Defeating IMSI catchers

CCS 2015

10-13-2015 Denver

Fabian van den Broek, Roel Verdult and Joeri de Ruiter

iCIS | Digital Security
Radboud University

IMSI catching

For this talk:
IMSI catching == catching IMSIs
(and nothing else)

IMSI catching

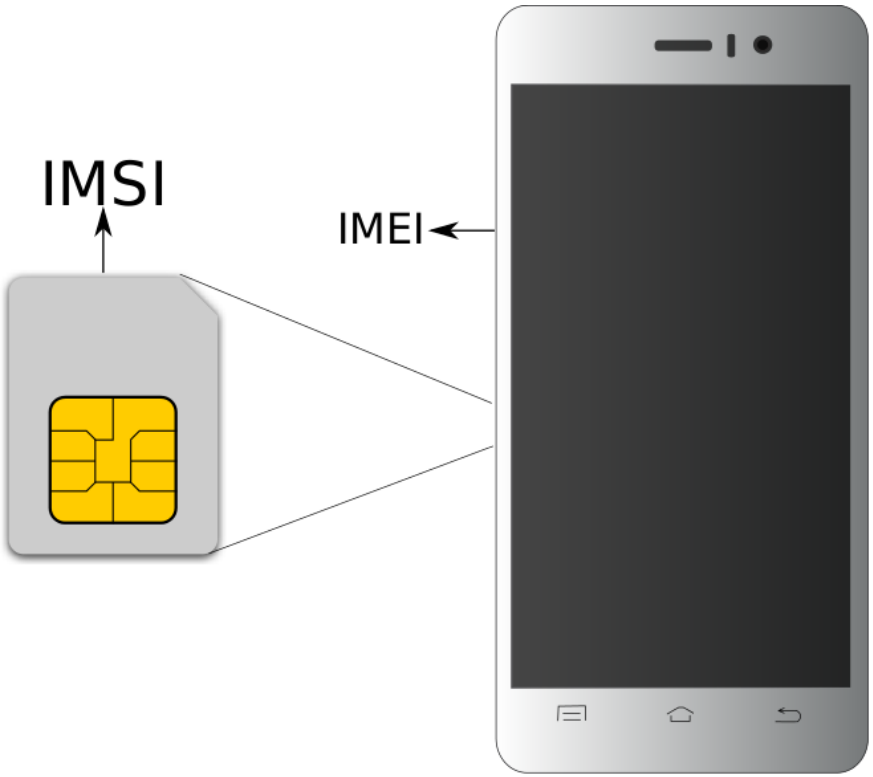
For this talk:
IMSI catching == catching IMSIs
(and nothing else)

IMSI catching is an attack that works on **all** generations of mobile networks

So, what is an IMSI?

So, what is an IMSI?

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



So, what is an IMSI? (II)

15 digits that identify:

- home country
- home network
- user

Example IMSI:

310030123456789

So, what is an IMSI? (II)

15 digits that identify:

- home country
- home network
- user

Example IMSI:

310030123456789

- The United States

So, what is an IMSI? (II)

15 digits that identify:

- home country
- home network
- user

Example IMSI:

310030123456789

- The United States
- AT&T

So, what is an IMSI? (II)

15 digits that identify:

