker

- Large scale espionage attack on mobile network subscribers in multiple countries
- Thousands of subscribers having location and device information obtained over at least a year
- Exploits vulnerability that allowed almost every single mobile devices in affected operators to be open to mobile control, without any user interaction
- Vulnerability believed exploited by professional surveillance company on behalf of a nation-state
- Surveillance company actively testing new variants of the attack and new attacks,
- Simjacker is arguably the most sophisticated attack ever seen over mobile core networks. Almost ‘Stuxnet-like’ leap in sophistication from previous attacks

High-level view of typical SIMJacker Attack

2 Stages:

1. **Attack Stage:** ‘Attack Message’ is sent from Malicious Handset or VASP servers to victim phones
   – ‘Attack Message’ are SIM Toolkit Messages

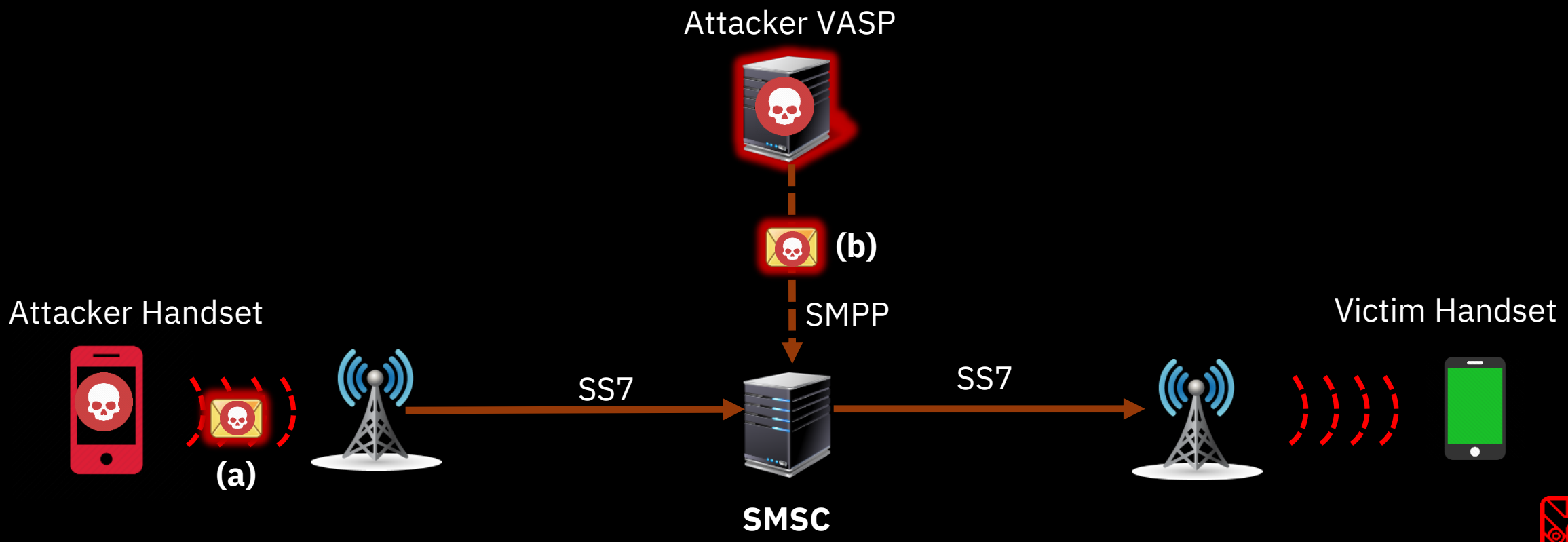
2. **Exfiltration Stage:** The Attack Message executable instructs the SIM Card to request Location and IMEI from the Handset, and send the Location and IMEI from the Handset in a SMS
   – This is called the ‘Data Message’

