Introduction – what did we set out to answer

- In VB2019 we revealed the Simjacker attacks

  - Exploit of SIM Card application by Surveillance companies

  - Extracting info from tens of thousands of mobile phone

  - Vulnerability present on several hundred million SIM cards

- The Simjacker Attack used **binary SMS** as a delivery mechanism. Here we look at:

  1. Binary SMS attacks, are there other similar vulnerable applications?
  2. Reaction of industry and attackers to revelation of Simjacker?

THE WALL STREET JOURNAL.

English Edition ▼ | Print Edition | Video | Podcasts | Latest Headlines

Home   World   U.S.   Politics   Economy   Business   Tech   Markets   Opinion   Books & Arts   Real Estate   Life & Work   WSJ. Magazine   S

TECH

Hackers Use Spyware to Track SIM Cards

Telecom security researchers identify 'Simjacker' spyware, used to track SIM cards in Mexico, Colombia and Peru

AdaptiveMobile Security

Simjacker

Simjacker
Technical
Paper

10OCT19-v1.01

More info: www.simjacker.com
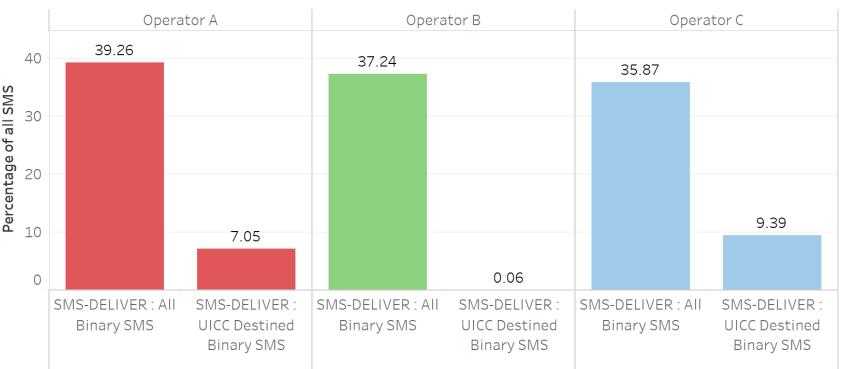
2

Binary SMS: Scale and Identification

Can occupy a large percentage of Mobile Operators traffic

Uses: Missed call notifications, change roaming settings, change SIM Card settings etc

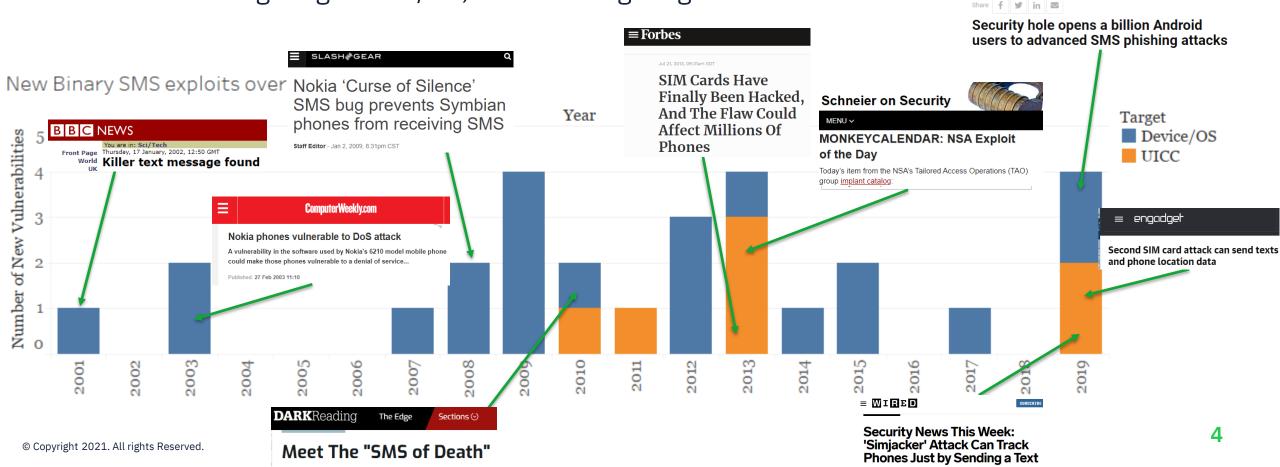(Mostly) 3 GSM-MAP parameters used to Identify Binary SMS
- TP-PID
- TP-DCS
- TP-UDH

