AdaptiveMobile Security

Simjacker and DFS

Cathal Mc Daid (CTO)

ITU DFS Webinar – 10th Nov 2020

What is Simjacker

- Simjacker is a vulnerability in SIM Cards that allowed mobile devices in targeted operators to be open to allow specific remotely executed commands, many without any user interaction

- Vulnerability exploited library present on SIM cards called **S@T Browser** , which had access to a subset of **STK commands**.

- Vulnerability was exploited on **tens of thousands** of mobile subscribers from multiple countries: primarily Mexico, but also Colombia & Peru

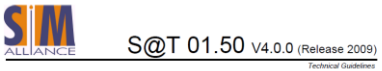
- Attacks led to the location and device information being obtained from these for a period of **one or more years**.

- Vulnerability believed exploited by **professional surveillance company** on behalf of nation-state(s)

- **More info: www.simjacker.com**

What is the S@T Browser?

- S@T == SIMalliance Toolkit Browser
- S@T browser specifications developed by the SIM Alliance. Aim of these specifications was to allow:
  - 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.



- Main role of the S@T browser is to act as an **execution environment for STK commands**.
- Last spec update 2009 (prior to this vulnerability).

Why is/was the S@T Browser vulnerable

<u>No authentication</u> - the S@T Browser will accept any message source for certain messages

- SIM Applications (e.g. S@T Browser) on the SIM Card, have one or more TAR values
- TAR values have a set of Minimum Security Levels (MSL)
- Incoming SIM OTA SMS types, must have security that matches this MSL

Note: full details in paper on www.simjacker.com

4 S@T Browser protocols:

- Pull
- Administration
- Low Priority Push
- High Priority Push

?

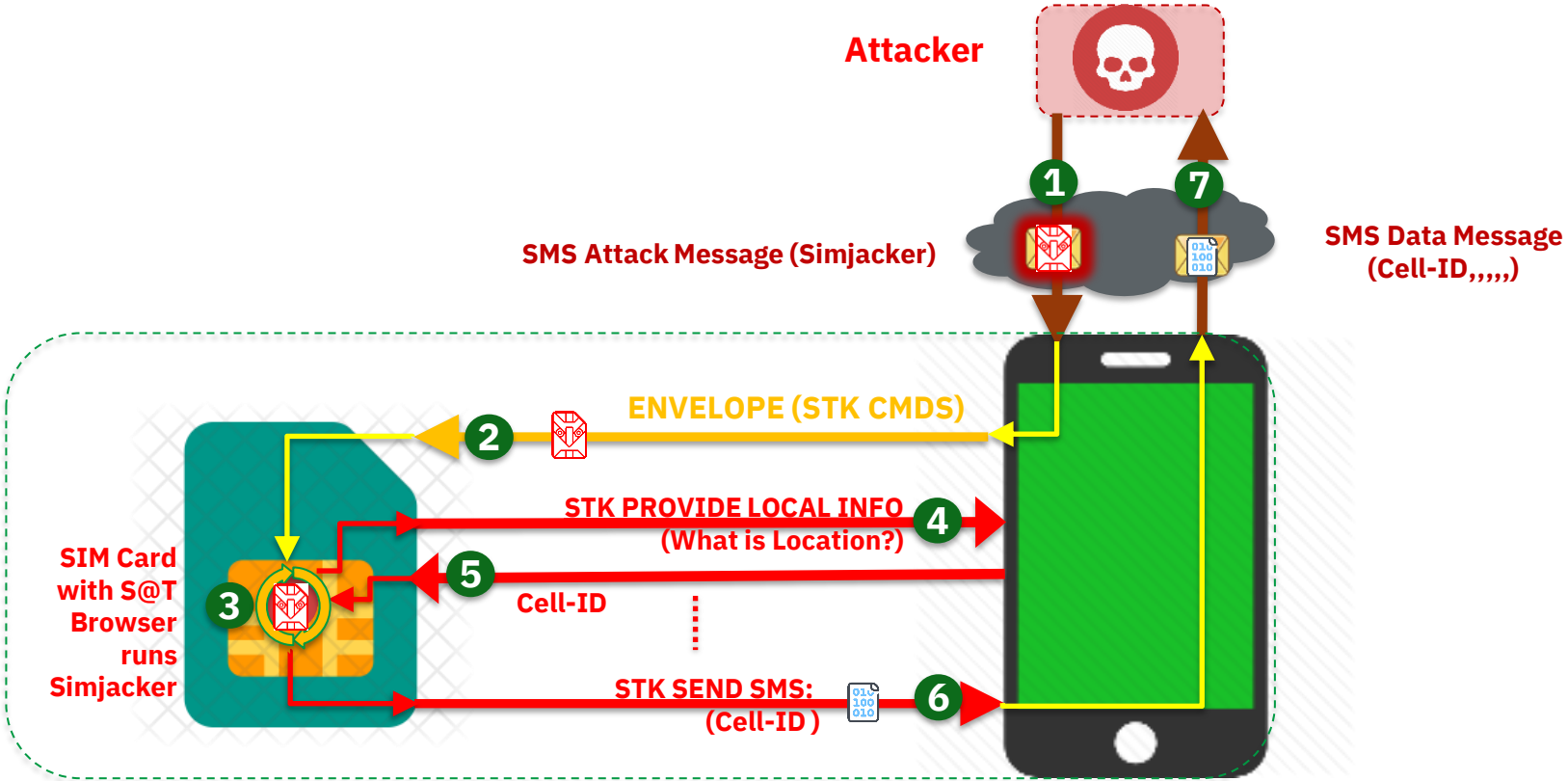
NO SECURITY LEVEL RECOMMENDED FOR PUSH MESSAGES!

