# Defeating IMSI Catchers

Fabian van den Broek et al.

CCS 2015

# ackground – 3GPP

3GPP – 3rd Generation Partnership Project

Encompasses:

- GSM and related “2G” standards
- UMTS and related “3G” standards
- LTE and related “4G” standards

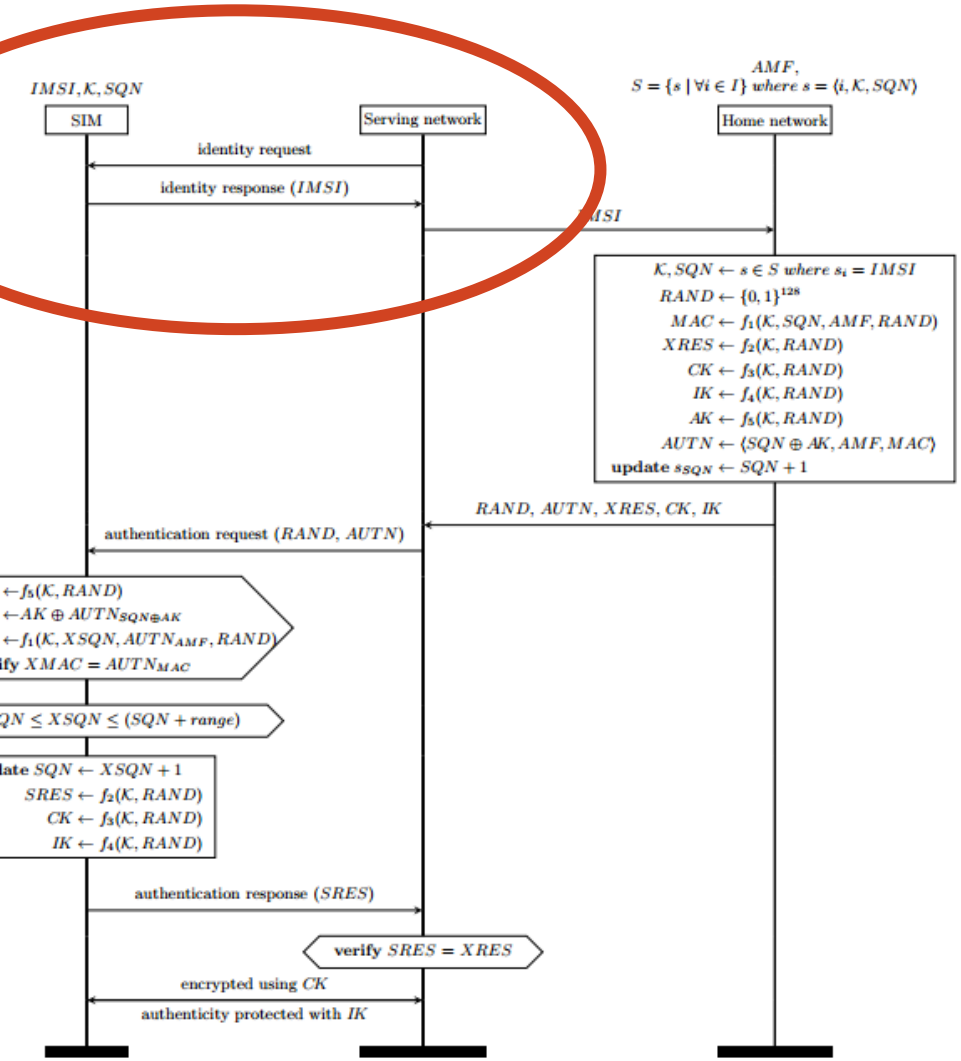
# ackground – 3GPP Identifiers

**International Mobile Subscriber Identifier** (IMSI): 15 digit number; main identifier and belongs to one SIM card

**Temporary Mobile Subscriber Identifier** (TMSI): Temporary pseudonym provided to protect against traceability attacks; updated when phone moves to a different region

**International Mobile Equipment Identifier** (IMEI): 15 digit number that identifies the phone – used to counteract phone theft