Percentage of Binary SMS Type Per Operator

Note: See VB2021 Paper for much more details

3

Malicious uses of Binary SMS

- At least 28 (known) separate vulnerabilities in last 20 years:
  - General Complexity increasing over time
    - Initial were simple DoS
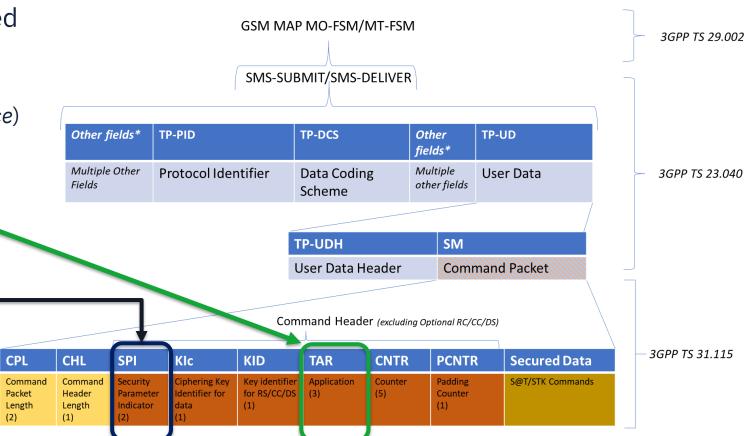 - Most targeting Device/OS, but 25% targeting UICC

4

UICC Application destined Binary SMS – When to Worry

- Simjacker (plus others like WIBattack), used binary messages that were directed to the specific vulnerable UICC (SIM Card) application by the **TAR** value
  - Example TARs (*Toolkit Application Reference*) for S@T Browser
    - 0x505348 (PSH)
    - 0x534054 (S@T)

- Allowed to be executed by the UICC application by the SPI value setting
  - **SPI1* Value (Leftmost 5 bits) == 0 / No security**
    - Note: Ambiguous setting of this in S@T specs was cause of Simjacker vulnerability
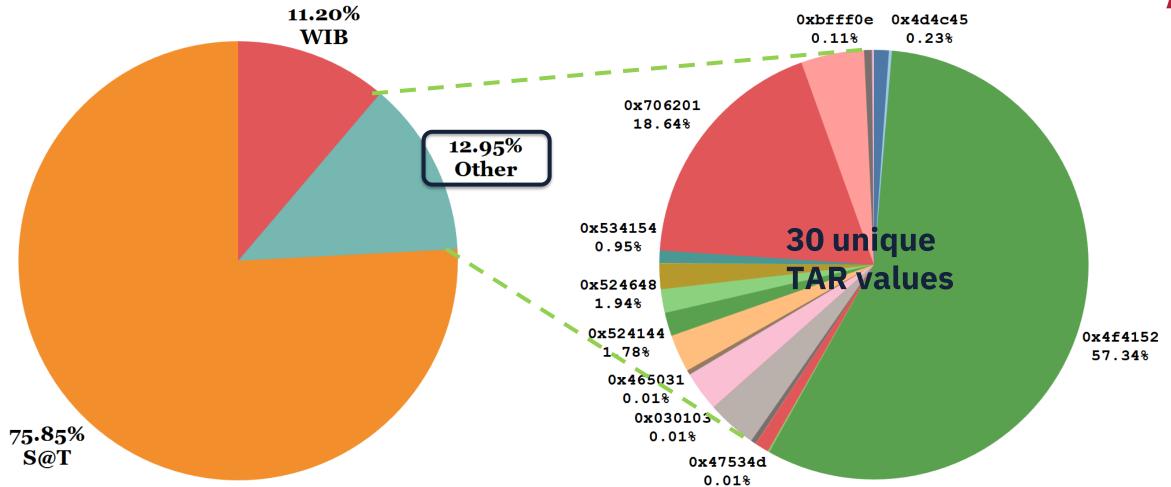
We looked to see were there **more** of these vulnerable SIM Card Applications

