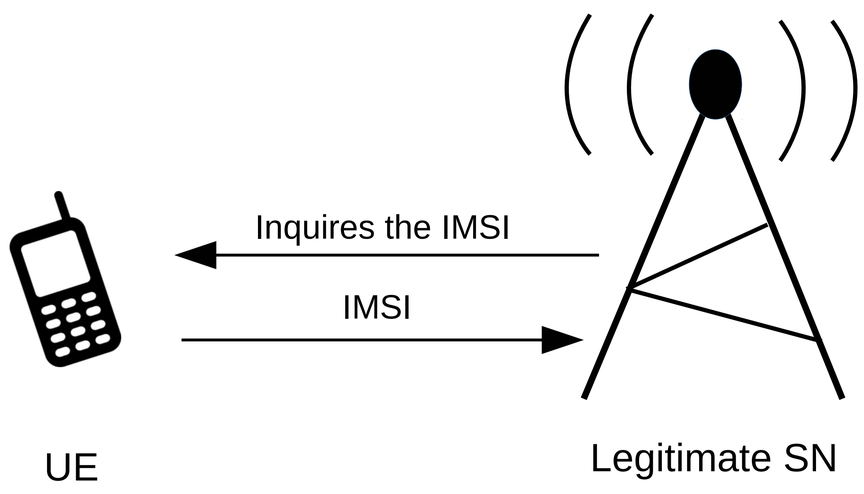
HELSINGIN YLIOPISTO
HELSINGFORS UNIVERSITET
UNIVERSITY OF HELSINKI
MATEMAATTIS-LUONNONTIETEELLINEN TIEDEKUNTA
MATEMATISK-NATURVETENSKAPLIGA FAKULTETEN
FACULTY OF SCIENCE

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

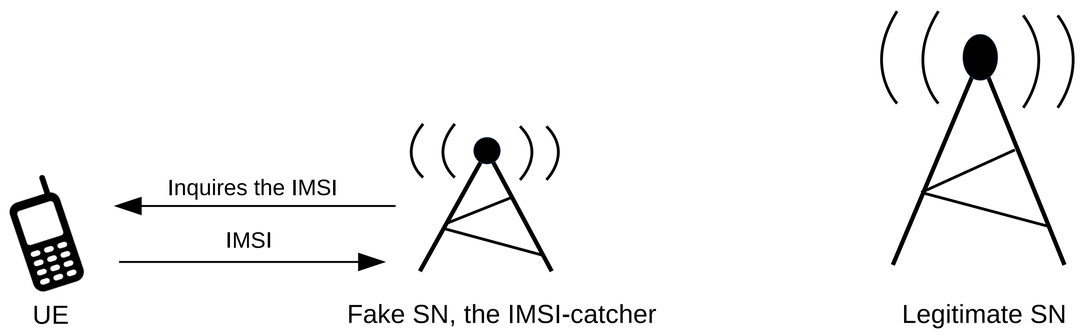
Mohsin Khan
Kimmo Järvinen
Philip Ginzboorg
Valtteri Niemi
Department of Computer Science, University of Helsinki

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 to the inquiry by providing the IMSI in cleartext.



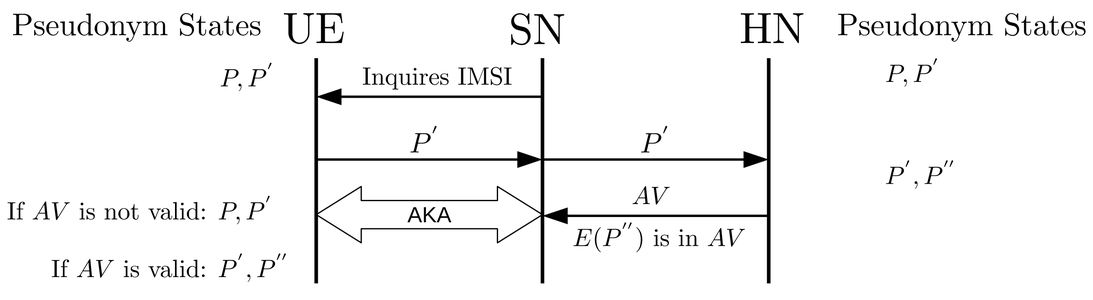
An IMSI-catcher is a fake SN that impersonates a legitimate SN. IMSI-catcher sends an IMSI inquiry to a UE. According to above mentioned protocol, the UE responds with the IMSI in cleartext.



- IMSI-catchers violate identity privacy and UEs needs to be protected from them.
- IMSI-looking temporary identifiers known as pseudonyms are proposed (Ginzboorg and Niemi, 2016; Norrman et al., 2016; Fabian van den Broek, 2015; Khan M.S.A., 2015) to defeat IMSI-catchers
- All these proposed solutions defeat the IMSI-catchers but open vulnerability to a DoS attack
- We choose (Fabian van den Broek, 2015) paper to demonstrate our attack. The same attack can be mounted on others.