5.5.2 Security Levels

The following security levels shall be supported by the S@T browser:

SPI	*KIc*	*KID*	*DESCRIPTION*	*NOTES*
0x0000	0x00	0x00	No security applied	Shall be supported for incoming (MT) and outgoing (MO) messages. This security level is not recommended for Administration protocol.
0x1200	0x00	0xX5	Triple DES Cryptographic Checksum (8-byted MAC); counter higher	Shall be supported for incoming (MT) messages. This security level is not recommended for Pull protocol.

Simjacker Internal Execution (7 steps)



More information: www.simjacker.com

STK Functionality available via S@T Browser

REFRESH
MORE TIME
POLL INTERVAL
POLLING OFF
SETUP EVENT LIST
SET UP CALL
SEND SS
SEND USSD
SEND SMS
SEND DTMF

LAUNCH BROWSER
PLAY TONE
DISPLAY TEXT
GET INKEY
GET INPUT
SELECT ITEM
SET UP MENU
PROVIDE LOCAL INFO
TIMER MANAGEMENT
SETUP IDLE MODE TEXT

Subset of all STK commands, although executing can sometimes be difficult

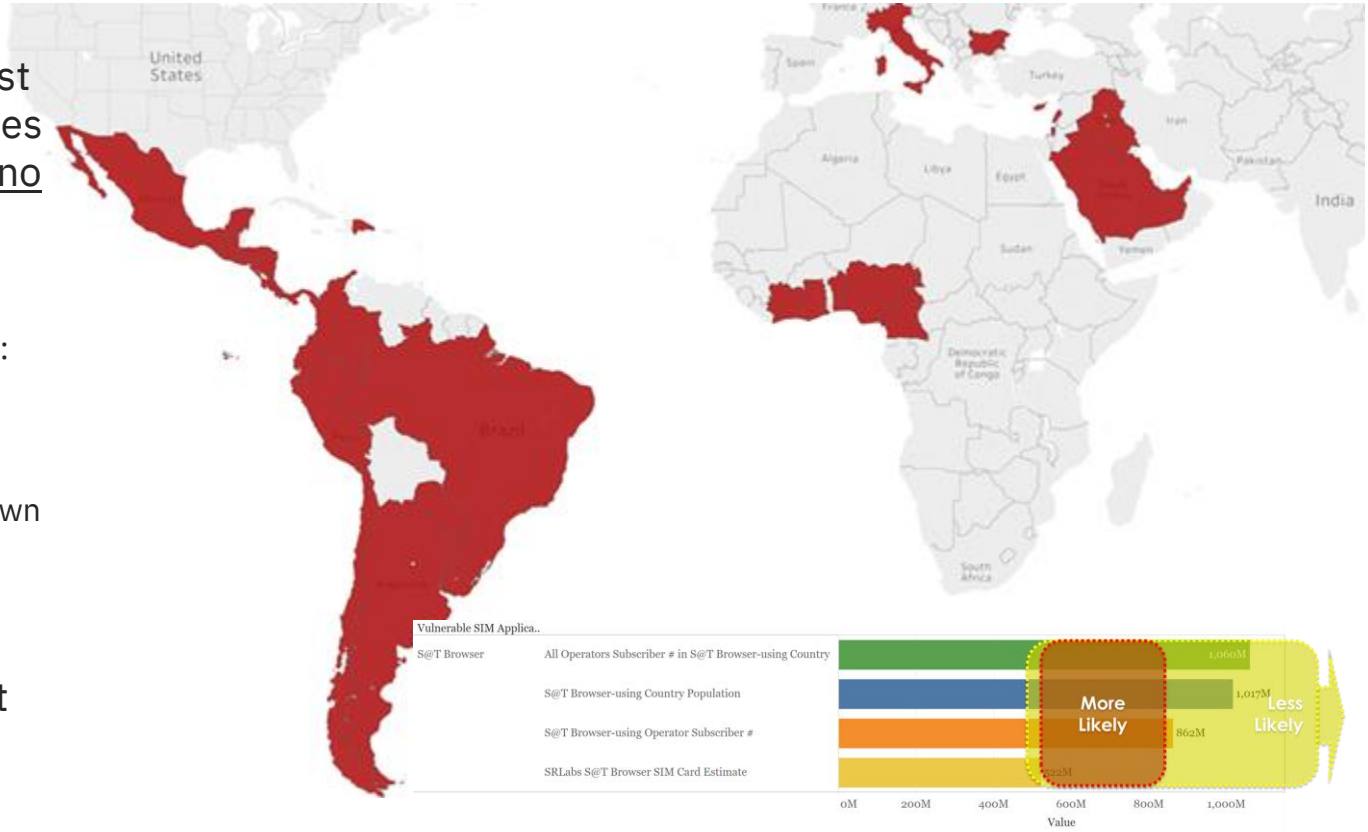
Simjacker Attacks in Real Life

