Defeating IMSI-Catchers Using Pseudonyms: A DDoS Attack and Solution

Mohsin Khan[1(Γ)], Kimmo Järvinen[1], Philip Ginzboorg[2], and Valtteri Niemi[1]

[1]University of Helsinki, Helsinki, Finland
{mohsin.khan, kimmo.u.jarvinen, valtteri.niemi}@helsinki.fi
[2] Huawei Technolgies
philip.ginzboorg@huawei.com

Abstract. IMSI-catchers are still in existence in all the 3GPP defined networks. Pseudonym based solutions to defeat IMSI-catchers have been published in the recent years. We have found one vulnerability in these solutions. The vulnerability enables an attacker to convince the home network (HN) to forget an old pseudonym of a legitimate UE without any participation of the legitimate UE. A malicious UE can exploit this vulnerability to kick a legitimate UE out of service. We show that, exploiting this vulnerability, a novel DDoS attack can be mounted against an entire network. The attack can send 50 percent of the UEs out of service using a reasonably large botnet of mobile users. We justify our claim by an analytical argument backed by a simulation. Even though, in principle, a malicious serving network (SN) can also exploit the vulnerability, we argue that the SN can not gain anything meaningful before the attack is detected and stopped. Besides, an SN can behave maliciously in other even more fatal ways. We present a solution to fight against the DDoS attack by using the location update message sent by an SN to an HN. We argue that our solution is immune to the the DDoS attack, protects the identity privacy, and remains backward compatible. We also discuss other practical issues of the usability of pseudonyms from charging and lawful interception point of view that appear to be ignored so far.

Keywords: 3GPP · IMSI-catchers · Pseudonym · Idenity · Privacy

1 Introduction

International mobile subscriber identity (IMSI) is the global identifier of a mobile phone subscriber. IMSI-catchers are devices that can create a list of IMSIs of the subscribers present in a certain geographical area. IMSI catching is an identity privacy problem. The problem has been known for long but still prevailing in all the 3GPP defined cellular networks (GSM, UMTS, LTE) for decades cite.

How IMSI-catchers catch IMSI? A subscriber's user equipment (UE) has to identify itself to the network before connecting. The identification message has to be sent in plain-text because the security of the network is based on

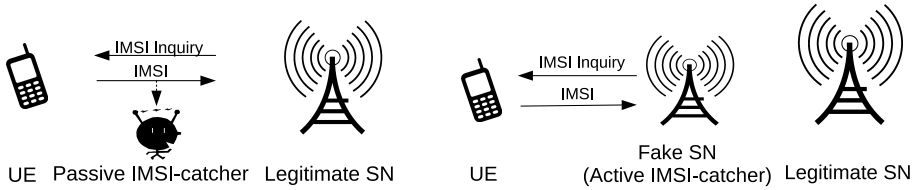

Fig. 1: IMSI-catcher

symmetric key cryptography cite. In symmetric key cryptography, a secret key has to be shared before starting any encryption. The home network (HN) stores a secret key for every subscriber in the subscriber database. The secret keys are also securely stored in the respective subscriber identity module (SIM). However, the HN needs to know the identity of the subscriber to choose the right secret key to start encrypting or decrypting any message. So, when an unknown UE appears, the network makes an IMSI inquiry to the UE . Consequently, the UE has to sent the IMSI in plain-text cite.

A passive IMSI-catcher who is just listening to the radio channel can read the identification message. An active IMSI-catcher who sets up a fake base station and impersonates a legitimate serving network (SN), do an IMSI inquiry to all the UEs that try to connect. The UEs respond with their respective IMSIs in plain-text cite. See Figure 1.

What an IMSI catcher can do with the caught IMSIs? With the caught IMSIs, an IMSI catcher can monitor who are coming and leaving a certain geographical area cite. An IMSI catcher can also track the locations of a targeted individual cite. There are other range of more sophisticated active man in the middle attacks that start with catching the IMSI of a subscriber, e.g., attacking the confidentiality of user data by downgrading the air interface encryption cite. Now a days, all these advanced attackers are called IMSI-catchers. However, in this paper, we will limit our discussion to the attackers who only gathers a list of IMSIs.

How available IMSI-catchers are in real life?

Current state of art in defeating IMSI-catchers

Our Contribution

Overview

2 Background

Identification in the existing networks

Authentication in the existing networks we need to discuss the authentication mechanism because the pseudonym based approach uses the messages in the authentication protocol to piggyback the messages required to be sent across.

How pseudonym based solution works

3 Vulnerability of Pseudonym Based Solutions

The fundamental idea of all the pseudonym based solutions [1,2,3,4] are essentially the same. When a certain old pseudonym is used by a user, the HN computes a new pseudonym, associate the new pseudonym to the respective IMSI and forget a certain old pseudonym. Forgetting an old pseudonym is important so that it can be reused.