PSEUDONYM BASED SOLUTION

In (Fabian van den Broek, 2015), the pseudonym based solution works as follows. Every user equipment (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 are 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), encrypted and piggybacked with AV to the SN and finally to the UE
6. Nobody except the UE can know P'' until the UE uses P'' as a response of an IMSI inquiry

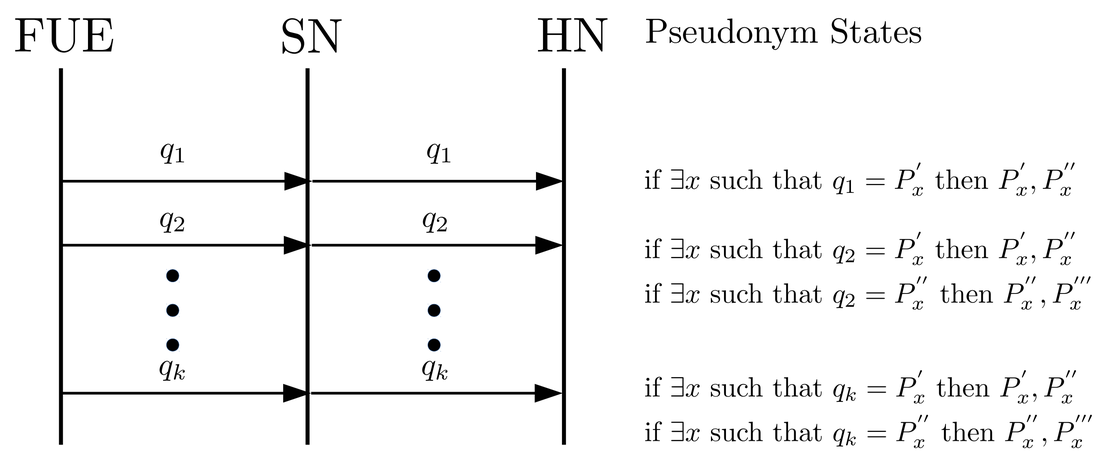
Weakness

1. The origin of the weakness is in item 4 in the above list
2. The HN does not check the message origin authentication a received pseudonym P'
3. That gives the opportunity to an attacker to guess and send a pseudonym to the HN via a legitimate SN, leading to a new pseudonym in HN

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 sucessfully anymore to the network. The attack is as follows:

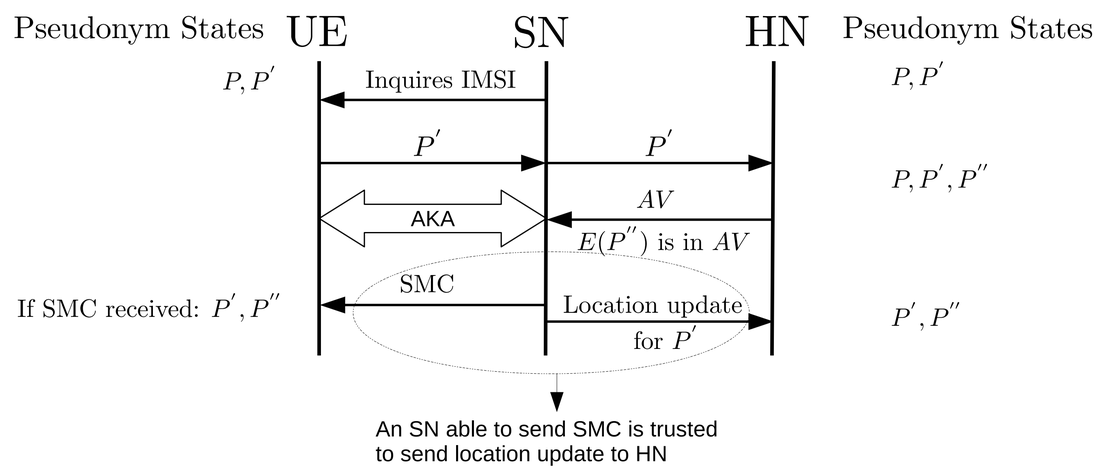
1. A fake UE (FUE) sends a pseudonym q_1 to a legitimate SN and SN forwards q_1 to respective HN
2. Let P_x, P_x' be the pseudonym state for a subscriber whose IMSI is x. Let us assume that $q_1 = P_x'$. The pseudonym state at HN will be updated to P_x', P_x''
3. The FUE then sends q_2 to the legitimate 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, completely different from the pseudonym state at 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 $1 \leq i < j \leq k$ such that $q_i = P_x'$ 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 distrubted fashion by employing hundreds of FUE, the whole IMSI space (10^{10}) can be exhusted within few hours and consequently the whole network will go out of service
- This attack can be used in cyberwarfare, terrorizing mass people or even blackmailing the network operator

SOLUTION

1. Use integrity protection of the message that carries 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) of UE and SN
   (c) There is a possiblity to defeat the MITM attack by confirming the UE that the pseudonym sent by an SN is not an MITM
   (d) Security mode command (SMC) might possibly be used to detect an MITM



REFERENCES

J. d. R. Fabian van den Broek, Roel Verdult. *Defeating IMSI Catchers.* CCS, 2015.

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

M. C. Khan M.S.A. *Improving Air Interface User Privacy in Mobile Telephony.* SSR, 2015.

Norrman, Näslund, and Elena. *Protecting IMSI and User Privacy in 5G Networks.* MOBIMEDIA, 2016.