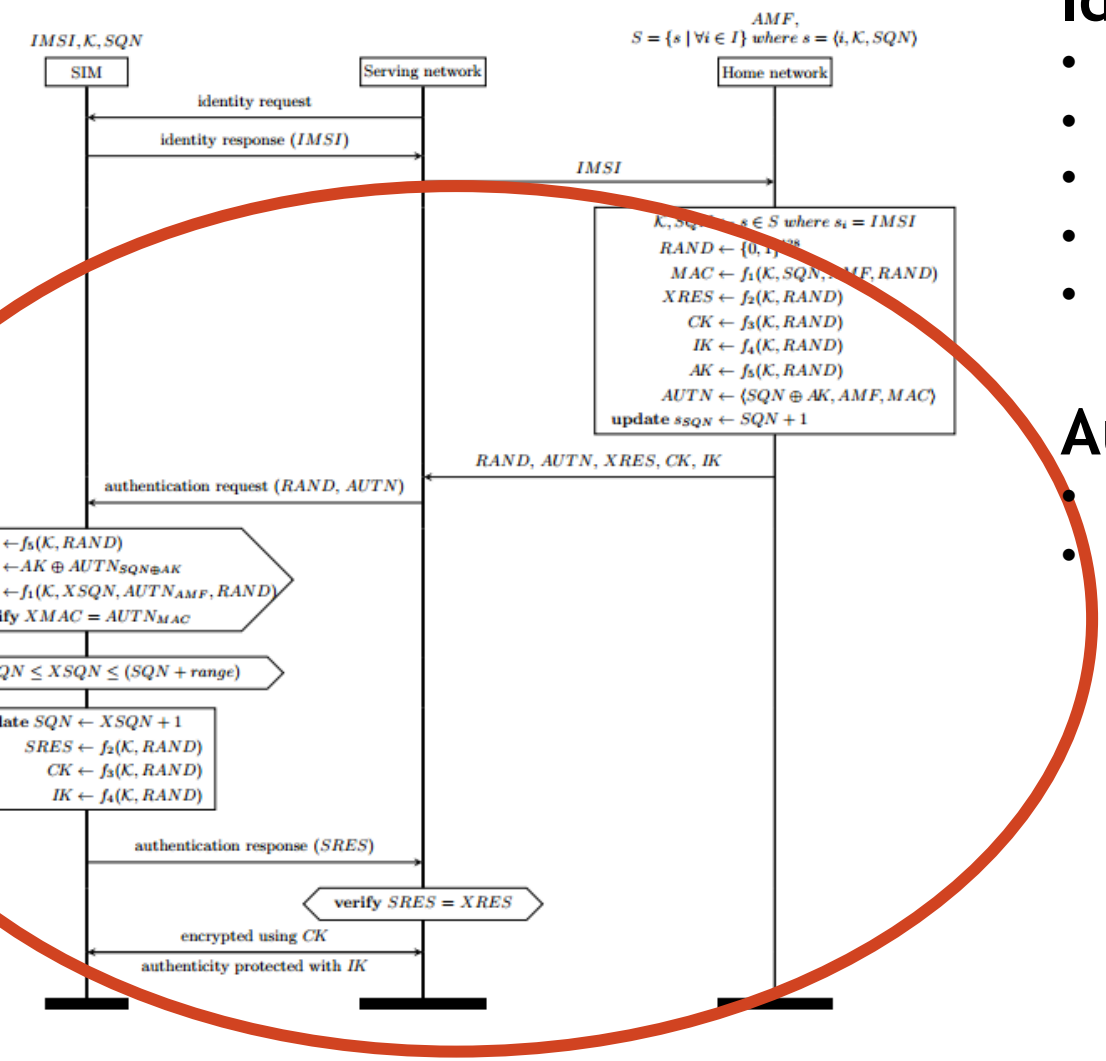
# GPP Protocol Overview




## Identification

- Cell towers broadcast identifiers
- Mobile phones look for certain networks using
- Mobile phone requests a channel
- Cell tower sends requests, including SIM ident
- Mobile phone sends response

# GPP Protocol Overview




## Identification

- Cell towers broadcast identifiers
- Mobile phones look for certain networks using
- Mobile phone requests a channel
- Cell tower sends requests, including SIM ident
- Mobile phone sends response

## Authentication

- Symmetric Key Encryption
- Sequence Number to combat replay attacks

# GPP Protocol – Authentication Details

- Authentication and Key Agreement (AKA) protocol
- Roaming taken care of through split between **home** and **serving** networks
- Home network sends a random number (RAND) as a challenge, along with the corresponding response, keys, authorization token (AUTN) and sequence number
- SIM checks authentication, checks sequence number, then computes response and sends to serving network.

