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

Mohsin Khan[1(✉)], 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. Pseudonym based solutions to defeat IMSI-catchers have been published in the recent years. No fatal vulnerability in these solutions has been reported until this month. However, we have found one vulnerability. The vulnerability enables an attacker to convince the home network (HN) to forget an old pseudonym of a legitimate UE and compute a new one. The attacker does not need any participation of the legitimate UE to mount this attack. A malicious UE or a serving network (SN) 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 cellular 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 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. Hence it is not important to protect against a malicious serving network in this context. We present a solution to fight against the DDoS attack by piggybacking the location update message sent by the serving network to the home network. We present a qualitative analysis of our solution. We argue that our solution is immune to the the DDoS attack and still protects the identity privacy, and remains backward compatible with the legacy networks. 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.

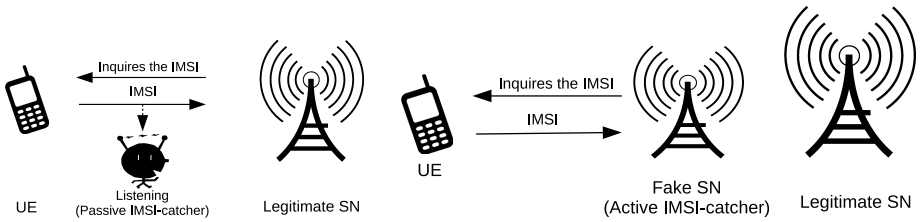

Fig. 1: IMSI-catcher

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 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 Conclusion

Acknowledgement.

References