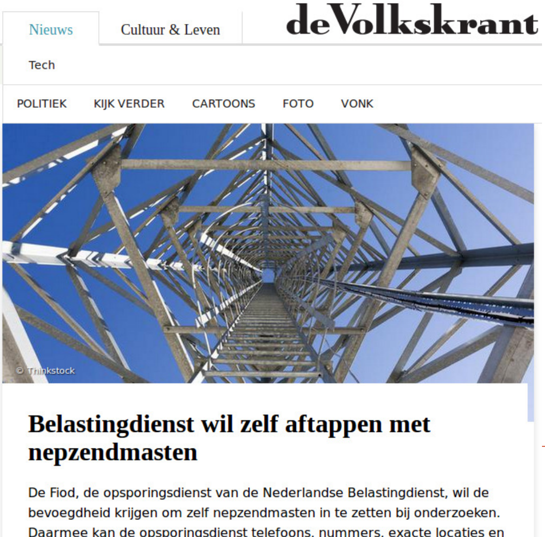
IMSI catching

Mobile (in)security
Black Hat Sessions
23-06-2016 Ede

Fabian van den Broek

In the news...



deVolkskrant

© Thinkstock

Belastingdienst wil zelf aftappen met nepzendmasten

De Fiod, de opsporingsdienst van de Nederlandse Belastingdienst, wil de bevoegdheid krijgen om zelf nepzendmasten in te zetten bij onderzoeken. Daarmee kan de opsporingsdienst telefoons, nummers, exacte locaties en

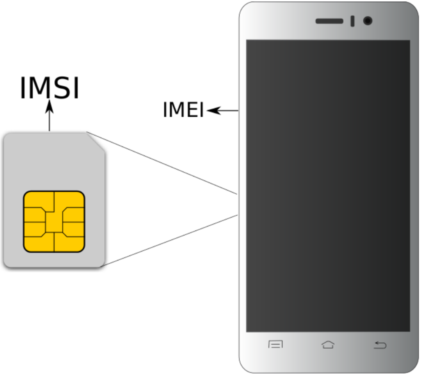
IMSI catching

- IMSI catcher, fake celltower, “nepzendmast”
- overloaded term
  - catching IMSIs
  - eavesdropping

So, what is an IMSI?

So, what is an IMSI?

- **IMSI** = International Mobile Subscriber Identity
- unique identifier of a SIM
- IMEI $\neq$ IMSI $\neq$ phone number



So, what is an IMSI? (II)

15 digits that identify:

- home country
- home network
- user

Example IMSI:

204080123456789

So, what is an IMSI? (II)

15 digits that identify:

- home country
- home network
- user

Example IMSI:
204080123456789

- The Netherlands

So, what is an IMSI? (II)

15 digits that identify:

- home country
- home network
- user

Example IMSI:

204080123456789

- The Netherlands
- KPN

So, what is an IMSI? (II)

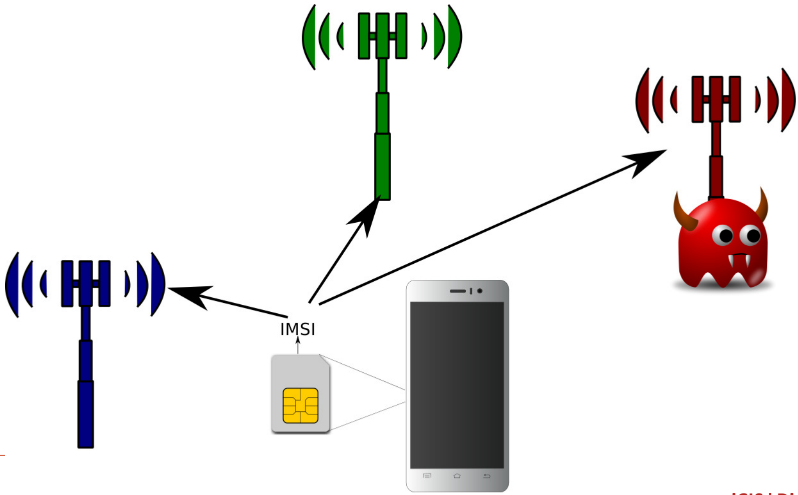
15 digits that identify:

- home country
- home network
- user

Example IMSI:
204080123456789

- The Netherlands
- KPN

And the IMSI is broadcast in plain text!



