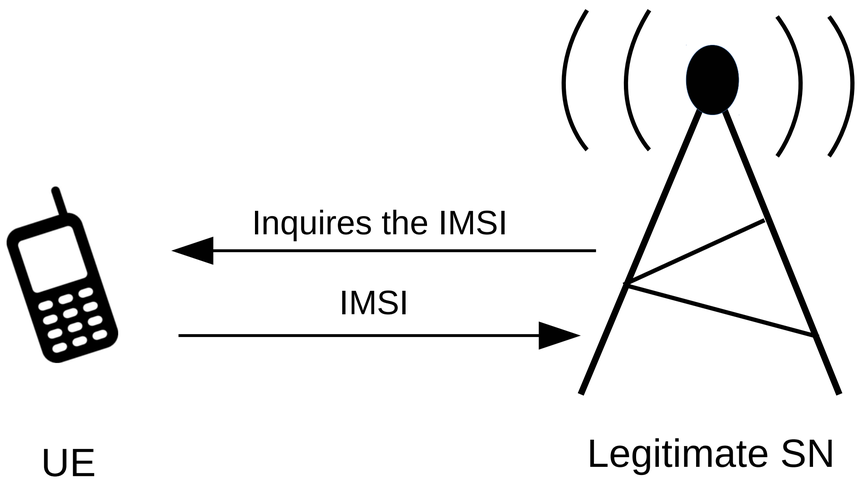
HELSINGIN YLIOPISTO
HELSINGFORS UNIVERSITET
UNIVERSITY OF HELSINKI
MATEMAATTIS-LUONNONTIETEELLINEN TIEDEKUNTA
MATEMATISK-NATURVETENSKAPLIGA FAKULTETEN
FACULTY OF SCIENCE

HOW A PSEUDONYM BASED SOLUTION TO DEFEAT IMSI-CATCHERS OPENS A VULNERABILITY TO DoS

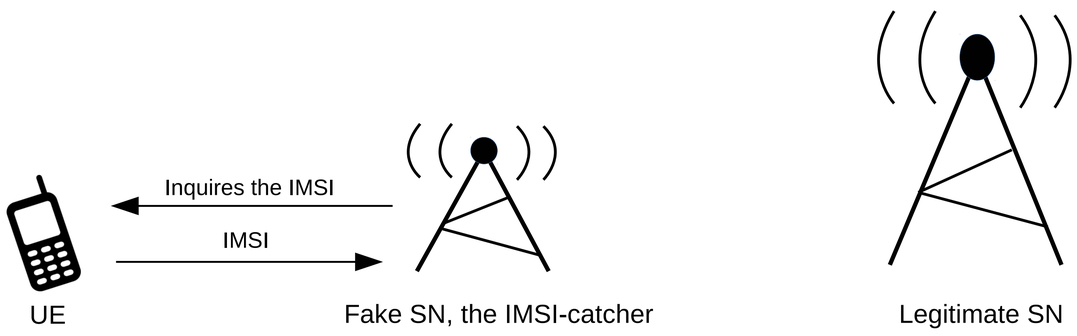
Mohsin Khan
Kimmo Järvinen
Philip Ginzboorg
Valtteri Niemi
Department of Computer Science
University of Helsinki

IMSI-CATCHERS

1. A user equipment (UE) has to identify itself before attaching to a serving network (SN)
2. Before identification, there is no agreed security context in between a UE and the SN
3. As a result, whenever an SN inquires a UE's IMSI, the UE responds with IMSI in cleartext