GSM MAP MO-FSM/MT-FSM

SMS-SUBMIT/SMS-DELIVER

3GPP TS 29.002

Other fields*	TP-PID	TP-DCS	Other fields*	TP-UD
Multiple Other Fields	Protocol Identifier	Data Coding Scheme	Multiple other fields	User Data

3GPP TS 23.040

TP-UDH	SM
User Data Header	Command Packet

Command Header *(excluding Optional RC/CC/DS)*

CPL	CHL	SPI	KIc	KID	TAR	CNTR	PCNTR	Secured Data
Command Packet Length (2)	Command Header Length (1)	Security Parameter Indicator (2)	Ciphering Key Identifier for data (1)	Key identifier for RS/CC/DS (1)	Application (3)	Counter (5)	Padding Counter (1)	S@T/STK Commands

3GPP TS 31.115

5

Other Vulnerable SIM Card applications

Source: Analysis of UICC destined Traffic to vulnerable TARs from 1 year of global inbound roamers
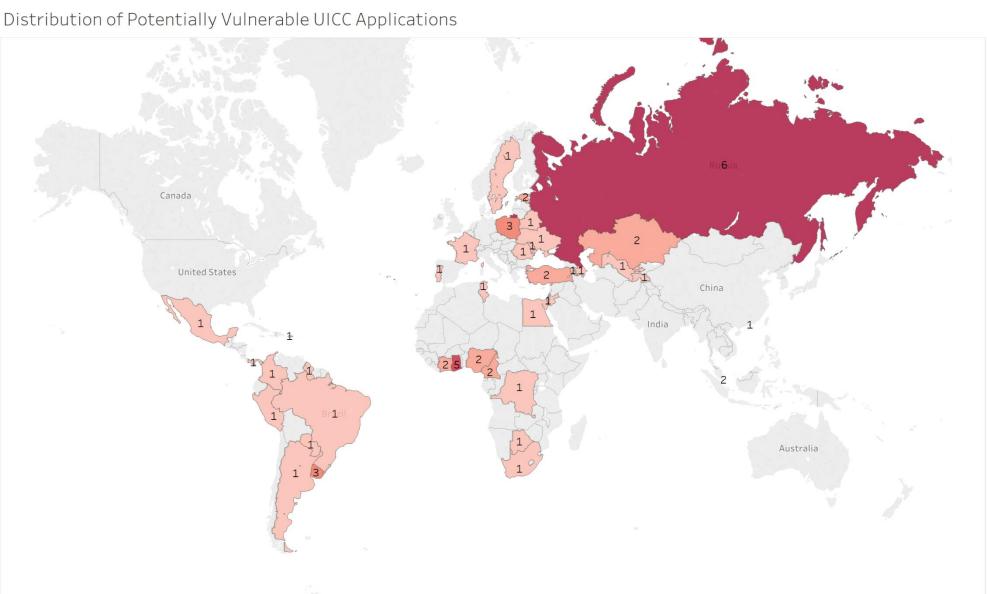
Where are these TARs used
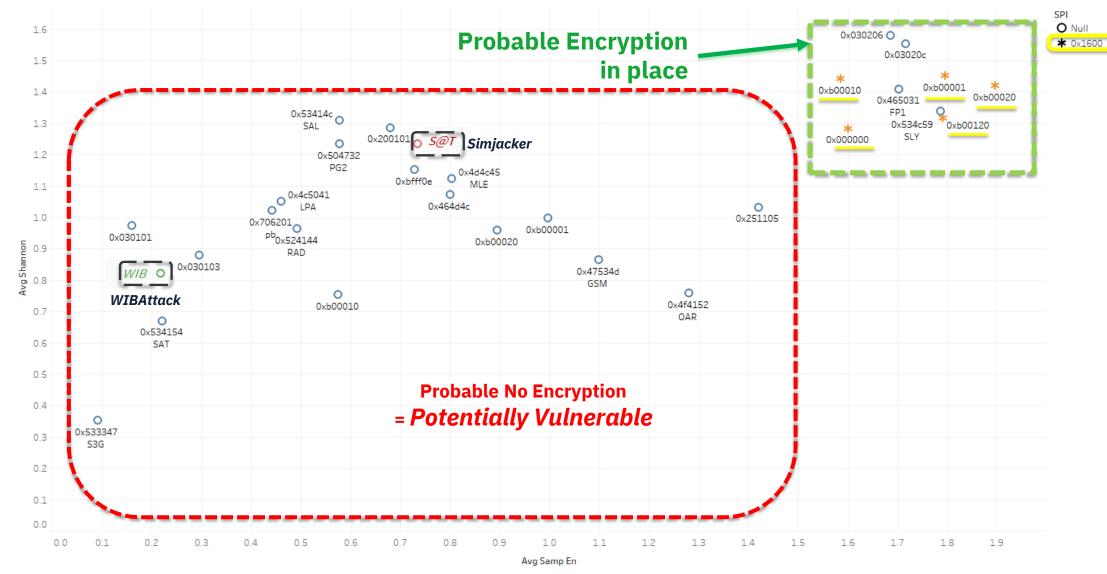
Detected 30 unique TAR values (UICC applications),