IMSI catchers

- passive
- active

IMSI catchers

- passive
- active
- eavesdropping and insertion

IMSI catchers

- passive
- active
- eavesdropping and insertion
- expensive and exclusively sold to governments

IMSI catchers

- passive
- active
- eavesdropping and insertion
- expensive and exclusively sold to governments
- or home made for $100,-

Why catch IMSIs?

- IMSIs reveal information

Why catch IMSIs?

- IMSIs reveal information
- Attack location privacy

Why catch IMSIs?

- IMSIs reveal information
- Attack location privacy
  - Tracking

Why catch IMSIs?

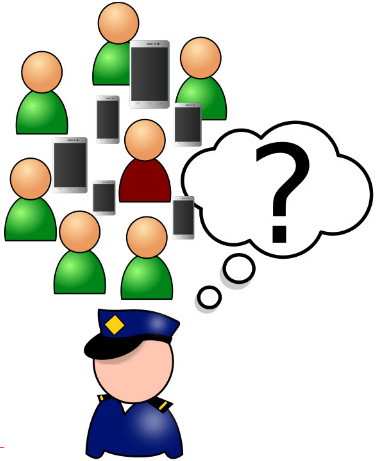
- IMSIs reveal information
- Attack location privacy
  - Tracking

Why catch IMSIs?

- IMSIs reveal information
- Attack location privacy
  - Tracking
  - Location monitoring

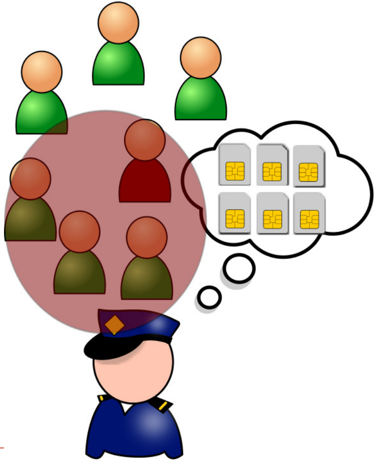
Why catch IMSIs?

- IMSIs reveal information
- Attack location privacy
  - Tracking
  - Location monitoring
- Linking identities to devices



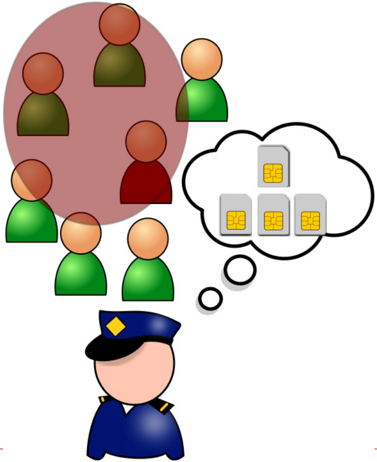
Why catch IMSIs?

- IMSIs reveal information
- Attack location privacy
  - Tracking
  - Location monitoring
- Linking identities to devices



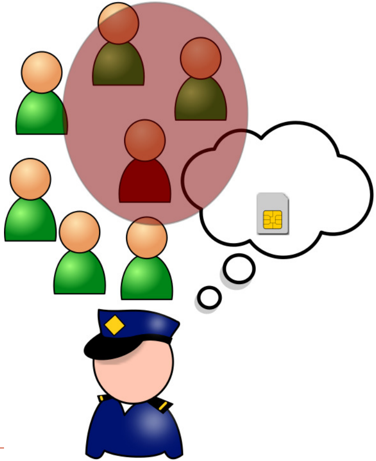
Why catch IMSIs?