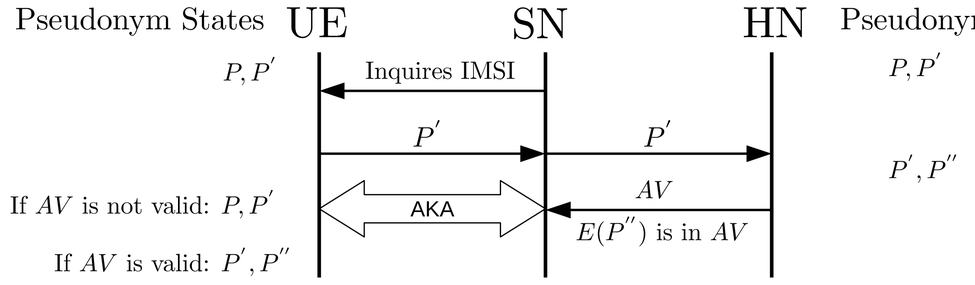
An IMSI-catcher is a fake SN that impersonates a legitimate SN. An IMSI-catcher sends an IMSI inquiry to a UE. According to above protocol, the UE responds with the IMSI in cleartext.



- IMSI-catchers violate identity privacy and UEs need to be protected from them
- IMSI-looking temporary identifiers known as pseudonyms are proposed (Ginzboorg and Niemi, MOBIMEDIA'16; Norrman et al., MOBIMEDIA'16; Fabian van den Broek, CCS'15; Khan M.S.A., SSR'15) to defeat IMSI-catchers
- We show that all of them defeat the IMSI-catchers but open a vulnerability to a DoS attack
- We choose (Fabian van den Broek, CCS'15) paper to demonstrate our attack. Similar attack can be mounted on others

PSEUDONYM BASED SOLUTION

In (Fabian van den Broek, CCS'15), the pseudonym based solution works as follows. Every user UE is given IMSI-looking temporary identifiers we call pseudonyms. When a network inquires for IMSI, the UE responds with a pseudonym instead of IMSI.



1. A pair P, P' of pseudonyms is involved with every UE
2. Whenever a network inquires for IMSI, the UE responds either with P or P'
3. If UE responds with P, the pseudonym states do not change
4. If UE responds with P', the pseudonym states change from P, P' to P', P''
5. P'' is generated at home network (HN)
6. P'' is encrypted and piggybacked with the authentication vector (AV)
7. Nobody except the UE can know P'' until the UE uses P'' as a response of an IMSI inquiry

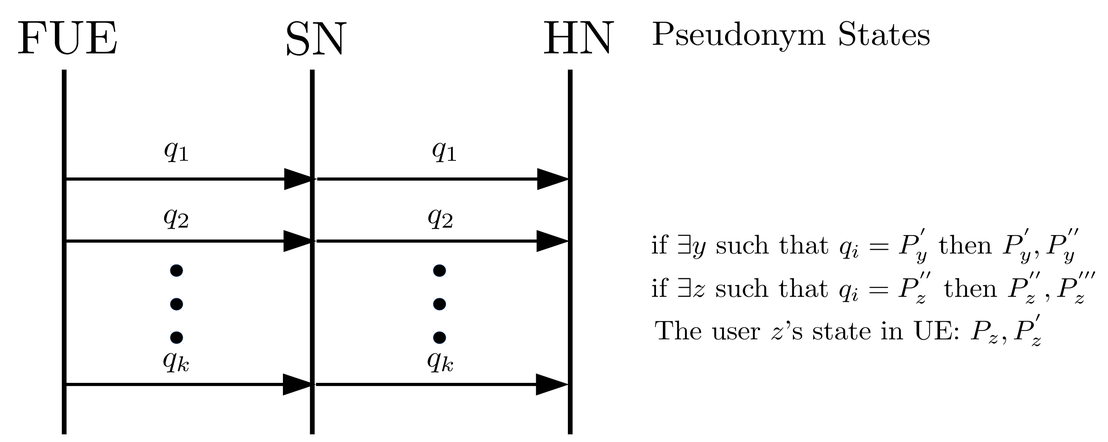
Weakness

This solution has a weakness in item 4. The HN does not authenticate the origin of the message that carries a pseudonym from UE to HN and generates a new pseudonym P'' whenever it observes the pseudonym P'. This fact can be exploited to mount a DoS attack.