• ‘Data Message’ is sent from the Victim Handset to a Recipient Number,

• This activity is not noticeable by the Victim – no indication on the handset

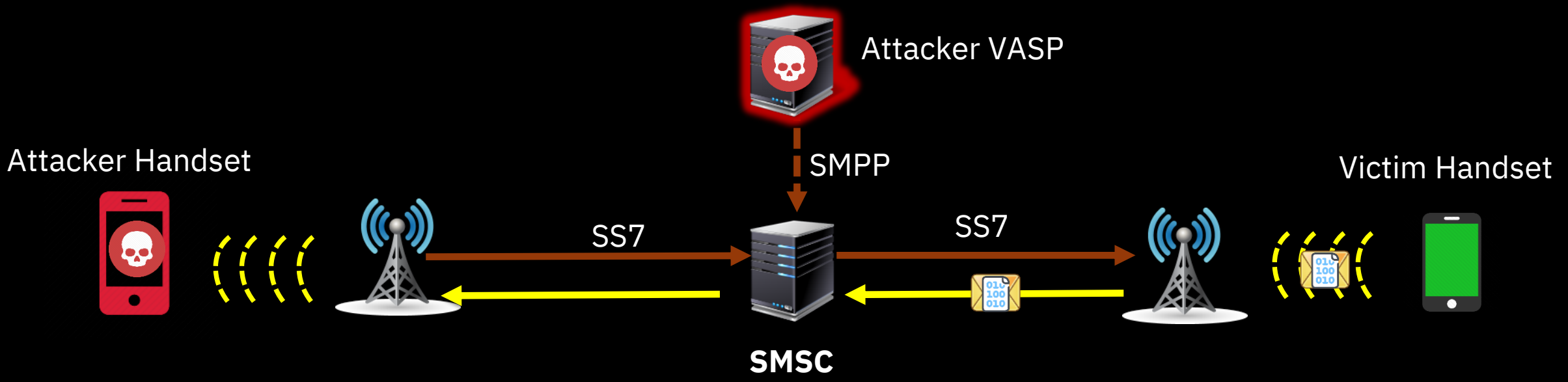
Step 1: Attack Stage: How the Attack Happens