- IMSIs reveal information
- Attack location privacy
  - Tracking
  - Location monitoring
- Linking identities to devices



Why catch IMSIs?

- IMSIs reveal information
- Attack location privacy
  - Tracking
  - Location monitoring
- Linking identities to devices



Why is the IMSI not protected?

- **TMSI**s; Temporary Mobile Subscriber Identity

Why is the IMSI not protected?

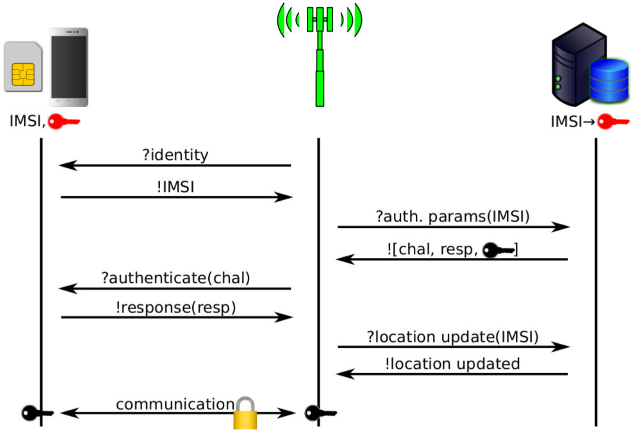
- **TMSI**s; Temporary Mobile Subscriber Identity
- But, the IMSI can still be requested without authentication or encryption!

Why is the IMSI not protected?

- **TMSI**s; Temporary Mobile Subscriber Identity
- But, the IMSI can still be requested without authentication or encryption!
- Identification before Authentication

2G authentication (simplified)

2G authentication (simplified)



IMSI, 🔑

IMSI→🔑

?identity

!IMSI

?auth. params(IMSI)

![chal, resp, 🔑]

?authenticate(chal)

!response(resp)

?location update(IMSI)

!location updated

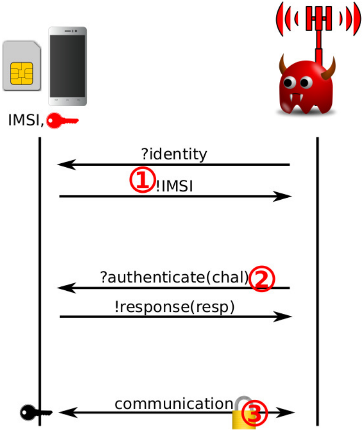
🔑 communication🔒 🔑

GSM weaknesses

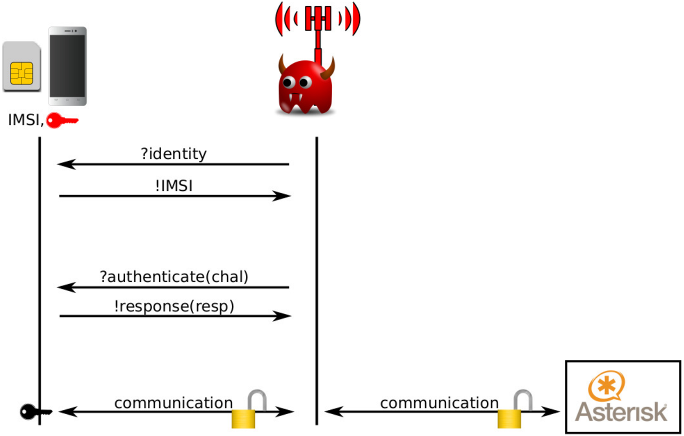
1. Identify before authenticate
2. No mutual authentication
3. Weak encryption options
   (A5/0, A5/1, A5/2)