# o what's the problem?

IMSI Catching attacks – Passive attacks observe traffic and store IMSI, and active attacks set up a fake base station (similar to a MITM attack)

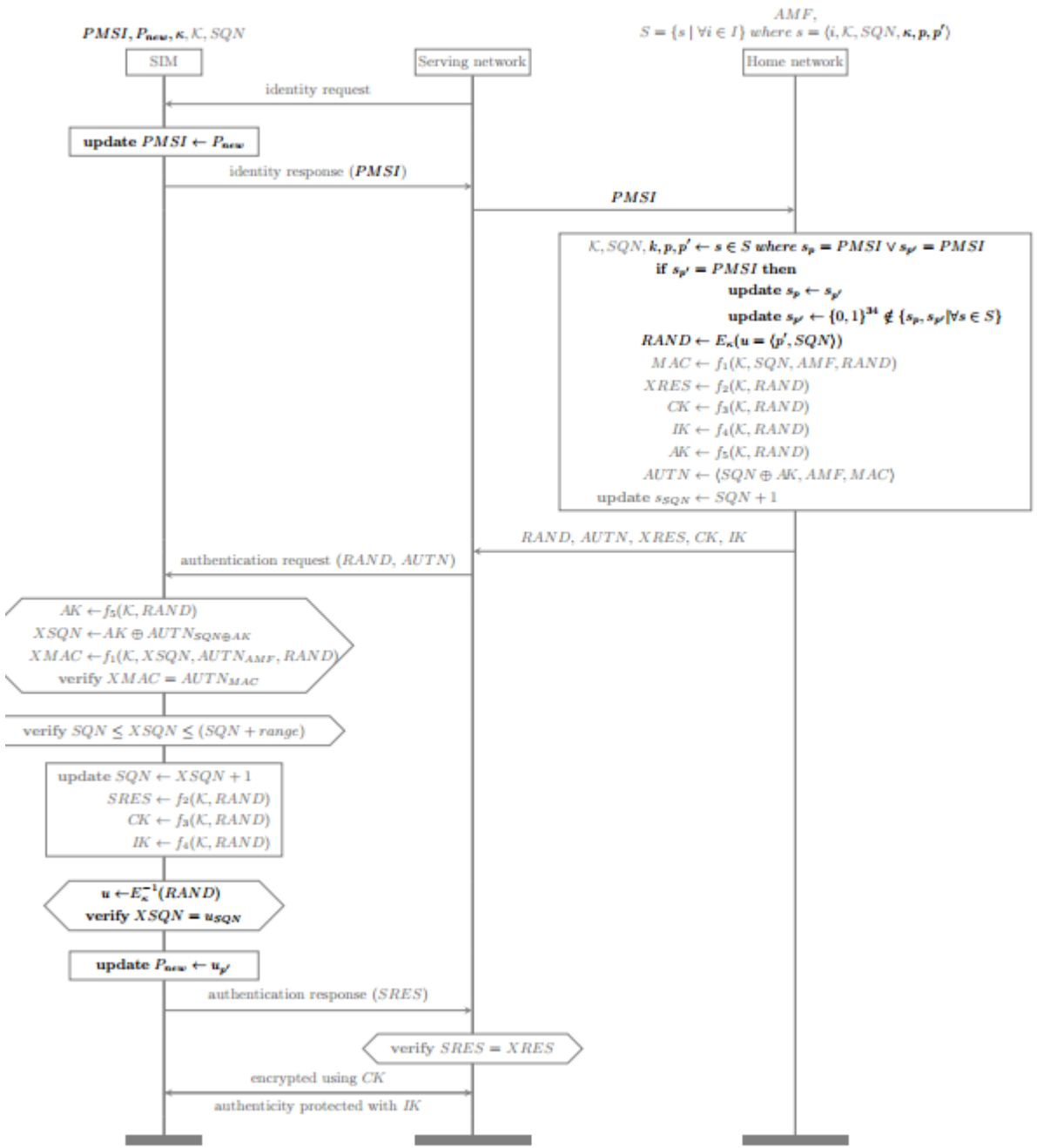
Why do we care? IMSI transmissions leak your approximate location, leading to monitoring or tracking attacks