If a fake UE (FUE) uses a random pseudonym and if by chance, the random pseudonym is associated with a legitimate UE, the HN forgets an old pseudonym for the legitimate UE. The network also computes a new pseudonym which the legitimate UE has no knowledge of. If the network remembers k number of pseudonyms before forgetting any, the FUE needs to make the attack k times so that the network forgets all the pseudonyms that the legitimate user possesses. This is a fatal damage to the identity of the UE, because all the successive authentications of the UE will fail.

If there are n number of subscribers in an HN, then the probability of the above attack being successful is $\frac{n}{10^{10k}}$, which is apparently a tiny probability. However, in Section **??**, we will show how this tiny probability can be exploited into a fatal DDoS attack. We will use the BVR scheme to demonstrate the attack, eve though similar attacks can be mounted against the other schemes also.

3.1 The DOS Attack Against the BVR Scheme

In the BVR scheme, a subscriber s has two pseudonyms (s_p, s'_p) in the HN and two pseudonyms $(PMSI, P_{new})$ in the UE. In an ideal case, $PMSI = s_p, P_{new} = s_{p'}$.

The attack is mounted by an FUE. The FUE sends a random pseudonym q_1 to a legitimate SN. The legitimate SN forwards the pseudonym to the respective HN. If by chance, $q_1 = s_{p'}$, the HN forgets s_p and sets $s_p \leftarrow s_{p'}$. The HN also generates an unused pseudonym p'' and sets $s_{p'} \leftarrow p''$. As a result, in the HN, the current pseudonym-state for the subscriber s is $(s_p = P_{new}, s_{p'} \neq PMSI, P_{new})$. At this stage, there is only one pseudonym present both at the UE and HN.

The FUE sends another pseudonym q_2. If again by chance, $q_2 = s_{p'}$, then the HN again forgets s_p, sets $s_p \leftarrow s'_p$. HN also generates an unused pseudonym p''' and sets $s_{p'} \leftarrow p'''$. Consequently, in HN, the current pseudonym-state of subscriber s becomes $(s_p \neq PMSI, P_{new}, s_{p'} \neq PMSI, P_{new})$. If there were no pseudonyms sent by the HN to the legitimate UE while the attack was mounted,

the pseudonym-state of the UE remains as $(PMSI, P_{new})$. So at this stage, there is no pseudonym present at both of the UE and HN sides. See Figure 2. The next time the user would need to authenticate itself to a network, the authentication will fail and hence be denied any service.

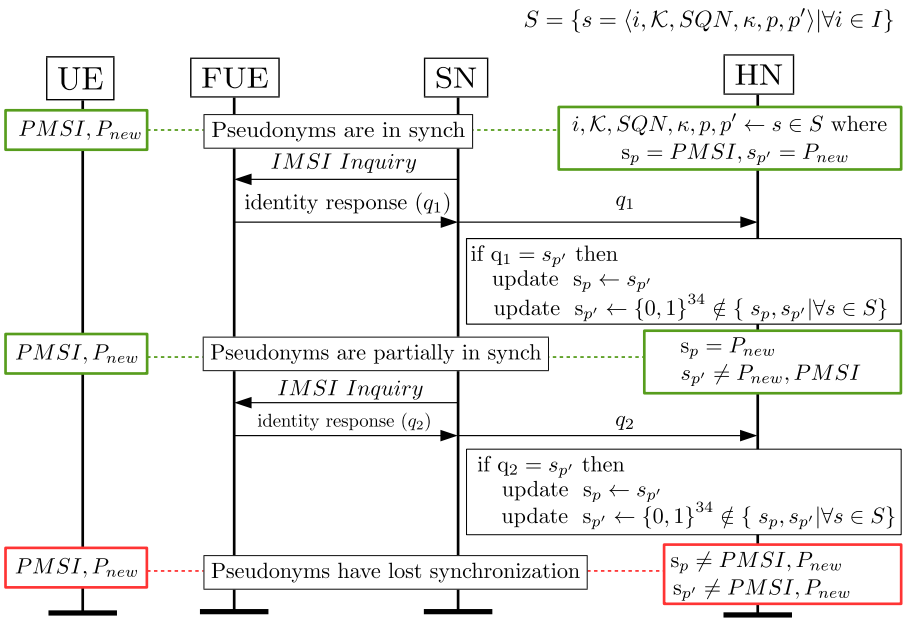

Fig. 2: A DoS Attack against the BVR scheme

If the probability of success of the above attack to a targeted user is $\frac{1}{10^{20}}$. The probability of success of the attack to any user is $\frac{n}{10^{20}}$. This is a tiny probability. But in Section **??**, we show that a very efficient and fatal DDoS attack can be mounted using by exploiting this tiny probability.

3.2 The DDOS Attack

In the DDoS attack, many FUEs send many pseudonyms to the targeted HN via a legitimate SN. The HN processes the pseudonyms as they arrive. Let us assume, the total number of pseudonyms sent to the HN is a large integer m. In this case, a user s will be affected by the attack if there exists two integers $0 < x < y \leq m$ such that $q_x = s_{p'}$ and $q_y = s_{p'}$. We have considered two different ways to mount this attack. In one way, the pseudonyms that are sent to the network are chosen randomly with replacement, which means the attack

might sent one pseudonym more than once to the network. In the other way, the pseudonyms are chosen without replacement, which means the attack send one pseudonym only once.