‘Attack Message’ is sent to Victim Handset,



Step 2: Exfiltration Stage: How the data is sent back

‘Data Message’ is sent from Victim Handset,
to Attacker Handset



Demo of the attack: Location Tracking

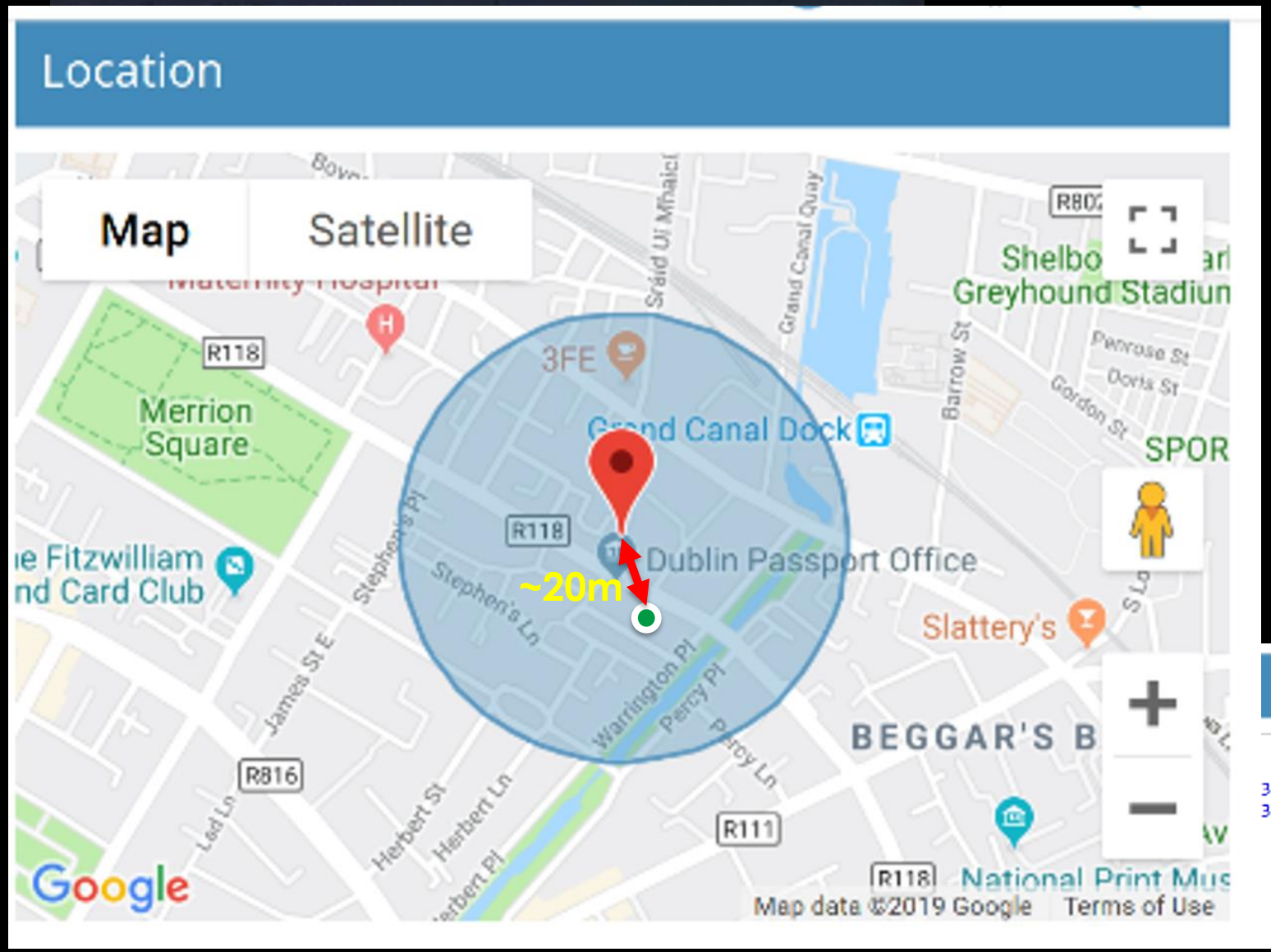
Demo for FASG#15 Delegates

Demo of the attack: Location Tracking – Note, ~5 second delay removed


```
File  Edit  View  Search  Terminal  Help

(simjacker)  $>
```

Location



72f210 0bd5 b73f 000c

272 : MCC Ireland
01 : Vodafone Ireland
0bd5 : LAC (3029)
b73f : CellId (46911)

*Note: VF Ireland are the roamed-to operator for the vulnerable SIM, they are **not** the vulnerable operator*

How the attack works

a) Attacks exploit ability to send SIM Toolkit Message

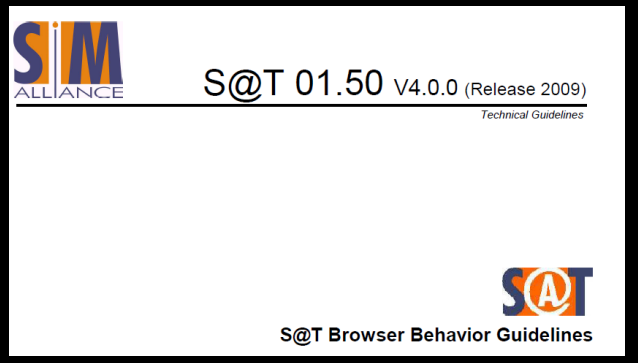
b) Attacks exploit the presence of S@T Browser on the SIM card for vulnerable subscribers

The Attack messages use the S@T Browser functionality-

1. trigger STK **Proactive Commands** that are sent to the handset
2. Responses to Proactive Commands are sent back from the handset to the SIM card and stored
3. Once all information is retrieved, another Proactive Command is used to send information externally via SMS

What is the S@T Browser?

- Stands for SIMalliance Toolkit Browser
- S@T browser specifications were developed by the SIM Alliance. Specifications include:
  - S@T 01.00 – S@T Bytecode,
  - S@T 01.20 – S@T Session Protocol
  - S@T 01.23 – S@T Push Commands
  - S@T 01.50 – S@T Browser Behaviour Guidelines
- Aim of these specifications was to allow a
  - thin client on a SIM
  - to run applications in the SIM
  - using commands and content downloaded OTA via SMS or BIP from an external server.
- Utilise STK/OTA mechanisms.
- Last update 2009 (prior to this vulnerability).



Main role of the S@T browser is to act as an **execution environment for STK commands**.

SIMJacker Classification – Spyware?