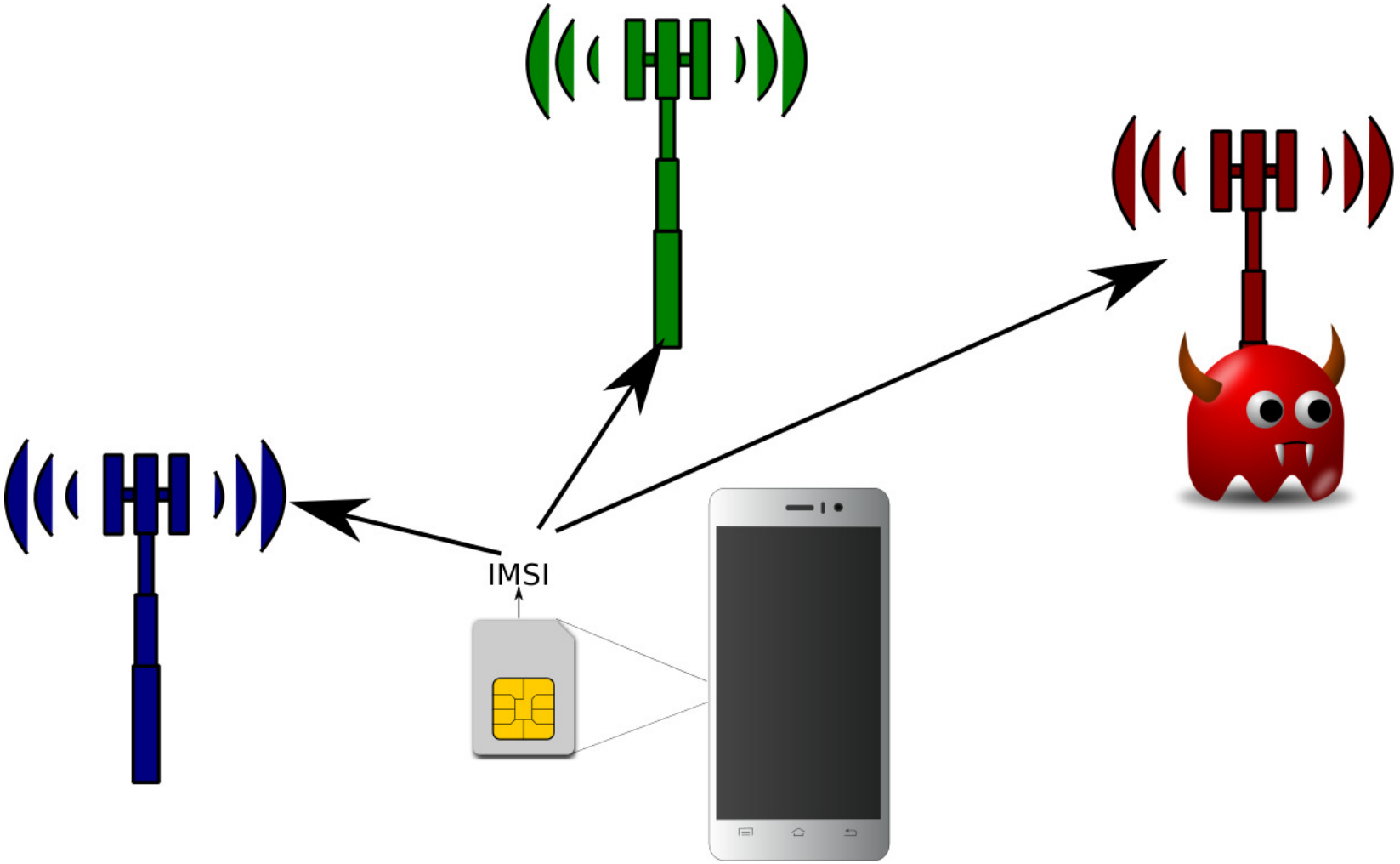
- home country
- home network
- user

Example IMSI:

310030123456789

- The United States
- AT&T

And the IMSI is broadcasted 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?

