Concealing Permanent or Long-term Identity of a Subscriber in 5G Using Identity Based Crypto

Mohsin Khan and Valtteri Niemi

University of Helsinki, Department of Computer Science,
P.O. Box 68 (Gustaf Hällsträmin katu 2b)
FI-00014 University of Helsinki
Finland
{mohsin.khan,valtteri.niemi}@helsinki.fi

Abstract. The aspirations for the next generation mobile network (5G) are high. It has a vision of improved security and privacy over the existing LTE network. Subscription privacy of a user has been a historical concern with all the previous generation mobile networks, namely GSM, UMTS, and LTE. While a little improvements have been achieved in securing the privacy of long-term identity of a subscriber, the so called IMSI catchers are still in existence even in the LTE and advanced LTE networks. This report looks into this problem of concealing long-term identity of a subscriber and presents different techniques of using public-key cryptography to tackle it. One special case of public-key crytography is identity based crypto. A rigorous comparison among the pros and cons of the different techniques show that identity based crypto is a potential solution for securing the identity privacy of a user in the 5G network.

1 Introduction

NGMN Alliance has pointed out that privacy of a user as a requirement of the 5G network under the requirement category of enhanced services [1]. In 3GPP TR 33.899 [2], subscribers' privacy is captured as one of the high level security requirements of the 5G network. However, in the context of diversified devices and complex business and service model of 5G, it is important to define who is a subscriber and what subscriber privacy means. According to 3GPP TR 21.905 [**?**] a subscriber is an entity (associated with one or more users) that is engaged in a Subscription with a service provider. A Subscription describes the commercial relationship between the subscriber and the service provider, cf. 3GPP TR 21.905 [1]. A subscription identifier is the identifier that uniquely identifies a subscription in the 3GPP system. The identifier is used to access networks based on 3GPP specifications. Subscription Privacy refers to the right to the protection to any information that (a) can be used to identify a subscription to whom such information relates, or (b) is or might be directly or indirectly linked to a subscription. This definition of privacy suggests to protect any personally identifiable information (PII) from an active or passive attacker. In this report we will keep our discussion limited only for the case of long-term identifier of a subscriber. In the case of 2G, 3G and 4G networks, this long-term identifier is known as IMSI.

One approach of protecting IMSI privacy is to use temporary IMSI instead of the original IMSI and keep changing the temporary IMSI at a feasible frequency. Note that the temporary IMSI has to be assigned over a confidentiality protected channel. Note that different entity of the network may assign different temporary IMSIs to the UE. In LTE network, the temporary IMSI assigned by serving core network is called GUTI and the home network does not assign any temporary IMSI to the UE. However, during the initial attachment of a user equipment (UE) to the network, the UE has neither a temporary IMSI nor a security context with the network that can assign it with a temporary IMSI. This forces the device to reveal the relevant IMSI to the network to keep itself from permanently locked out of the network. Provisioning the UE with an initial temporary IMSI assigned by the home network doesn't solve the problem because such temporary IMSI can be lost or be unsynchronised. In this report we try to show how a security context can be set up in between the network and the UE even before the identification of the UE so that the UE can use the security context to send its identity with confidentiality protection. Such a security context will mitigate the passive IMSI catchers (PICa). Nevertheless, we show that the active IMSI cathers (AICa) would not be able to agree on a legitimate security context with the UE.

In order to present a formal discussion we need to know what are the entities involved in this identification process, what are the communication interfaces among those entities and how much the entities can be trusted with the IMSI. As the architecture of 5G security is yet to be finalized, we present an abstraction of the involved entities and assume that what ever the security architecture of 5G eventually be, it will contain these entities and interfaces. This abstraction is directly extracted from LTE security architecture and we use some LTE acronyms to present the entities for better understanding. Figure ?? shows the entities. It involves the user equipment (UE), serving radio network (eNB), serving core network (MME), home network (HSS), PICa, and AICa. The interface UE-NB in between UE and eNB is initially unprotected. Nevertheless, eNB-MME and MME-HSS are always protected and the security of these interfaces is out of the scope of this report. The PICas eavesdrop on the UE-eNB interface when it is unprotected to extract and IMSI. The AICas impersonate a legitimate network and run a legitimate protocol with UE in order to reveal the IMSI.

Both PICa and AICa are untrusted. It is technically possible to not trust eNB and MME. However, by some other specification in 3GPP TS xx.xxx it is required to reveal IMSI to the MME to enable lawful interception (LI) without involving HSS. HSS and UE both owns the IMSI and they are trusted with it.

We propose solutions that makes the UE-eNB interface protected even during the initial attachment to fight against the PICa. Our solutions also stop the active IMSI catchers from running a legitimate protocol successfully that reveals an IMSI. However, different solutions assumes different level of trust in eNB and MME. In the evaluation section we present elaborate discussion on that.

However, as reduced signalling overhead is another important requirement of 5G, signalling overhead is also considered in our evaluation. We will see that to achieve reduced signalling overhead and improved control plane latency, our solutions would work best when it is used with temporary IMSI called pseudonyms assigned by the HSS.

2 Public key cryptography against IMSI catchers

Here we use public key cryptography which may or may not be based on identity based crypto to secure the privacy of the long term identity of a mobile phone user called IMSI (International mobile subscriber identity). We discuss different techniques of using the public key cryptography:

1. Identity based crypto based on the identity of SN where the HN is the key generator
2. HN assigned public private key pair for each SN
3. HN owned public private key pair

In the consequent sections we describe the aforementioned techniques in further detail.

3 Based on Identity of Serving Network

In this technique the HN has a public and private key pair. Every phone knows the public key of the HN. Whenever a SN asks the phone to provide its IMSI, the phone computes the public key of the SN using the public key of the HN. Then the phone encrypts the IMSI with the computed public key of the SN and sends it to the SN along with the HN identity. The SN obtains (possibly already have obtained) its private key from the mentioned HN. Using this private key, the SN can decrypt IMSI. Figure **??** represents the high level protocol.

3.1 Concerns and Solutions

1. How to provision, revoke and re-provision the public key of HN in the phone?
2. How to black list a SN?

3.2 Based on HN generated public private key pair for every SN

4 Conclusion

5 Acknowledgement

References

[1] NGMN 5G White Paper V1.0 [cited Jan, 2017]. Available at: https://www.ngmn.org/uploads/media/NGMN_5G_White_Paper_V1_0.pdf

[2] 3GPP TR 33.899 V0.6.0 [cited Jan, 2017]. Available at: https://portal.3gpp.org/desktopmodules/Specifications/SpecificationDetails.aspx?specificationId=3045