- Active in 50 operators from 39 countries,

with zero security set

Note: Varying activity per TAR

Distribution of Potentially Vulnerable UICC Applications

Threat level: Are all of these TARs Vulnerable?

Entropy per TAR : Average Sample Entropy (x) by Average Shannon Entropy (y)

Probable Encryption in place

Probable No Encryption = *Potentially Vulnerable*

Simjacker — S@T

WIBAttack — WIB

SPI
- ◯ Null
- ✳ 0x1600

- What do these UICC application do
  - Majority: Notification, Contacts exchange
    - Attacks limited, although these could be exploited
  - However some TARs (e.g 0xb...) have access to sensitive info
    - Could be used for location tracking (EF_{LOCI}), potentially extract info from SIM Card: IMSI, SIM Key (K_C - if phone on), Roaming settings

- Subscribers potentially affected ?
  - Theoretical maximum(unrealistic): ~770 million
    - some TARs were used very infrequently
  - Very conservative : ~37million SIM Card
  - Probable: less than <100m
- **<u>NO</u>** sign of these UICC applications being exploited
- All identified affected operators informed

Simjacker Vulnerability – looking back, and forward

Issues with communicating to industry in 2019:

- Very obscure technology but wide ability, only mobile operators could mitigate
- Being actively exploited by sophisticated surveillance company to track thousands of people
- Widescale use (61+ known mobile operators, 29+ countries, with potentially up to a billion subscribers) **+ unknown more operators**

Plan to inform community via **GSM Association CVD program**, but:
- **Gaps** in participation of specific operators in GSMA Working groups
  - Lesser concerns: Effectiveness, leakage (to attacker), others

How to make sure all vulnerable operators know (safely)?

Branded Vulnerability – Everybody loves them?

Images courtesy of https://io.netgarage.org/logo/

11

Staged Approach to Inform Industry

1. June -> Sept 2019: Inform all community as best as possible through GSM Association via CVD program (and direct contacts)

2. Sep 12th 2019: Do initial 'Public notification' with publicity to notify any unaware mobile operators
   - Give concepts but limited technical detail so attacks could not be replicated.
     - However this causes other problems in interim
   - Point mobile operators to the GSMA where full technical info available

3. Oct 3rd 2019: Later (+4 weeks) do full Technical Information release

Was this the right approach?

Daniel Cuthbert @dcuthbert · Sep 12, 2019
When an attack by Karsten Nohl from 6 years ago, is turned into a tool and people go wild. adaptivemobile.com/blog/simjacker...

Karsten has done amazing research into SS7 security and seemingly not listened to as he should have been theregister.co.uk/2013/09/23/whi...

8   129   202

Vess
@VessOnSecurity

I've been researching the SimJack issue and the more I am, the more something smells fishy about it...