GSM weaknesses

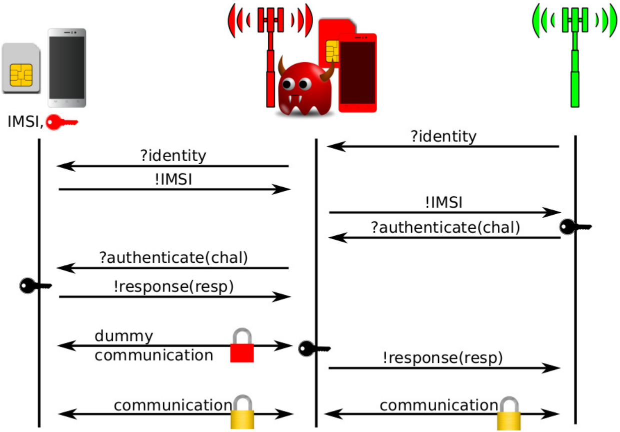
1. Identify before authenticate
2. No mutual authentication
3. Weak encryption options (A5/0, A5/1, A5/2)



GSM Man-in-the-Middle

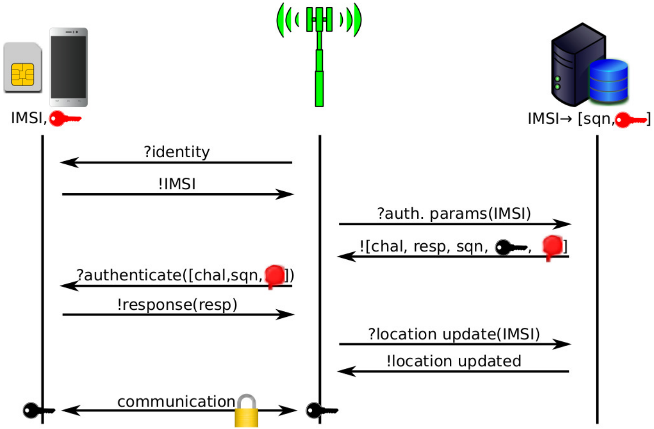


GSM Man-in-the-Middle

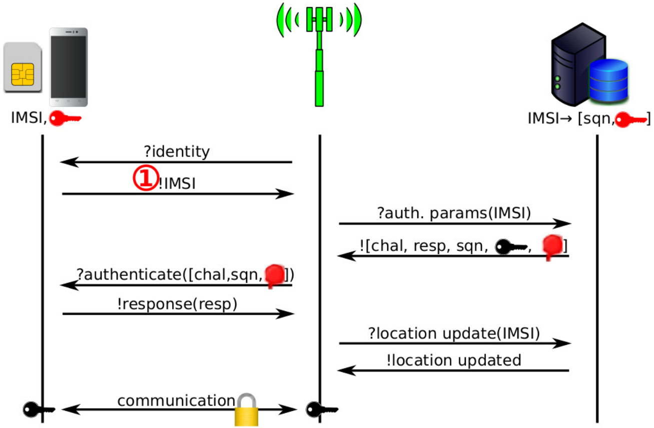


3G+4G authentication (simplified)

3G+4G authentication (simplified)



3G+4G weakness



So...

- IMSI catching works on all currently deployed 3GPP technology (GSM, GPRS, UMTS, LTE, etc.).
- UMTS and LTE protect against eavesdropping,
- but a fall-back attack to GSM is easy.
- Major updates to current technologies infeasible.

Protection

Protection against eavesdropping

- Switch off GSM
- Use secure tunnels

Protection against IMSI catching

1. IMSI-catcher catcher

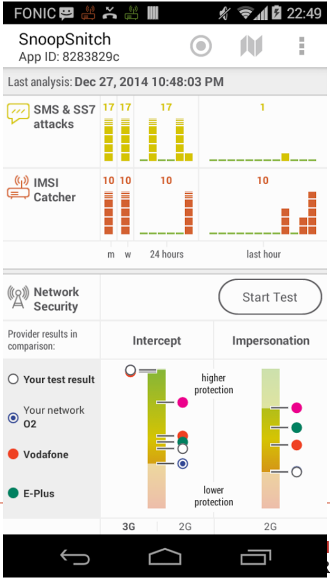
2. Pseudonyms

IMSI-catcher catcher apps

- SnoopSnitch
- Cell Spy Catcher
- Android IMSI-Catcher Detector (AIMSICD)

