HELSINGIN YLIOPISTO
HELSINGFORS UNIVERSITET
UNIVERSITY OF HELSINKI
MATEMATTIS-LUONNONTIETEELLINEN TIEDEKUNTA
MATEMATISK-NATURVETENSKAPLIGA FAKULTETEN
FACULTY OF SCIENCE

Gizem Akman
Mohsin Khan
Valtteri Niemi
Department of Computer Science, University of Helsinki

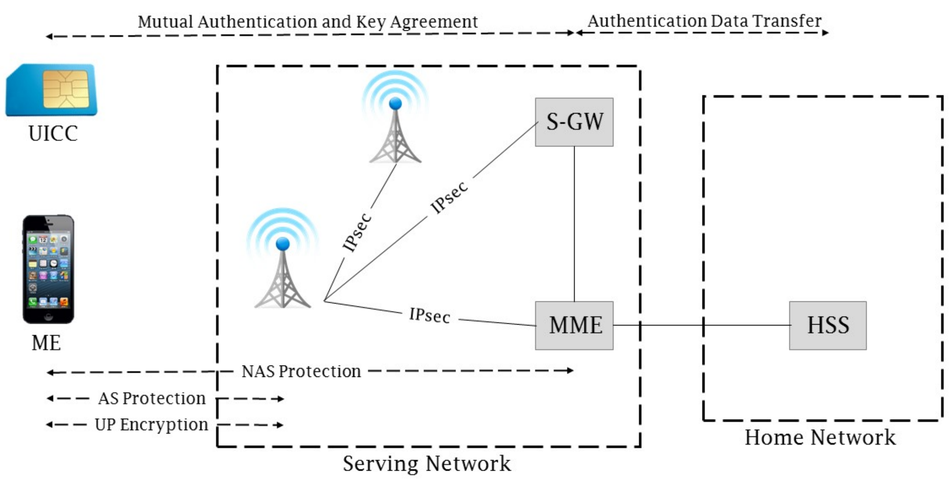
# IDENTITY PRIVACY IN 5G

## IMSI

An IMSI (Internation Mobile Subscriber Identity) is the long term identity of a mobile equipment (ME) user. It has three parts: mobile country code (MCC) of 3 digits, mobile network code(MNC) of 2 digits, and mobile subscriber identification number (MSIN) of 10 digits.

$$IMSI = MCC||MNC||MSIN$$

## LTE SECURITY ARCHITECTURE



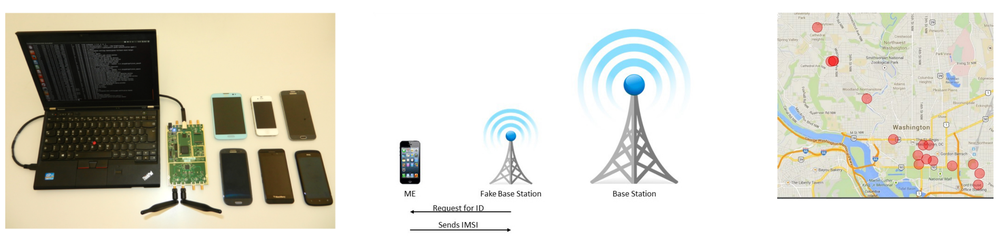

## IMPORTANT FACTS ABOUT LTE/3G/GSM

1. An ME connects to the base station in the vicinity that offers the strongest signal.
2. An ME identifies itself with the user's IMSI at the very first time it connects to a serving network (SN).
3. After the authentication and key agreement (AKA), the ME is given a temporary identity (TMSI) securely.
4. It is possible that either ME or SN loses TMSI causing the ME to remain out of the network.
5. To prevent from being kicked out of the network permanently, ME provides its IMSI in cleartext to any base station that asks for it.

## IMSI CATCHERS IN LTE/3G/GSM

It is a well known mechanism (Ginzboorg and Niemi, 2016), (Shaik et al., 2016).

1. IMSI catcher is a fake base station that impersonates a legitimate base station
2. The IMSI catcher offers strongest signal in the vicinity
3. All the users in the vicinity try to connect with the IMSI catcher since it offers the strongest signal
4. The IMSI catcher simply asks the identity of the ME user that tries to connect
5. Every ME provides its user's IMSI in cleartext in response




IMSI catching is not just a theoretical attack. The rightmost figure above shows how densely the IMSI-catchers existed in Washington in 2014 (Washington Post). To stop the IMSI catchers three different solutions have been published by researchers.