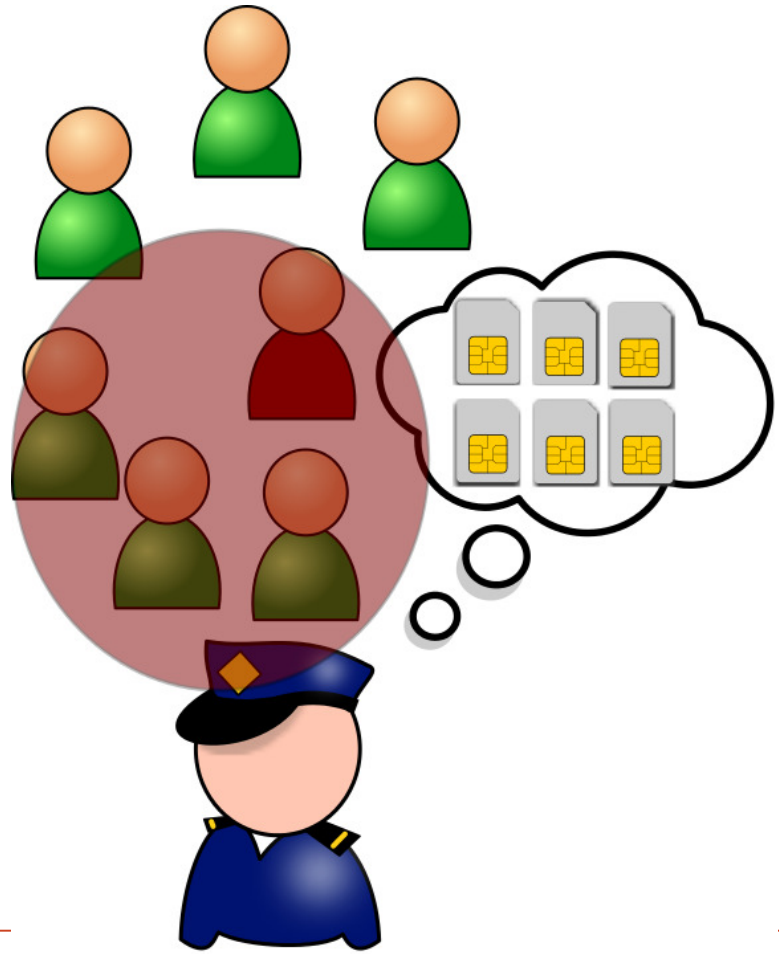
- IMSIs reveal information
- Attack location privacy
  - Tracking
  - Location monitoring

Why catch IMSIs?

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

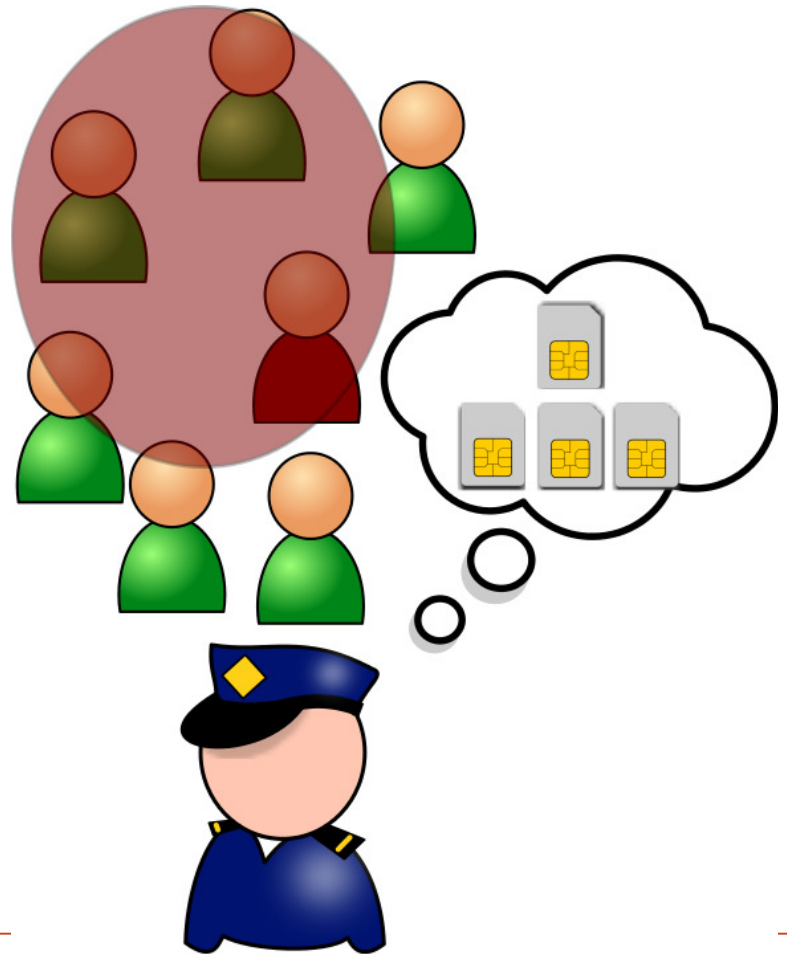
Why catch IMSIs?