IMSI-catcher catcher apps

- SnoopSnitch
  - 100,000 - 500,000 downloads
  - requires root access & Qualcomm chipset
  - low level access gets good results
- Cell Spy Catcher
- Android IMSI-Catcher Detector (AIMSICD)

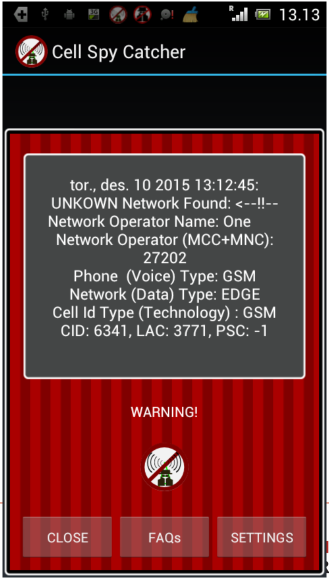


SnoopSnitch
App ID: 8283829c

Last analysis: Dec 27, 2014 10:48:03 PM

IMSI-catcher catcher apps

- SnoopSnitch
- Cell Spy Catcher
  - 10,000 - 50,000 downloads
  - no special permissions, but a learning period
  - cell IDs not very reliable
- Android IMSI-Catcher Detector (AIMSICD)

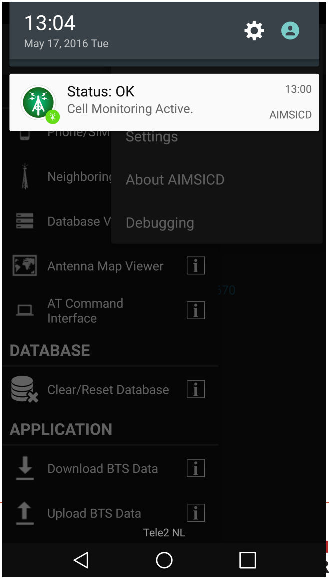


tor., des. 10 2015 13:12:45:
UNKOWN Network Found: <--!!--
Network Operator Name: One
Network Operator (MCC+MNC): 27202
Phone (Voice) Type: GSM
Network (Data) Type: EDGE
Cell Id Type (Technology) : GSM
CID: 6341, LAC: 3771, PSC: -1

WARNING!

IMSI-catcher catcher apps

- SnoopSnitch
- Cell Spy Catcher
- Android IMSI-Catcher Detector (AIMSICD)
    - open source on Github
    - phone support is flaky



13:04
May 17, 2016 Tue

Status: OK 13:00
Cell Monitoring Active. AIMSICD

Phone/SIM
Settings
Neighboring
About AIMSICD
Database V
Debugging
Antenna Map Viewer
570
AT Command Interface

DATABASE

Clear/Reset Database

APPLICATION

Download BTS Data
Upload BTS Data

Tele2 NL

IMSI-catcher catcher apps

- SnoopSnitch
- Cell Spy Catcher
- Android IMSI-Catcher Detector (AIMSICD)

These apps:

- only work for Android
- require high permissions
- can only warn the user

Preventing IMSI catching

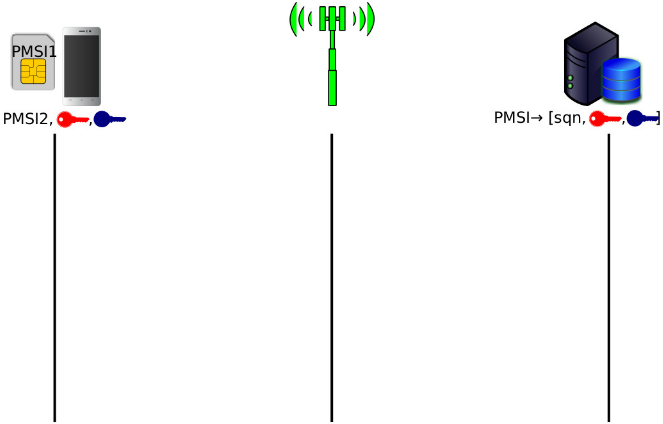
Preventing IMSI catching

- uses temporary pseudonyms: PMSIs
- can be deployed by any Home network / provider
- does not prevent IMSI catching, but hinders attack goals (e.g. tracking, etc.)
- is formally verified using ProVerif
- successor PMSIs are only known to SIM and Home network
- the Home network generates successor PMSIs

