Sim Card Hack

By Sida Gao, Tianyou Luo, Shigang Zhu

Edward Snowden

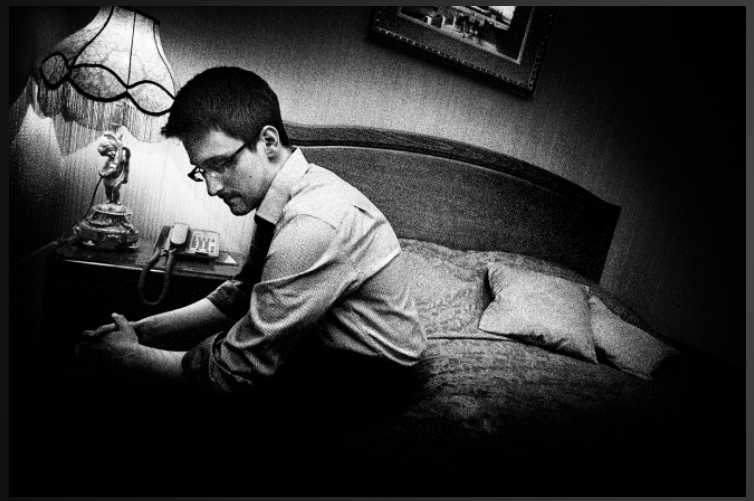


Photo by Platon

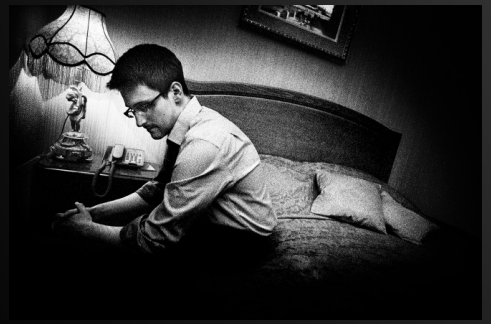
During a Reddit Ask Me Anything session on 02/16, he said the NSA and the British spy agency GCHQ had “screwed all of us” when it hacked into the Dutch firm Gemalto to steal cryptographic keys.

A multinational firm incorporated in the Netherlands that makes the chips used in mobile phones and next-generation credit cards. Among its clients are AT&T, T-Mobile, Verizon, Sprint and some 450 wireless network providers around the world.

...

...

"They screwed all of us!"



We might be hacked by someone before but the consequence may not be as severe.

gemalto
security to be free

How NSA & GCHQ did it?

1. Collected information of employees of Gemalto (mostly from email in this case)
2. Gained access of the company's network
3. Planted backdoors and other tools to give them a persistent foothold
4. Intercepted the unencrypted files(**Ki & OTA keys**) when Gemalto sent them to mobile companies via email or FTP
5. Game over!

NSA pretended to be Facebook in its effort to infect ‘millions’ of computers

- CAPTIVATEDAUDIENCE is used to take over a targeted computer’s microphone and record conversations taking place near the device.
- GUMFISH can covertly take over a computer’s webcam and snap photographs.
- FOGGYBOTTOM records logs of Internet browsing histories and collects login details and passwords used to access websites and email accounts.
- GROK is used to log keystrokes.
- SALVAGERABBIT exfiltrates data from removable flash drives that connect to an infected computer.

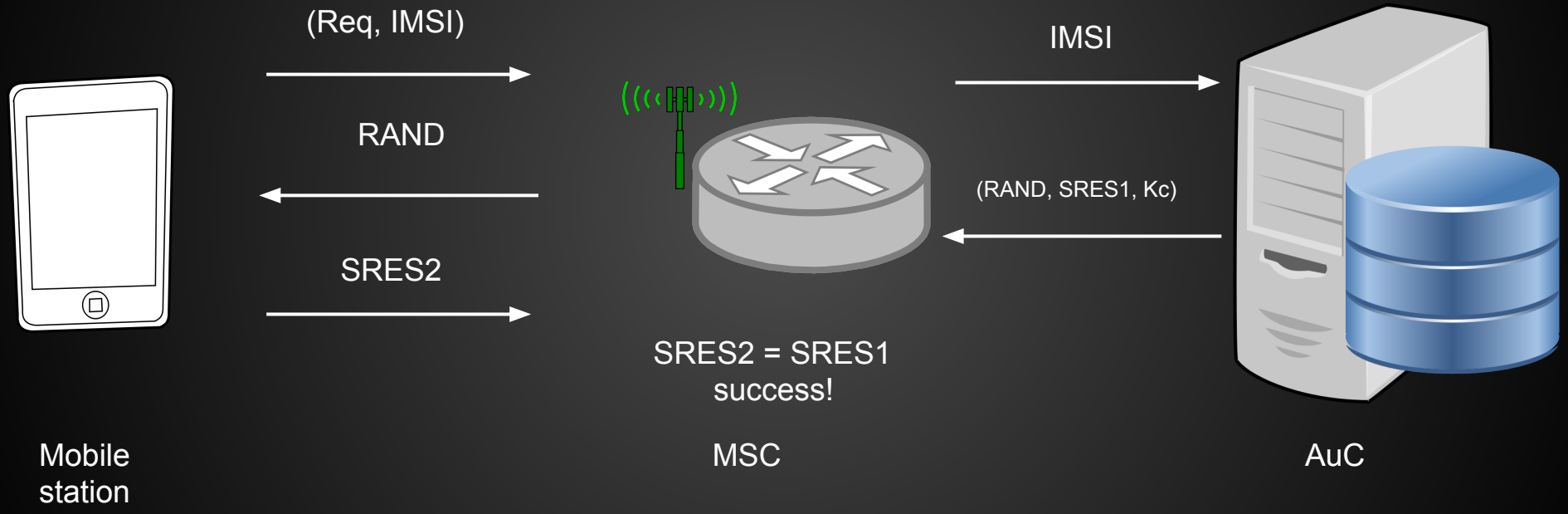
How NSA & GCHQ did it?