- If Malware is malicious software

- And Software is a set of instructions to be executed

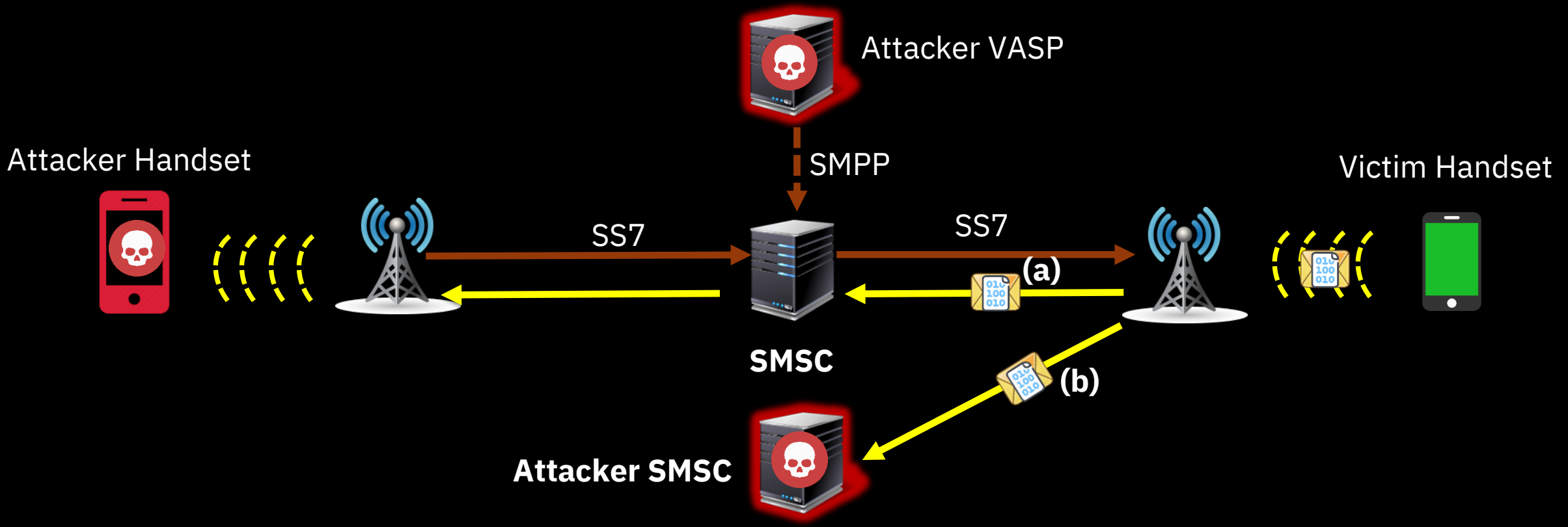
- Then SIMJacker, being a set of S@T and STK commands to be executed by the S@T Browser, is malware
  - (specifically spyware)

SIMJacker would be the first known, spyware spread by SMS in the wild

- excluding SMS which contain links

Note: open to corrections on this

Evading/modifying (1) : Exfiltration Method of Data Message



Evading/modifying (2) : SIMJacker SMS Packet Encoding

Constant Changing of

- DCS
- PID
- UDH
- UserData

Also Use:

- Reserved Values,
- REDACTED,
- Multi-part messages,
- Omitted values
- Corrupted/non-standard parameters
- Others

TP-MTI	localValue	TP-DCS
SMS-SUBMIT	mo-forwardSM	33
SMS-SUBMIT	mo-forwardSM	34
SMS-SUBMIT	mo-forwardSM	35
SMS-SUBMIT	mo-forwardSM	36
SMS-SUBMIT	mo-forwardSM	37
SMS-SUBMIT	mo-forwardSM	38
SMS-SUBMIT	mo-forwardSM	39
SMS-SUBMIT	mo-forwardSM	40
SMS-SUBMIT	mo-forwardSM	41
SMS-SUBMIT	mo-forwardSM	42
SMS-SUBMIT	mo-forwardSM	43
SMS-SUBMIT	mo-forwardSM	48
SMS-SUBMIT	mo-forwardSM	49
SMS-SUBMIT	mo-forwardSM	50
SMS-SUBMIT	mo-forwardSM	51
SMS-SUBMIT	mo-forwardSM	52
SMS-SUBMIT	mo-forwardSM	53
SMS-SUBMIT	mo-forwardSM	54
SMS-SUBMIT	mo-forwardSM	55
SMS-SUBMIT	mo-forwardSM	56
SMS-SUBMIT	mo-forwardSM	57

Evading/modifying (3) : Information Retrieved

Normal Information Retrieved in Location Retrieval Attack:

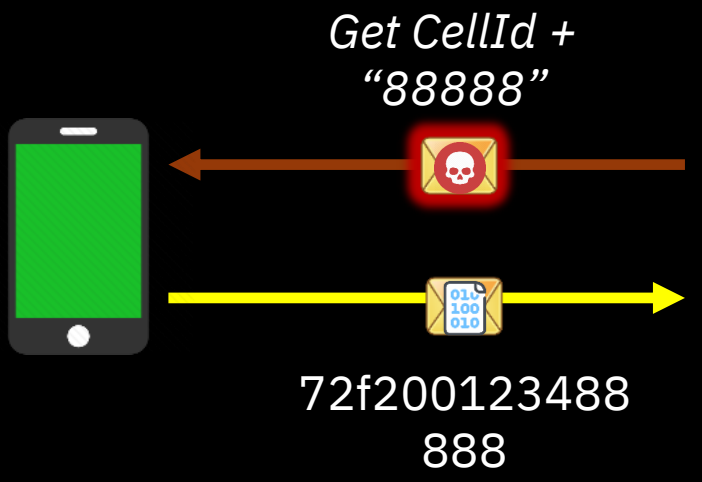
- Cell-ID and/or
- IMEI

However **Filler/Random Bits** are specified in the Attack Message to insert into response Data Messages.