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



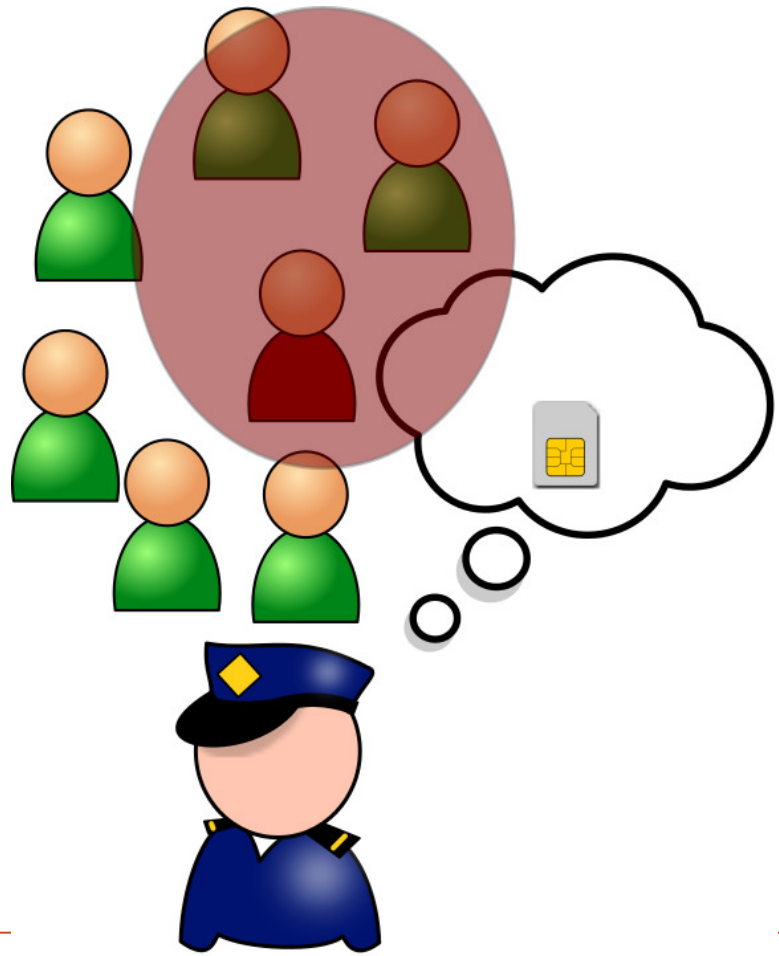
Why catch IMSIs?