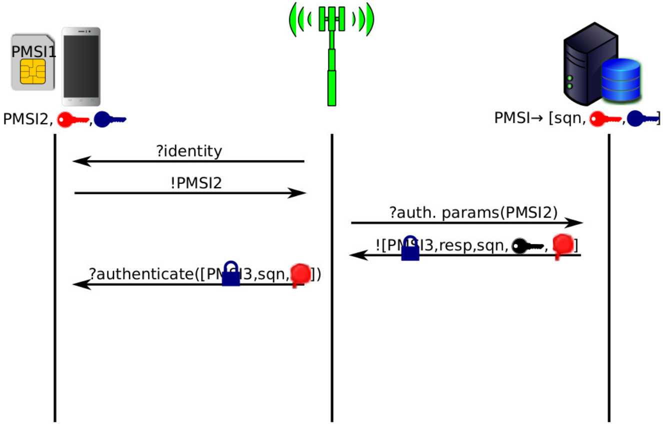
Preventing IMSI catching

- uses temporary pseudonyms: PMSIs
- can be deployed by any Home network / provider
- does not prevent IMSI catching, but hinders attack goals (e.g. tracking, etc.)
- is formally verified using ProVerif
- successor PMSIs are only known to SIM and Home network
- the Home network generates successor PMSIs,
  but how to get them to the SIM?

