Protection Against the IMSI Catchers Using Identity Based Crypto in 5G

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 improving security and privacy over the existing LTE network. Identity privacy of a user has been a historical concern with all the previous generation mobile networks, namely GSM, UMTS, and LTE. While little improvements have been achieved in securing the privacy of long term identity of a user, the so called IMSI catchers are still in existence even in the LTE and advanced LTE networks. This report looks into this privacy problem 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 these 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 identity privacy of a user as a requirement of the 5G network under the requirement category of enhanced services [**?**]. In 3GPP TR 33.899 [**?**], 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]. Subscription Identifier: The identifier that uniquely identifies a subscription in the 3GPP system. The identifier is used to access networks based on 3GPP specifications. 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. Privacy requirements: Set of requirements to take into account when a 3GPP node is processing personally identifiable information (PII).

What are the privacy requirements in the context of subscription privacy?

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