1. Collected information of employees of Gemalto (mostly from email in this case)
2. Gained access of the company's network
3. Planted backdoors and other tools to give them a persistent foothold
4. Intercepted the unencrypted files(**Ki & OTA keys**) when Gemalto sent them to mobile companies via email or FTP
5. Game over!

SIM Authentication Key (Ki)

- Burned into SIM cards by the manufacturer (e.g. Gemalto) in a process called personalization.
- Each SIM card has a unique identifier (IMSI) and a key (Ki) associated with its identifier
- (IMSI, Ki) entry is stored in the DB of mobile operator
- Used for mobile device authentication
- Not accessible by the mobile device

Authentication Process (GSM)



1. Tapping with no trace
2. Man-in-the Middle: Data still encrypted!!

OTA (Over-The-Air)

“used to communicate with, download applications to, and manage a SIM card without being connected physically to the card” -- Gemalto

How does OTA work?

OTA Server

r = (header || c || i)

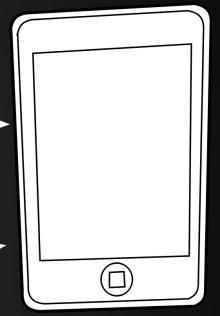
OTA GW

convert requests r to SMS format s

SMSC

s

Mobile Subscriber



reserved

reserved

index	keys pair
0	(KIc_0, KID_0)
1	(KIc_1, KID_1)
2	(KIc_2, KID_2)
3	(KIc_3, KID_3)
...	...

m = “update”

c = $Enc_{KIc}(m)$

i = $Integrity_{KID}(c)$

header = index of (KIc, KID) pair

(header || c || i) = s

get (KIc, KID) pair,

integrity check using KID,

m = $Dec_{KIc}(c)$

execute commands

Leak of OTA keys is BAD! Why?

- OTA commands are unrefusable as long as it’s using the proper OTA key
- whole process can be completely hidden from the user
- total access to the phones

How to fix it?

1. Use apps to encrypt your communication (text, phone call, email)

2. “Recall and replace every SIM sold by Gemalto” - Edward Snowden

Related Articles

Background:

https://firstlook.org/theintercept/2015/02/19/great-sim-heist/

http://www.digitaltrends.com/web/nsa-pretended-facebook-spread-malware/

http://www.wired.com/2015/02/snowden-spy-agencies-screwed-us-hacking-crypto-keys/

OTA:

http://www.gemalto.com/techno/ota

http://bgr.com/2015/02/25/nsa-gemalto-sim-hack-spyware/

http://www.theverge.com/2015/2/24/8101585/the-nsas-sim-heist-could-have-given-it-the-power-to-plant-spyware-on

http://en.wikipedia.org/wiki/Over-the-air_programming

http://www.bluefish.com/files/BFT%20Aperio%20OTA%20Brochure.pdf

http://blog.fortinet.com/post/millions-of-sim-cards-vulnerable-to-remote-compromise

https://books.google.com/books?id=9iwFQarJdBMC&pg=PA267&lpg=PA267&dq=what+ota+keys+used+for&source=bl&ots=ggFg_ASgtr&sig=sQ1pCW3wTILY8uW9ZJLptqKkkcA&hl=en&sa=X&ei=-6z3VPayMsiWNqTQgZgM&ved=0CFEQ6AEwCA#v=onepage&q=what%20ota%20keys%20used%20for&f=false

Ki:

http://en.wikipedia.org/wiki/Subscriber_identity_module

http://www.digitaltrends.com/mobile/nsa-gchq-sim-card-hack-snowden-leak-news/2/

http://en.wikipedia.org/wiki/Network_switching_subsystem#Authentication_center_.28AuC.29

Questions?

Thank you