Underlying problem: use of symmetric cryptography means there needs to be an identification phase before mutual authentication

Previous solutions: randomizing, encryption

# roposed Solution

- New variable: Psuedo Mobile Subscriber Identifier (PMSI)
- During authentication, server provides SIM with new PMSI
- SIM uses PMSI next time it identifies itself
- Server and SIM need to store new secret key, current PMSI and new PMSI


$PMSI, P_{new}, \kappa, \mathcal{K}, SQN$
SIM
Serving network
$AMF,$
$S = \{s \mid \forall i \in I\}$ where $s = \langle i, \mathcal{K}, SQN, \kappa, \mathbf{p}, \mathbf{p}' \rangle$
Home network
identity request
update $PMSI \leftarrow P_{new}$
identity response ($PMSI$)
$PMSI$
$\mathcal{K}, SQN, \mathbf{k}, \mathbf{p}, \mathbf{p}' \leftarrow s \in S$ where $s_p = PMSI \vee s_{p'} = PMSI$
if $s_{p'} = PMSI$ then
update $s_p \leftarrow s_{p'}$
update $s_{p'} \leftarrow \{0,1\}^{34} \notin \{s_p, s_{p'} | \forall s \in S\}$
$RAND \leftarrow E_\kappa(u = \langle p', SQN \rangle)$
$MAC \leftarrow f_1(\mathcal{K}, SQN, AMF, RAND)$
$XRES \leftarrow f_2(\mathcal{K}, RAND)$
$CK \leftarrow f_3(\mathcal{K}, RAND)$
$IK \leftarrow f_4(\mathcal{K}, RAND)$
$AK \leftarrow f_5(\mathcal{K}, RAND)$
$AUTN \leftarrow \langle SQN \oplus AK, AMF, MAC \rangle$
update $s_{SQN} \leftarrow SQN + 1$
$RAND, AUTN, XRES, CK, IK$
authentication request ($RAND$, $AUTN$)
$AK \leftarrow f_5(\mathcal{K}, RAND)$
$XSQN \leftarrow AK \oplus AUTN_{SQN \oplus AK}$
$XMAC \leftarrow f_1(\mathcal{K}, XSQN, AUTN_{AMF}, RAND)$
verify $XMAC = AUTN_{MAC}$
verify $SQN \leq XSQN \leq (SQN + range)$
update $SQN \leftarrow XSQN + 1$
$SRES \leftarrow f_2(\mathcal{K}, RAND)$
$CK \leftarrow f_3(\mathcal{K}, RAND)$
$IK \leftarrow f_4(\mathcal{K}, RAND)$
$u \leftarrow E_\kappa^{-1}(RAND)$
verify $XSQN = u_{SQN}$
update $P_{new} \leftarrow u_{p'}$
authentication response ($SRES$)
verify $SRES = XRES$
encrypted using $CK$
authenticity protected with $IK$

# roposed Solution – 2G

No network authentication, no sequence numbers

Add sequence numbers to the solution, and accept a larger set of SQN values to prevent replay attacks

To prevent faking the base station (active attack), the server has a cryptographic MAC using a secret key.

Cryptographic MAC also prevents DoS attacks forcing the sequence numbers out of sync

# nalysis – How does the solution perform?

Passive attacks – stopped because the use of changing pseudonyms

Active attacks – stopped through the use of secret keys

MITM - still there

Traceability – better than current use of TMSI, as switching PMSI will refresh TMSI

PMSI still reveals home country and home network – *k*-anonymity

All necessary variables fit in the current space

- Challenge is 16 bytes (128 bits)
- 34 bits for PMSI
- 48 bits for SQN

# ow easily could it roll out?

Don’t swap the SIMs – Update them remotely!

Backwards compatible

Low computational overhead

Small overhead for serving network because SIM switching to new PMSI will look like a new phone

Proverif shows that new system has unlinkability & authentication given that the cryptography doesn’t break

# ummary

- First work combatting IMSI catching in 3GPP networks
- Use of changing pseudonyms (PMSI) for identification
- Unlinkabiltiy and authentication
- Easily deployed by service providers

# iscussion

What are the main advantages to this approach?

Do you think the defenses provided are sufficient?

How relevant is this paper today?

What limitations does this paper have?