  - Can be multiple instances of these

Order of response Data Message can be varied

  - *IMEI, FILLER, CELLID*
  - *IMEI, FILLER, CELLID, FILLER*
  - *IMEI, CELLID, FILLER*
  - *IMEI, CELLID*
  - *IMEI, FILLER*
  - *CELLID, FILLER*
  - *IMEI, FILLER*
  - *Etc*



Evading/modifying (4) : Other Variations

- Internal Structure of SIMJacker Message
- Corrupted Attack Message Encoding
- REDACTED
- Source Addresses
- REDACTED
- S@T Push Type
- Entry Network points
- Additional STK Commands
- Recipient Numbers
- Etc, etc – there are many more

Attackers are very, very good at evading/modifying

- **Observed several hundred variants in main attack type, millions of variants possible**
  - Multiple Reasons for this
- **Bad news: Filtering on SMS interface is not just a set of SMS parameters that you set once and walk away!**
  - You need to monitor and block on specific header + binary substrings that will change over time

Additional Information on who is Vulnerable

- We know Operators in 3 countries actively targeted
  - Observed others being tested

- We have detected operators in at least 30 countries actively using S@T Browser Technology
  - However, we are finding more and more **other** operators having a subset of SIMs using the technology

- Also relies on specific logic to be set in the SIM Service Table (EF_{SST})
- The issue is that in affected operators,
  - SIM cards do not check origin of messages that use the S@T Browser
  - SIMs allow Data Download via SMS

Other types of attacks are possible using S@T Browser!

What else could be possible using S@T Browser

- There are Multiple PROACTIVE UICC commands, which could be executed by the S@T Browser, they include:
  - PLAY TONE
  - SEND SHORT MESSAGE
  - SET UP CALL
  - SEND USSD
  - PROVIDE LOCAL INFORMATION
    - *LOCATION INFORMATION, IMEI, BATTERY, NETWORK, LANGUAGE, etc*
  - POWER OFF CARD
  - RUN AT COMMAND
  - SEND DTMF COMMAND
  - LAUNCH BROWSER
  - OPEN CHANNEL
    - *CS BEARER, DATA SERVICE BEARER, LOCAL BEARER, UICC SERVER MODE, etc*
  - SEND DATA
  - GET SERVICE INFORMATION
  - SUBMIT MULTIMEDIA MESSAGE
  - GEOGRAPHICAL LOCATION REQUEST

What other attacks are possible

- **Many Fraud Types:**
  - Dialing of PRNs, sending SMS/MMS to short codes, Steering of Roaming etc.
- Location Tracking
- Denial of Service
- Eavesdropping
- Misinformation
- (Potential) Call interception

Effect of Blocking Simjacker SMSs

- Extensive Testing by Attackers

As well as that, there is a separate ‘division’ who are actively experimenting to extend SIMJacker vulnerability use,

Observed Attackers:

- *REDACTED,*
- *Set up calls,*
- *Send USSD commands,*
- *REDACTED,*
- *Open up specific web pages*
- *REDACTED (via **AT Commands**)*
- *others*

Big Question: Who is doing this and why

SIGIL Dashboard

- Using SIGIL (Signalling Intelligence Layer) , can correlate Simjacker sources with known malicious threat actors.
  - As a result can say with high degree of certainty the source is a large surveillance company, which has **nation-state** customers. with very sophisticated abilities in both signalling and handset exploits

Simjacker is designed as a ***next generation*** mobile core network attack, to obtain sensitive information and control devices in operators who

- 1) do not have active monitoring and
- 2) trust in ‘standard’ security systems

Recommendations (for this vulnerability)