A DoS ATTACK

The DoS attack forces the pseudonym state of a user in HN to go to a state which is completely different from the pseudonym state of the user in its UE. Consequently the UE will not be able to identify itself successfully any more to the network. The attack is as follows:

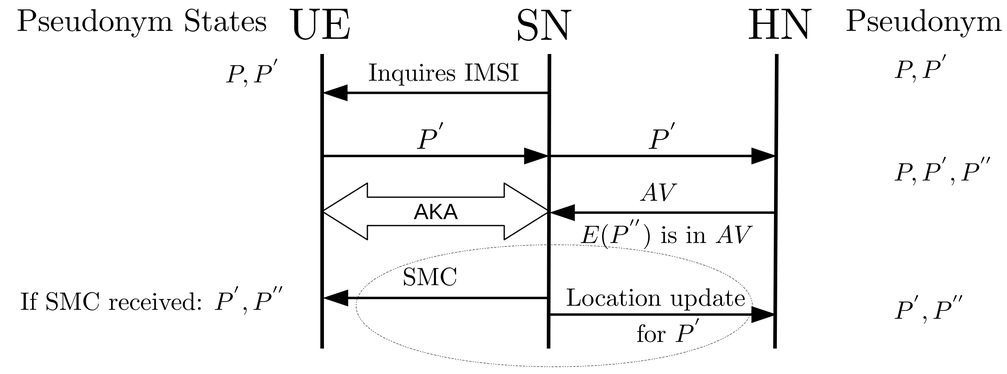
1. A fake UE (FUE) sends a pseudonym q_1 to a legitimate SN and SN forwards q_1 to the HN
2. Let P_x, P'_x be the pseudonym state of a user x. Let us assume that $q_1 = P'_x$. The pseudonym state at HN will be updated to P'_x, P''_x
3. The FUE then sends q_2 to the legitimate SN and the SN forwards q_2 to respective HN
4. Let us assume that $q_2 = P''_x$. The pseudonym state at HN will be updated to P''_x, P'''_x
5. Pseudonym state for the user x is still P, P' in UE, but P''_x, P'''_x in HN



- Now if k is a large number, we can expect that there would be many users x for which $\exists i, j$ such that $1 \leq i < j \leq k$, $q_i = P'_x$ and $q_j = P''_x$
- All such users x would then have different pseudonym states in their UE than in the HN
- If an attacker mounts such an attack in a distributed fashion by employing hundreds of FUEs, the whole IMSI space (10^{10}) can be exhausted twice within few hours and consequently the whole network will go out of service
- This attack can be used in cyber warfare, terrorism or blackmailing the network operator

SOLUTION

1. Authenticating the message that carries a pseudonym from the UE to the SN using MAC
   (a) The HN knows if the pseudonym is sent by the user associated with the pseudonym
   (b) This solution works in 5G but doesn't work in 3G or 4G
2. Use existing messages to confirm HN that UE has received the new pseudonym
   (a) Location update message sent by an SN to the HN can be used
   (b) This solution introduces a new DoS attack by introducing a man in the middle (MITM)
   (c) An MITM can possibly be detected using Security mode command (SMC)



If no location update is received for pseudonym P' but P'' is observed at the HN, the new pseudonym generated by the HN is still P''. It is trusted that if an SN is capable of sending a valid SMC to the UE after an AKA, the SN will send the location update to the HN.

REFERENCES

J. d. R. Fabian van den Broek, Roel Verdult. *Defeating IMSI Catchers.* CCS'15.

Ginzboorg and Niemi. *Privacy of the Long-Term Identities in Cellular Networks.* MOBIMEDIA'16.

M. C. Khan M.S.A. *Improving Air Interface User Privacy in Mobile Telephony.* SSR'15.

Norrman, Näslund, and Elena. *Protecting IMSI and User Privacy in 5G Networks.* MOBIMEDIA'16.