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

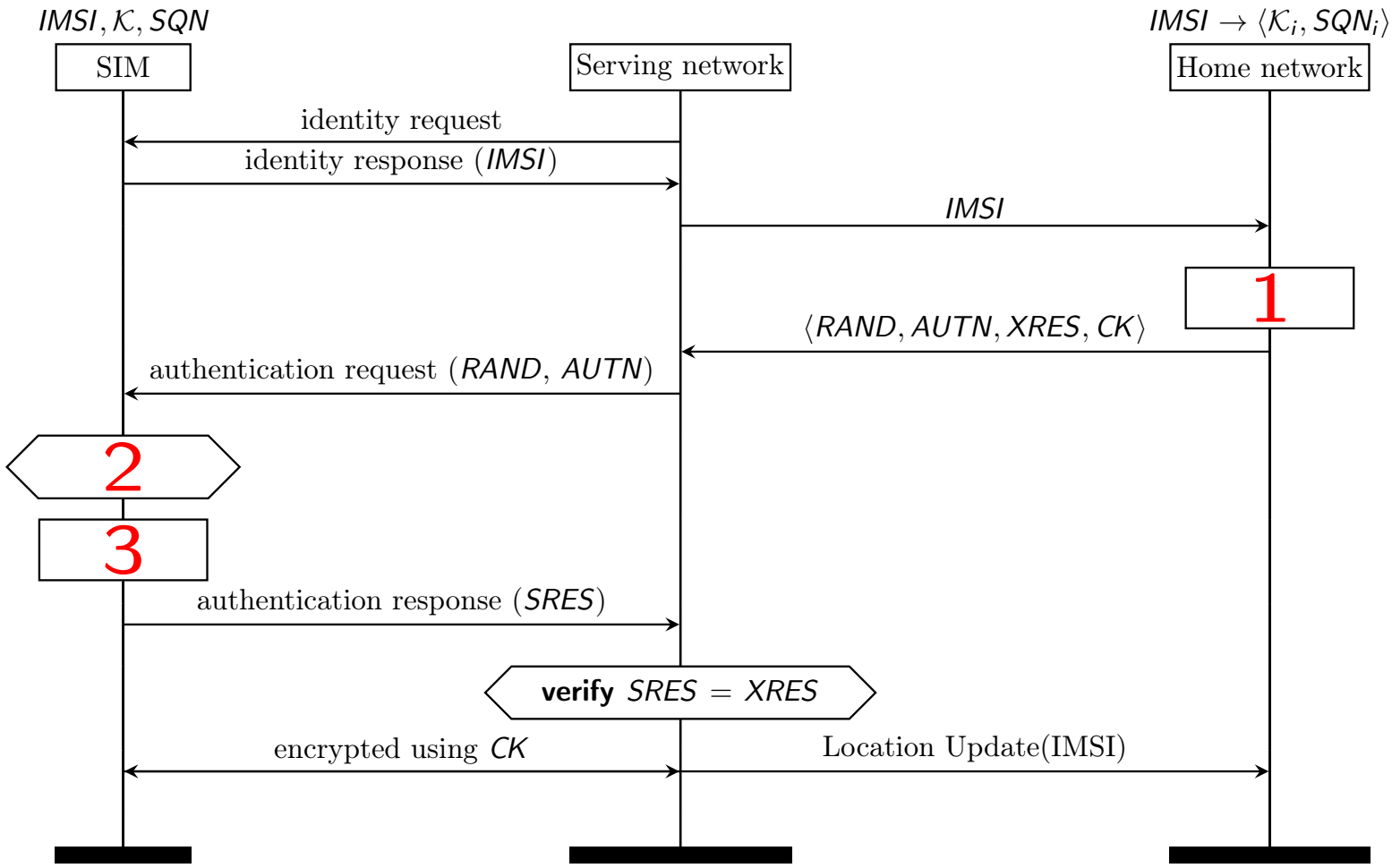


Why catch IMSIs?

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



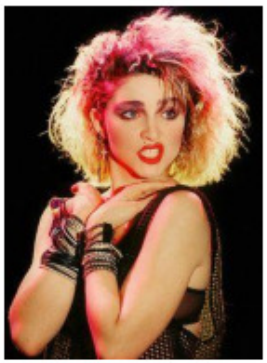
3G+4G authentication (simplified)



Who is to blame?

Who is to blame?

80s



Who is to blame?