4:51 PM · Sep 16, 2019 · TweetDeck

47 Retweets   7 Quote Tweets   135 Likes

computing
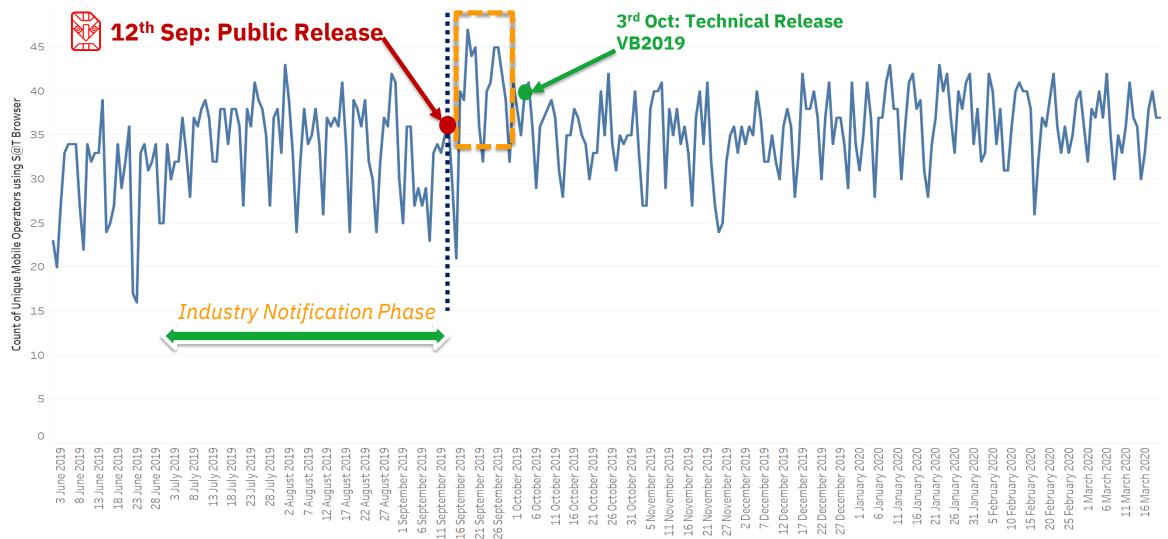
Doubts raised over Simjacker security flaw

Dev Kundaliya
18 September 2019 ·

12

...and I took that personally

Reaction of Mobile Operators
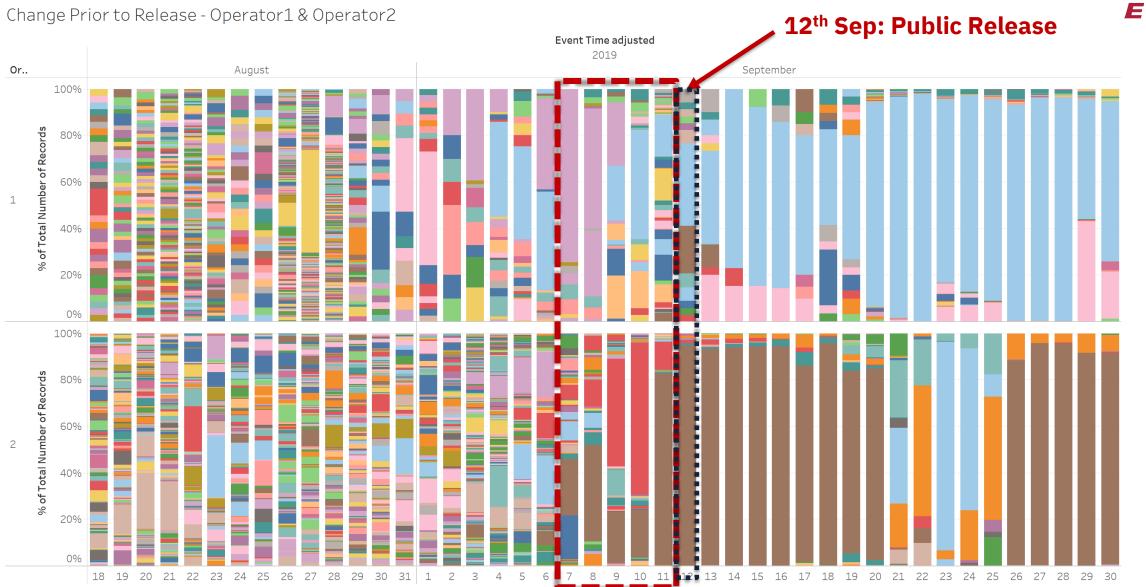
Count of Operators using S@T Browser with MSL ==0