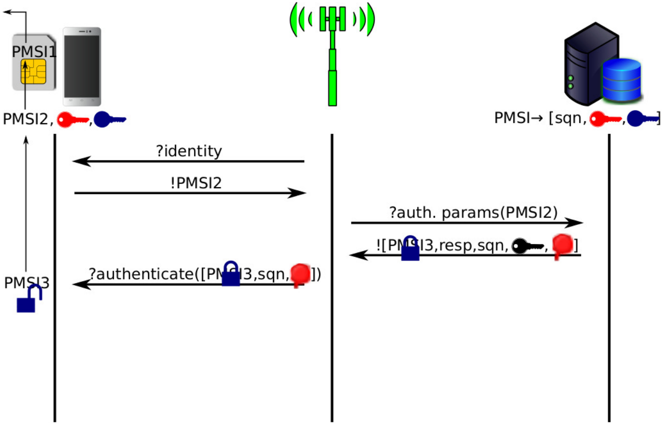
3G+4G solution



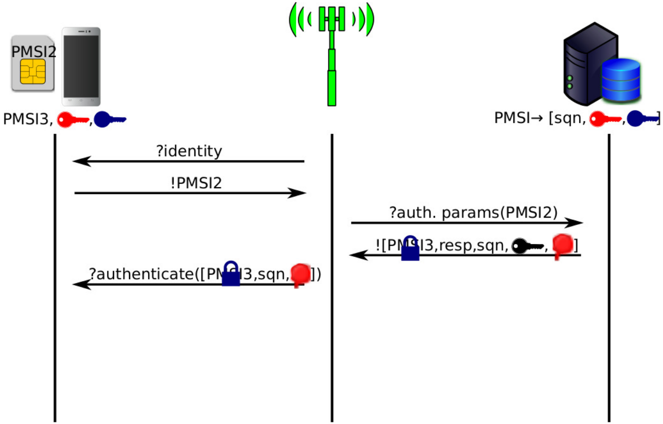
3G+4G solution



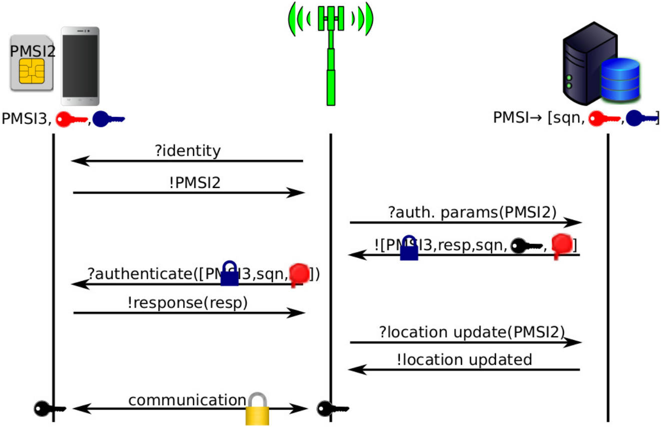
3G+4G solution



3G+4G solution



3G+4G solution



3G+4G solution (II)

- the random challenge can transmit the new PMSIs
- an extra key is shared between SIM and provider
- each SIM stores 2 PMSIs, the current and its successor
- when provider receives a successor PMSI, it hands out a new PMSI

3G+4G solution (II)

- the random challenge can transmit the new PMSIs
- an extra key is shared between SIM and provider
- each SIM stores 2 PMSIs, the current and its successor
- when provider receives a successor PMSI, it hands out a new PMSI

Some technicalities

- Chal $= E_{key}$(PMSI,SQN)

3G+4G solution (II)

- the random challenge can transmit the new PMSIs
- an extra key is shared between SIM and provider
- each SIM stores 2 PMSIs, the current and its successor
- when provider receives a successor PMSI, it hands out a new PMSI

Some technicalities

- Chal $= E_{key}$(PMSI,SQN)
- As E choose AES?

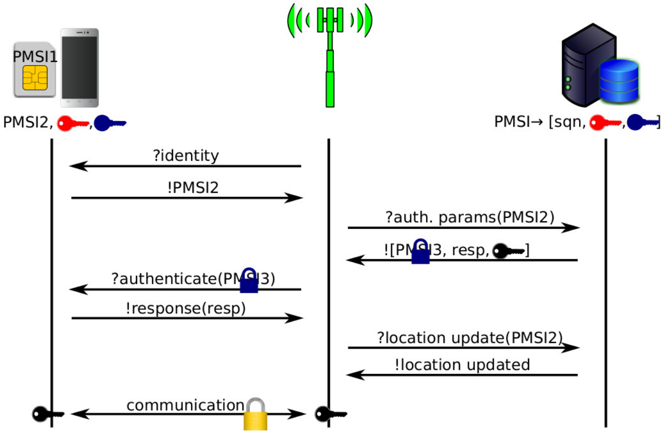
3G+4G solution (II)

- the random challenge can transmit the new PMSIs
- an extra key is shared between SIM and provider
- each SIM stores 2 PMSIs, the current and its successor
- when provider receives a successor PMSI, it hands out a new PMSI

Some technicalities

- Chal $= E_{key}$(PMSI,SQN)
- As E choose AES?
- PMSI is only the last 10 digits of the IMSI (MSIN)

2G solution



PMSI1

PMSI2, 🔑, 🔑

PMSI→ [sqn, 🔑, 🔑]

?identity

!PMSI2

?auth. params(PMSI2)

![PMSI3, resp, 🔑]

?authenticate(PMSI3)

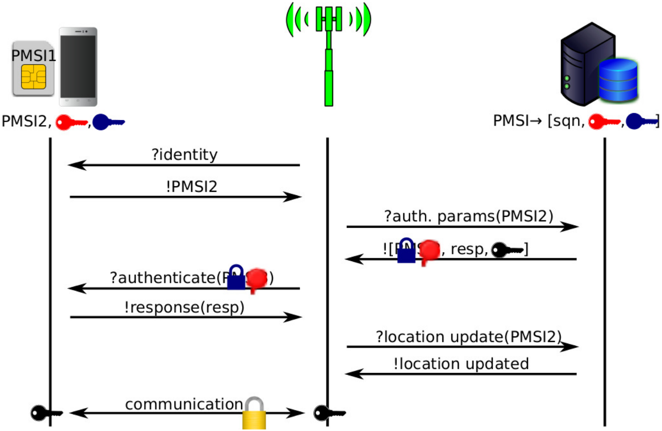
!response(resp)