## SOLUTION 1: PUBLIC-KEY

Solution with the public-key for every SN has the requirement of setting up a public key infrastructure (PKI) which is too expensive and hence has not been considered as feasible. However, solution with public-key for the HN is still a potential candidate (Ginzboorg and Niemi, 2016).

### Summary

1. The ME encrypts the IMSI with the public key of HN and sends the ciphertext to HN via SN
2. HN decrypts the ciphertext with its private key and reveals IMSI.
3. HN generates and sends an authentication vector (AV) to the SN.
4. The AV is needed in an authentication and key agreement (AKA) protocol that runs in between ME and SN.

### Pros

1. It doesn't require the ME and HN to be in any synchronized state.

### Cons

1. The public key ciphertexts are much longer than an IMSI. This causes exchange of longer messages during the AKA which is not compatible with legacy SNs.
2. Extra computational load on the home subscription server (HSS) since public-key cryptography is computationally heavy
3. Increased latency

## SOLUTION 2: GROUP-KEY

### Summary

1. Every user belongs to a group in HN. Every group has a group-id and a group-key
2. Group-id is a public information but the group-key is known only by HN and the users belonged to the group
3. When an ME connects to an SN, it encrypts the IMSI using the group-key and sends the encrypted IMSI along with the group-id
4. The SN forwards the encrypted IMSI and group-id to HN.
5. HN resolves the group-key from the group-id and decrypt the IMSI
6. HN sends the IMSI the SN, together with AV that is needed for running the AKA procedure.

### Pros and Cons

We have a trade-off situation for the size of the group (Ginzboorg and Niemi, 2016):

1. If the group is too small, the group identity reveals too much about the user identity. For instance, it could be the case that only one member of the group is roaming in a certain country at a certain time point.
2. If the group is too large, then too many people would have access to the group key and the active attacker could be an insider from the group.

## SOLUTION 3: PSEUDONYM

1. Every user having an IMSI is given a pseudonym $P$ by the HN initially.
2. When the user identifies itself with $P$ to the SN, the SN forwards $P$ to the HN
3. In response, the HN sends a new pseudonym $P^{'}$ to the SN encrypted by the secret key $K$ or by some other secret key derived from $K$. The encrypted $P^{'}$ is embedded in the random challenge RAND that is needed for AKA.
4. The SN runs the AKA with UE based on the AV. It also sends the encrypted new pseudonym $P^{'}$ to the UE.
5. If the AKA is successful then the ME will be able to decrypt it and obtain $P^{'}$. The old pseudonym $P$ will be continued in use instead of IMSI until the UE tries to connect via another SN.
6. When the UE tries to connect to the network via a new SN, the new SN has no knowledge about $P$. At this point instead of sending the IMSI, the UE identifies itself with $P^{'}$.

### Pros

1. Potentially compatible (if not readily) with legacy SNs and USIMs.

### Cons

1. It requires synchronized states in between ME and HN. Our research is currently focusing on this synchronization with minimal effort in the HSS. Currently our solution can generate an AV in at most 0.24 milliseconds.
2. The size of the pseudonym space is only $10^{10}$. It seems the history of pseudonyms used has to be stored for a while because of billing. Storing this history will create some pressure on this space. We are working on estimating the pressure on this space and the usability of multiple MNC for a single operator to overcome the problem

## CONCLUSIONS

IMSI-catching is an attack that has existed though-out the history of cellular network. 3GPP focused on mitigating the attack during the design phase of GSM, 3G and LTE. But eventually no solution was adopted because of the added complexities they came with. We have studied the aforementioned three solution candidates. We found the pseudonym approach to be the most appealing one because it has the opportunity to be implemented in 5G even when the SN is of from older generation.

## REFERENCES

Ginzboorg and Niemi. *Privacy of the Long-Term Identities in Cellular Networks.* MOBIMEDIA, 2016.

Shaik, Borgaonkar, Asokan, Niemi, and Seifert. *Practical Attacks Against Privacy and Availability in 4G/LTE Mobile Communication Systems.* NDSS, 2016.