12th Sep: Public Release

3rd Oct: Technical Release VB2019

Industry Notification Phase

Count of Unique Mobile Operators using S@T Browser
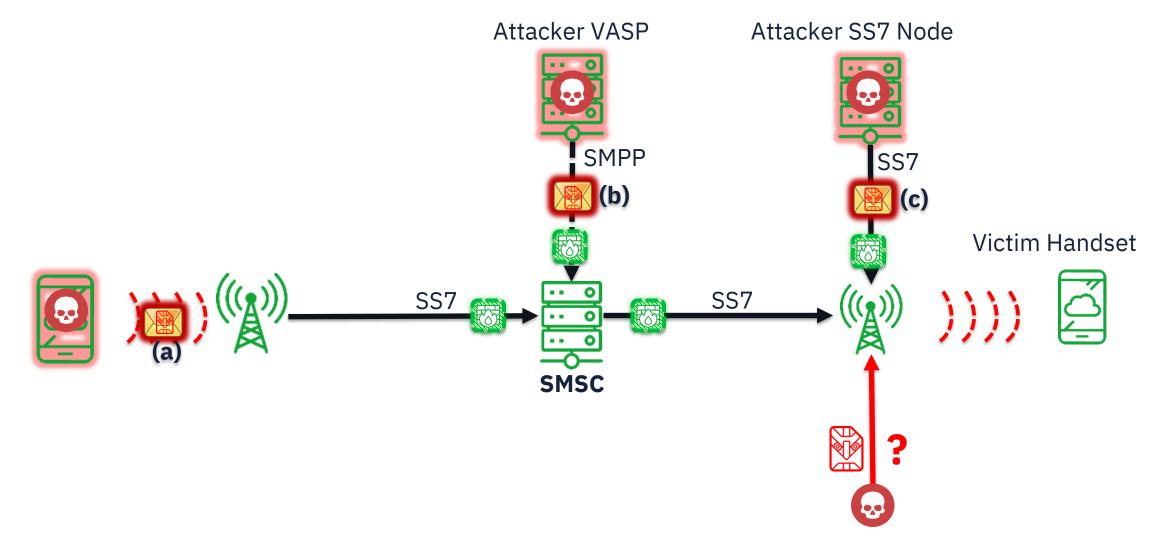
Reaction of Simjacker Attackers

Change Prior to Release - Operator1 & Operator2

Event Time adjusted
2019

12th Sep: Public Release

Simjacker Evasion techniques

Attacker VASP

Attacker SS7 Node

Victim Handset

SMPP **(b)**

SS7 **(c)**

SS7

SS7

SMSC

(a)

?

Simjacker Evasion techniques

```
> Internet Protocol Version 4, Src: [redacted], Dst: [redacted]
> User Datagram Protocol, Src Port: 5090, Dst Port: 5090
v Session Initiation Protocol (MESSAGE)
    > Request-Line: MESSAGE sip:[redacted]                SIP/2.0
    > Message Header
    > Message Body
v STK Protocol
    > Command Header
    v Secured Data
        v S@T Push
            v S@T Deck
                > Deck Attribute
                  S@T Deck Id: [redacted]
                v S@T Card
                    > S@T Card Attribute: [redacted]
                    > STK Provide Local Information: [redacted] (IMEI Information)
                    > STK Provide Local Information: [redacted] (Location Information)
                    > S@T Variable initialization ([redacted])
                    > S@T Concatenate ([redacted])
                    > STK Send Short Message: [redacted]
```

Attack via
SMS over SIP
MESSAGE

Scale of Attacks

Temporary gaps over time allow us to make estimates on scale & devices tracked

Wide scale of devices tracked:

- Largest Type: 91.7% Smartphone
- Largest Brand: 30.2% Apple
- Largest Model: 4.3% iPhone 12 Pro Max

Representative of Mexican market, not device vulnerability

Extrapolated Simjacker attacks in Mexico pre-detection:

- **~259k** location lookups per year
- **~31k** unique subscribers per year

Attackers not going away – constant exercise to detect and block

Conclusions

- Binary SMS vulnerabilities attacks happen, and will continue to happen
  - *Work ongoing within the industry to define defences*

- We uncovered many potentially vulnerable SIM Card applications
  - *Mobile Operators need to be aware and focus on security*

- Surveillance companies react faster than Mobile Operators
  - *Slow is fast, old is new, but threat intelligence is key*

AdaptiveMobile
Security

an Enea company