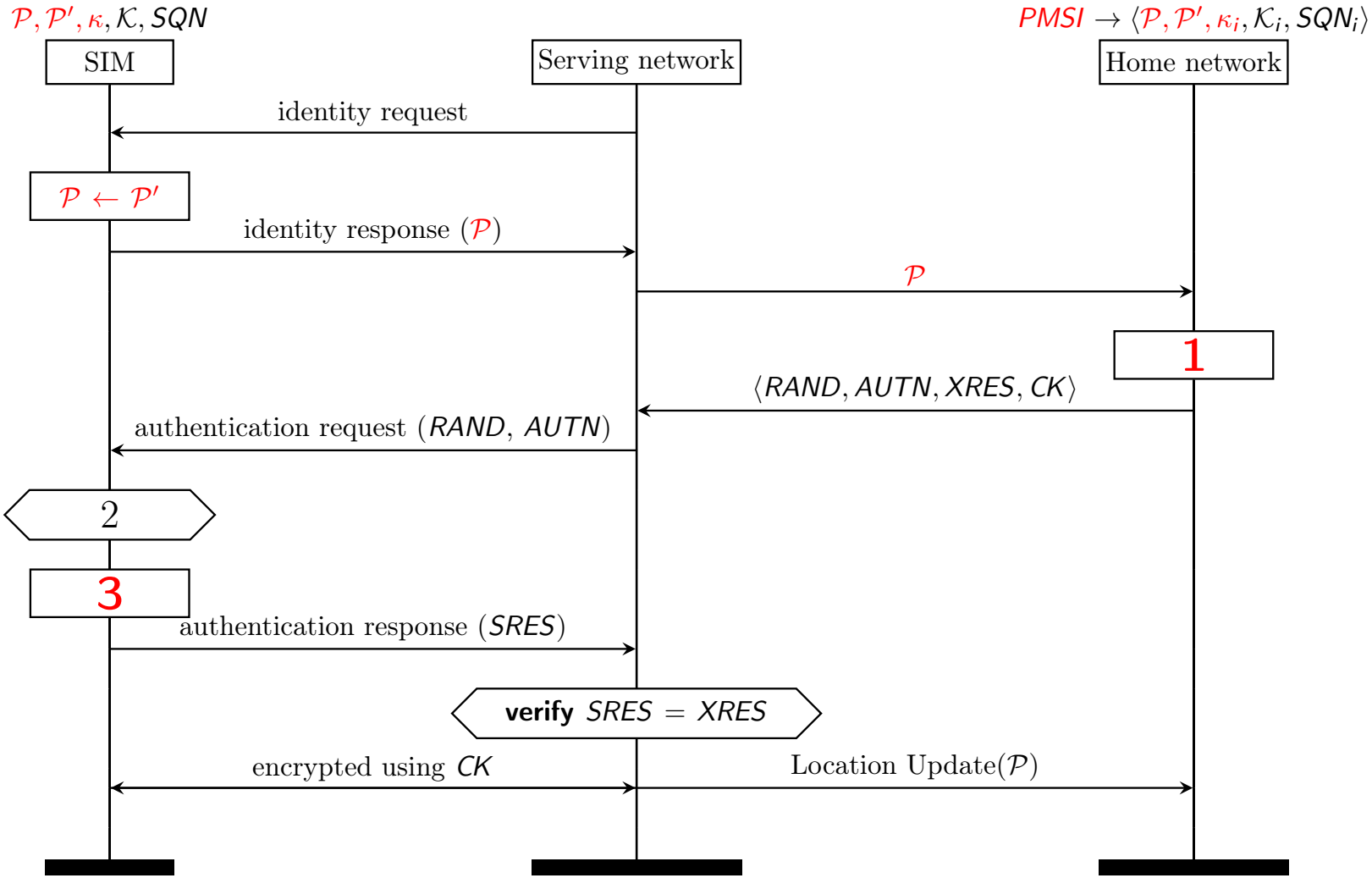
Our solution

- 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

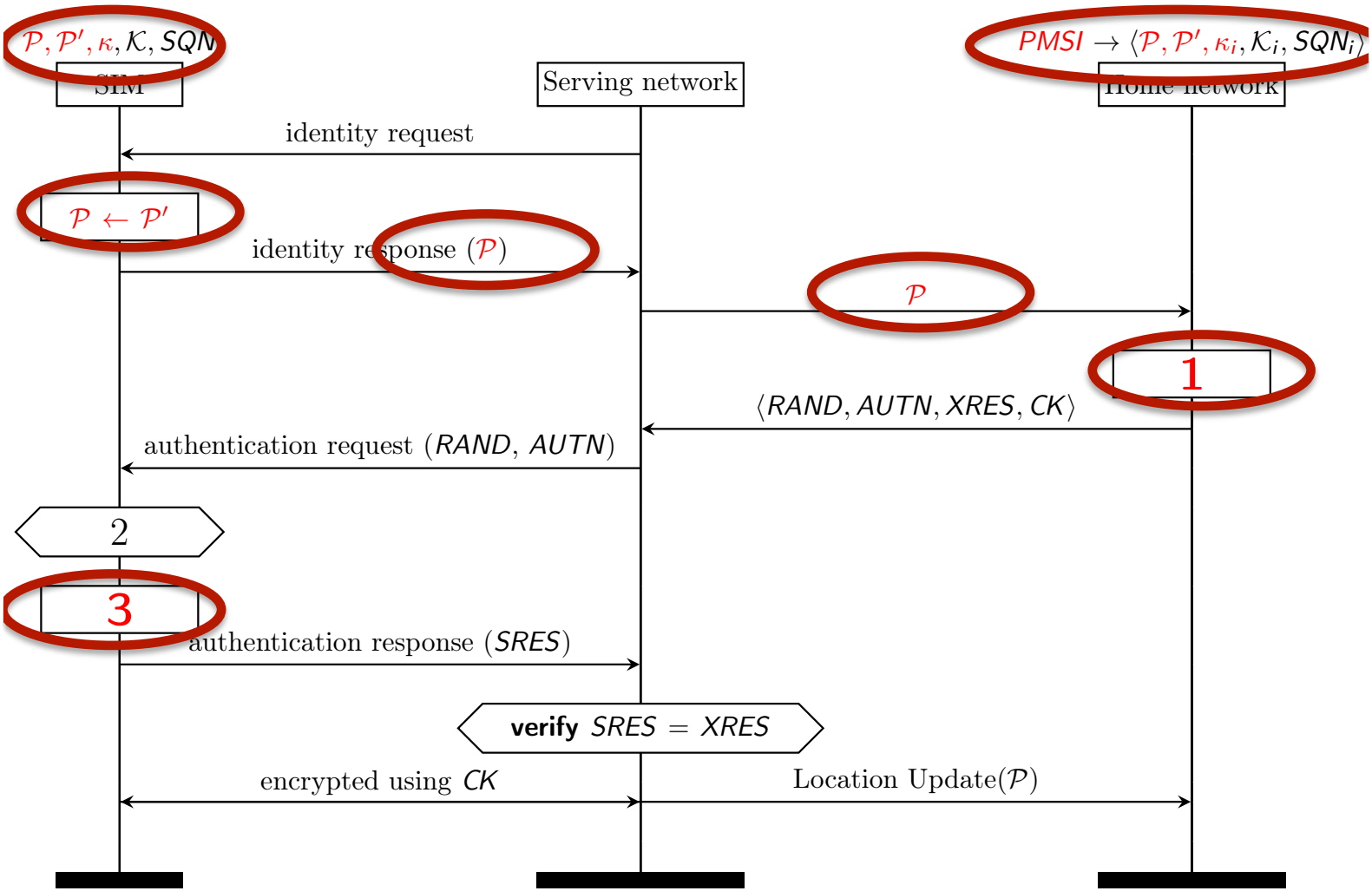
Our solution

- 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 (II)

Step 1 is extended with:

if $PMSI = \mathcal{P}'_i$ **then**
  $\mathcal{P}_i \leftarrow \mathcal{P}'_i$
  $\mathcal{P}'_i \leftarrow \{0-9\}^{10}$
fi
$RAND \leftarrow \mathrm{ENCRYPT}_\kappa(\mathcal{P}'_i, SQN_i)$

Step 3 is extended with:

$[PMSI, SQN'] \leftarrow \mathrm{DECRYPT}_\kappa(RAND)$
if $SQN = SQN'$ **then**
  $\mathcal{P}' \leftarrow PMSI$
fi

3G+4G solution (III)

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

3G+4G solution: Security guarantees

An attacker without knowledge of k cannot:

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

Discussion

The presented solution

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

Discussion

The presented solution

- provides k-anonymity, with k = #subscribers from same HN
- does not prevent MitM attacks, but it does hinder them,

Discussion

The presented solution

- provides k-anonymity, with k = #subscribers from same HN
- 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 HN
- 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,
- assumes the SIM is secure...

Discussion

The presented solution

- provides k-anonymity, with k = #subscribers from same HN
- 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,
- assumes the SIM is secure...
- increases back end traffic

What about the future?

- 5G is coming
- Use asymmetric crypto

What about the future?

- 5G is coming
- Use asymmetric crypto
- but what about the message size? Currently, an IMSI is transmitted in 60 bits.

What about the future?

- 5G is coming
- Use asymmetric crypto
- but what about the message size? Currently, an IMSI is transmitted in 60 bits.
- what if we want to be quantum secure?

Conclusions

- IMSI catching is not unpreventable!
- Our solution can be implemented by individual providers within the current architecture.
- We also have a variant for 2G

  BONUS: adds mutual authentication to 2G retrospectively
- Current technologies (2G - 4G) are not easily replaced

Conclusions

- IMSI catching is not unpreventable!
- Our solution can be implemented by individual providers within the current architecture.
- We also have a variant for 2G

  BONUS: adds mutual authentication to 2G retrospectively
- Current technologies (2G - 4G) are not easily replaced

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

Questions

?