- Highly-sophisticated Attacker, sending S@T Browser Push commands in large volumes for surveillance
- Primarily Targeting Mexican Mobile phone users
  - Thousands of subscribers being targeted per month in Mexico alone
  - Subscribers from Colombia and Peru also targeted (not to same extent)
- Primary goal was to obtain Location information (Cell-ID) and IMEI details
  - Small subset of other activity
- Attacks launched from many SMS sending mobile connected devices,
  - often co-ordinated with global SS7 sources
- Detection and blocking of these attacks requires constant analysis
  - highly dedicated attacker who adapts and changes

Global Usage of S@T Browser

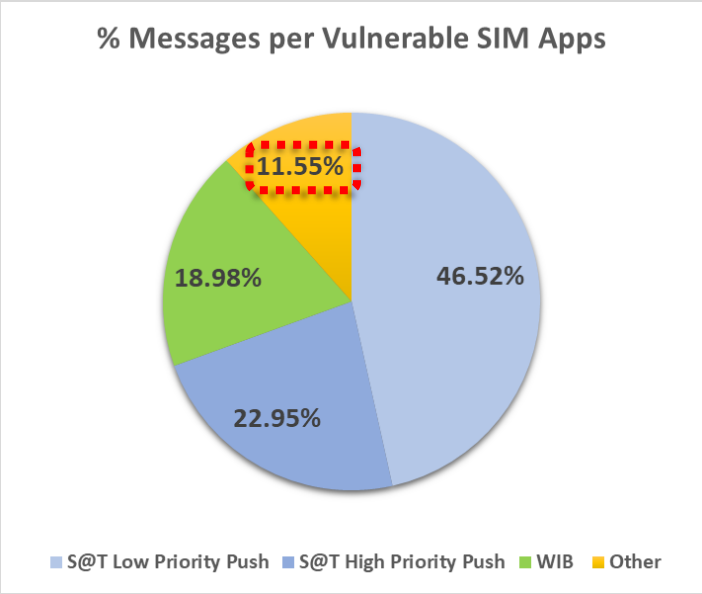
S@T Browser

- At time (Oct 2019) at least 61 Operators, 29 Countries using S@T Browser with no security
  - Best (conservative) estimates of vulnerable S@T Browser SIM Cards : mid to high hundreds of millions of SIM Cards globally are affected
  - Other operators also known but not directly observed
- 1 Year on: still observing vulnerable messaging traffic being sent by most of these