?location update(PMSI2)

!location updated

🔑 communication 🔒 🔑

2G solution



PMSI1

PMSI2, 🔑, 🔑

PMSI→ [sqn, 🔑, 🔑]

?identity

!PMSI2

?auth. params(PMSI2)

![P🔒, resp, 🔑]

?authenticate(P🔒)

!response(resp)

?location update(PMSI2)

!location updated

🔑 communication 🔒 🔑

3G+4G solution: Security guarantees

An attacker without knowledge of the new key cannot:

- link subsequent PMSIs
- insert false PMSIs
- replay genuine authentication messages
- get the SIM and provider out-of-sync

Discussion

The presented solution

- provides k-anonymity, with k = #subscribers from same provider

Discussion

The presented solution

- provides k-anonymity, with k = #subscribers from same provider

- does not prevent MitM attacks, but it does hinder them,

Discussion

The presented solution

- provides k-anonymity, with k = #subscribers from same provider
- does not prevent MitM attacks, but it does hinder them,
- does not protect other identifiers in your phone, e.g. IMEI, MAC, BT address, etc,

Discussion

The presented solution

- provides k-anonymity, with k = #subscribers from same provider
- does not prevent MitM attacks, but it does hinder them,
- does not protect other identifiers in your phone, e.g. IMEI, MAC, BT address, etc,
- increases back end traffic

Discussion

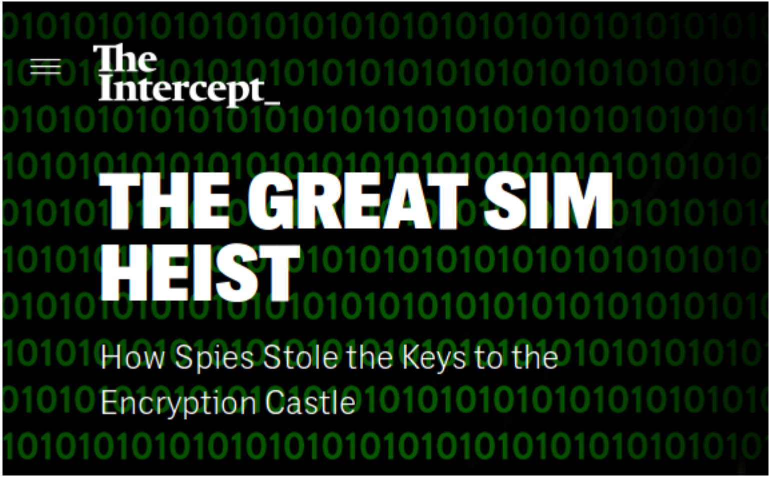
The presented solution

- provides k-anonymity, with k = #subscribers from same provider
- does not prevent MitM attacks, but it does hinder them,
- does not protect other identifiers in your phone, e.g. IMEI, MAC, BT address, etc,
- increases back end traffic
- requires willing providers

Discussion

The presented solution

- provides k-anonymity, with k = #subscribers from same provider
- does not prevent MitM attacks, but it does hinder them,
- does not protect other identifiers in your phone, e.g. IMEI, MAC, BT address, etc,
- increases back end traffic
- requires willing providers
- assumes the SIM is secure...



The Intercept_

THE GREAT SIM HEIST

How Spies Stole the Keys to the Encryption Castle

Conclusions

- current technologies (2G - 4G) are not easily replaced
- and have serious security issues
- but you are not helpless!

Conclusions

- current technologies (2G - 4G) are not easily replaced
- and have serious security issues
- but you are not helpless!

So, who will be the first to sell IMSI Catcher resilient SIM cards?

Questions

?