With replacement In this case, the expected number of affected users $E[u_a]$ is

$$E[u_a] = n\left(1 - \left(1 - \frac{1}{10^{10}}\right)^m - m\left(\frac{1}{10^{10}}\right)\left(1 - \frac{1}{10^{10}}\right)^{(m-1)}\right) \quad (1)$$

See Appendix **??** for the derivation. We have run a simulation of this attack and found that above model is fairly accurate. See Figure 3.

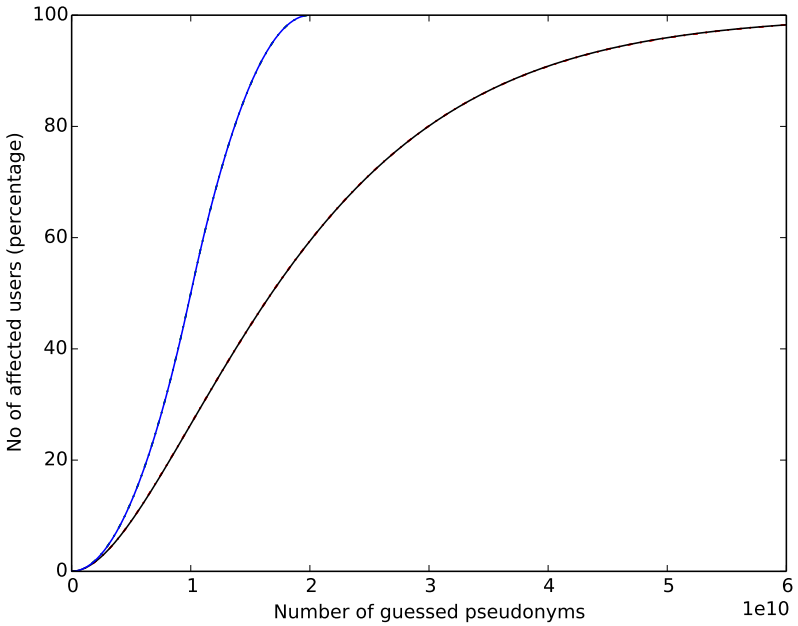

Fig. 3: Success Rate of the DDoS Attack. IMSI space 10^{10}. Number of subscribers in HN is 10^7. The black and blue line presents the expected number of affected users in case of the with and without replacement attacks respectively. Under the black line, there are three red lines which represent the results of three simulations of with-replacement attack. Under the blue line, there are three green lines which represent the results of three simulations of without-replacement attack.

Without replacement In this case the attacker runs two rounds of the attack. In the first round the attacker sends all the pseudonyms in the IMSI-space without replacement, means each pseudonym is sent exactly once. Once the first round is completed, the attacker runs the attack for one more round. However, after sending m number of pseudonyms to the network, the expected number of affected users $E[u_a]$ is

$$E\big[u_a\big] = \begin{cases} \frac{m^2}{2 \cdot 10^{10}}, & \text{if } 0 < m \leq 10^{10} \\ 2m - 10^{10} - \frac{m^2}{2 \cdot 10^{10}}, & \text{if } 10^{10} < m \leq 2 \cdot 10^{10} \end{cases} \tag{2}$$

See Appendix **??** for the derivation. We have run a simulation of this attack and found that above model is fairly accurate. See Figure 3. Note that, this is an estimation where the without-replacement attack is not a distributed attack. Rather the attack is mounted by only a single FUE. In case of distributed without-replacement attack, the expected number of affected users will be less than what is shown in the plot. However, we believe that, the distributed without-replacement attack will have higher number of affected users than that of distributed with-replacement attack.

3.3 Why SN is not a Potential Adversary

Modeling and Simulation

4 Solution

5 Analysis

why the solution is good what happens in the error cases

6 Related work

how good the newest paper really is

7 Usability of pseudonyms

8 Conclusion

Acknowledgement.

References

1. Van den Broek, F., Verdult, R., de Ruiter, J.: Defeating IMSI Catchers. In: Proceedings of the 22nd ACM SIGSAC Conference on Computer and Communications Security. CCS '15, ACM (2015)
2. Khan, M.S.A., Mitchell, C.J.: Improving Air Interface User Privacy in Mobile Telephony. In: Second International Conference, SSR 2015, Proceedings, Springer International Publishing (2015)
3. Ginzboorg, P., Niemi, V.: Privacy of the long-term identities in cellular networks. In: Proceedings of the 9th EAI International Conference on Mobile Multimedia Communications. MobiMedia '16, ICST (2016)
4. Norrman, K., Näslund, M., Dubrova, E.: Protecting IMSI and User Privacy in 5G Networks. In: Proceedings of the 9th EAI International Conference on Mobile Multimedia Communications. MobiMedia'16, ICST (2016)

References