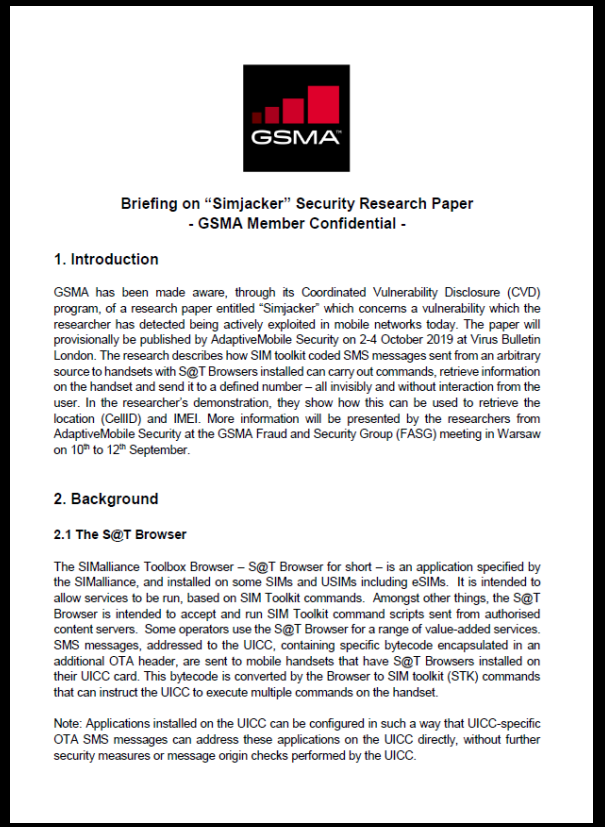
See GSMA CVD Briefing Paper

- **If you use S@T Browser Technology, investigate whether it can be disabled and removed completely**

If can't

1. See if you can update, to improve security model (Minimum Security Level)
2. Network Filter on Messaging Level

NB: If you do attempt filtering, you will need to constantly monitor and investigate!



GSMA

Briefing on "Simjacker" Security Research Paper
- GSMA Member Confidential -

1. Introduction

GSMA has been made aware, through its Coordinated Vulnerability Disclosure (CVD) program, of a research paper entitled "Simjacker" which concerns a vulnerability which the researcher has detected being actively exploited in mobile networks today. The paper will provisionally be published by AdaptiveMobile Security on 2-4 October 2019 at Virus Bulletin London. The research describes how SIM toolkit coded SMS messages sent from an arbitrary source to handsets with S@T Browsers installed can carry out commands, retrieve information on the handset and send it to a defined number – all invisibly and without interaction from the user. In the researcher's demonstration, they show how this can be used to retrieve the location (CellID) and IMEI. More information will be presented by the researchers from AdaptiveMobile Security at the GSMA Fraud and Security Group (FASG) meeting in Warsaw on 10th to 12th September.

2. Background

2.1 The S@T Browser

The SIMalliance Toolbox Browser – S@T Browser for short – is an application specified by the SIMalliance, and installed on some SIMs and USIMs including eSIMs. It is intended to allow services to be run, based on SIM Toolkit commands. Amongst other things, the S@T Browser is intended to accept and run SIM Toolkit command scripts sent from authorised content servers. Some operators use the S@T Browser for a range of value-added services. SMS messages, addressed to the UICC, containing specific bytecode encapsulated in an additional OTA header, are sent to mobile handsets that have S@T Browsers installed on their UICC card. This bytecode is converted by the Browser to SIM toolkit (STK) commands that can instruct the UICC to execute multiple commands on the handset.

Note: Applications installed on the UICC can be configured in such a way that UICC-specific OTA SMS messages can address these applications on the UICC directly, without further security measures or message origin checks performed by the UICC.

Recommendations for the Future

- SIMJacker is just the first (known) next generation mobile core network attack
  - We have strong indications of other types of innovative techniques being used
  - These are currently being researched within AdaptiveMobile Security

- We have uncovered huge amounts of testing and optimisation by the attackers, signifying large resources, abilities and high-paying customers.
  - These attackers will not stop

Operators need to:

1. Move away from **tick-the-box security.** FS.11, FS.19, FS.20 were not designed as objectives, they are initial guides, the journey is only beginning
2. Focus on operational security., **continuous after-install investigation** is needed
3. Realise that Attackers will try to and **probably already have** bypassed your firewall,
4. Actively be **researching and improving** their core network security. If you or your vendor just follows the GSMA, its too late, you are wasting your time and money as attackers will bypass you

Some Operators perception of FASG

What do you need to do

- What ongoing investigation and research are you doing on what is being encountered in your network?

Do you know if attacks like SIMJacker or other next generation attacks are happening in your network?

More information/contact details: **simjacker.com**

AdaptiveMobile
Security