Other potential SIM Card library risks

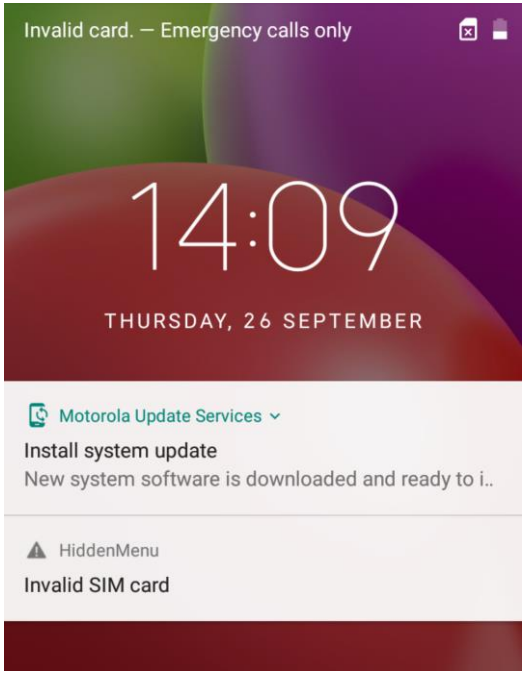
- S@T Browser not the only SIM Card library which has risks
- **WIB Browser**:
  - Wireless Internet Browser, roughly similar to S@T Browser (although no-security is explicitly not recommended)
  - Observed operators with MSL = no security, using WIB technology in real life
  - Not as widely used, scattered globally: 8 Operators, 7 Countries using WIB Browser
  - Volumes vulnerable probably in low hundreds of millions of SIM Cards
- There are potentially other vulnerable SIM Card applications
  - Note: Just because they exist, they may not actually be exploitable
    - No single ‘big’ vulnerable application like S@T Browser or WIB



Possible Simjacker-using Attacks which could Affect DFS applications

Known:

- Denial of Service
- Misinformation – generate SMS from subscriber's handset
- Call/SMS Generation – Premium rate numbers
- Open Browser to malicious/malware site



Potential:

- Execute SS/USSD commands from the victim's Handset ?
  - Use SEND SS & SEND USSD , to execute SS/USSD commands, and execute one way DFS-affecting commands
- Inbound Call Interception ?
  - Via SS/USSD – Enable + Disable Call Forwarding
  - Requires 2 Simjacker SMS + VoIP Box
  - man-in-the-middle attack via VoIP
  - Same method as used in SS7 attacks (RegisterSS Inbound Call interception)
- Others ? (to discuss)

Mobile Operator Ecosystem Changes since discovery

Standards changes:

- GSMA: Information was shared to GSMA via CVD program in June 2019
  - Worked closely for several months with GSMA to disseminate mitigation information within Operator community
  - Public made aware of vulnerability reveal in Sep 2019, (some) Technical detail released to public in Oct 2019
  - GSMA has subsequently worked on creating a best practice paper on Binary Security Messaging
- SIMalliance has updated S@T Browser recommendations

Physical countermeasures:

- Observed: Few operators have increased standard S@T Browser security level on SIM Cards
  - Mainly intermittent Operator users
  - And only after public release (not due to GSMA)
- Instead: Security method of choice seems to be Network filtering
  - This requires constant monitoring to be successful

Recommendations for DFS ecosystem

- Make Sure Mobile Operators know what libraries are present on SIM Cards
  - Easy to say, hard to get right - most Operators have more than one SIM vendor, and multiple variants over time

- If Mobile Operators have vulnerable SIM Card libraries:
  - If you use S@T Browser Technology, investigate whether it can be disabled and removed , or updated to improve MSL
  - If not removed , then Network Filter on Messaging Level
  - Attackers can and will use any path and vary payloads to execute attack

- For DFS - check your mobile telecom assumptions/trust model
  - Constant review of Mobile Network Security – need for Intelligence
  - 4G and 5G still have an 3G SMS pathway – technology is not going away
  - Security only as strong as weakest link

AdaptiveMobile
Security