A Security Enhanced 5G Authentication Scheme for Insecure Channel

Xinxin HU†, Caixia LIU†, Shuxin LIU†, Nonmembers, and Xiaotao CHENG†, Member

SUMMARY More and more attacks are found due to the insecure channel between different network domains in legacy mobile network. In this letter, we discover an attack exploiting SUCI to track a subscriber in 5G network, which is directly caused by the insecure air channel. To cover this issue, a secure authentication scheme is proposed utilizing the existing PKI mechanism. Not only does our protocol ensure the authentication signalling security in the channel between UE and SN, but also SN and HN. Further, formal methods are adopted to prove the security of the proposed protocol.

key words: 5G network, network security, authentication protocol, strand spaces model

1. Introduction

The Fifth Generation Mobile Communication System (5G) is expected to serve more people around the world compared to LTE. 5G security is critical because it is related to subscriber privacy, industrial safety and even national security. However, there are some studies shown that the current 5G authentication protocol is not as safe as 3GPP claimed in [1]. Basin et al. [2] give a comprehensive analysis of 5G AKA and found some critical security goals are not met because of implicit authentication. Based on the same method, Borgaonkar et al. [3] discovered a logical vulnerability of XOR in 5G AKA and proposed 3 fix schemes. However, those schemes are still based on a strong assumption that the communication channel between serving network (SN) and home network (HN) is secure when subscribers are roaming. In fact, this assumption is too strong to be met in operators’ commercial networks. Because it’s impossible for all operators to deploy SEPP at the edge of 5G network. Once there was one exception, the global 5G network would be placed in unsafe situation. Moreover, the 5G authentication protocol proposed by 3GPP is considered to be safe enough even in the air channel. But the air interface attack methods are always diverse. Besides, with the advancement of technology, the attacker’s capabilities are also improving, and previous security assumptions in the air interface may be difficult to meet. And new technologies introduced by 5G new radio will bring more uncertainty to 5G networks. Therefore, it is necessary to carefully study the protocols in the insecure channel.

By carefully studying the 5G authentication protocol and the SUPI encryption mechanism, we find a potential attack in 5G that could be exploited by attacker to track subscriber’s location. Then, we analyze the root reason of the attack and find that the insecure channel is the root cause. Next, we design a security enhanced protocol to remove the security threat and other potential threats exploiting insecure channels. Finally, we use strand spaces model to prove the security of the proposed protocol.

An overview of our contributions is presented as follows:

We discovered a vulnerability in air channel that could be exploited by attackers to track a subscriber.

For the insecure channel between UE, SN and HN, we propose a security enhanced 5G authentication protocol.

The proposed protocol is proved secure through formal methods.

2. Background

Similar to legacy cellular network, 5G mainly consists of three parts, user equipment, service network, and home network. User equipment may include mobile phone, wearable devices, etc. Serving network mainly composes of some mobile management functions such as AMD, SEAF, SMF, etc. And home network is mainly responsible for subscriber authentication and identity information management. The simplified 5G network is shown in Fig. 1.

A major security feature of 5G network is the use of asymmetric encryption to encrypt SUPI to prevent user identity information from leaking in the air interface. As shown in Fig. 2, the public key of home network (PK_HN) and the temporary private key generated by UE are combined into a temporary shared key, which is used to encrypt the MSIN in the SUPI. The home network generates the same temporary shared key to decrypt SUCI with the temporary public key generated by UE and the home private key.
3. An Attack Exploiting the Insecure Channel

Due to the insecure channel in the air interface, attacker is very likely to initiate an active attack. In this section, we present a potential attack exploiting SUCI of a target subscriber. The attack steps are shown in Fig. 3. Firstly, the attacker can capture and save the freshly generated SUCI of a victim UE. Secondly, the attacker sends the fabricated registration request with the captured SUCI. The legitimate network will send an authentication request to the victim UE. The attacker can distinguish the victim by synchronization failure message. This attack can be used to track a 5G subscriber’s location.

4. The Proposed Scheme

In fact, in addition to exploiting the insecure channel between UE and SN, the attacker can also utilize the insecure channel between HN and SN. In order to solve the found attack and prevent other attacks that may occur, we propose a secure authentication scheme that guarantees protocol security in the case where the aforementioned channels are not secure.

In order to ensure the communication security between SN and HN, SN is designed to generate a public/private key pair (PKSN, SKSN) in our scheme. According to 3GPP specification [1], there is already a pair of public/private key pair (PKHN, SKHN) for HN which is used to conceal SUPI. SN and HN know each other’s public key. Besides, our scheme utilizes Eph.private key and Eph.public key generated by UE to ensure the security of the channel between UE and SN. As shown in Fig. 4, the proposed protocol runs as follows:

1. UE sends a registration request to SN, which includes SUCI and Eph.public key, where SUCI = \{MMC, MNC, \{SUPI, Eph.private key\}\}PKHN.

2. After receiving the registration request, SN saves Eph.public key and encrypts the SNname (SNN) with PKHN, namely CSNN = \{SNN, Rs\}PKHN, and sends \{SUCI, CSNN, \{SNN, Rs\}PKHN\} to HN.

3. After receiving the message of SN, HN decrypts the SUCI in SIDF to obtain the corresponding SUPI using SKHN, and calculates the authentication vector 5G AV (RAND, AUTN, HXRES*, KSEAF) using the root key K. Next, HN encrypts the 5G AV into \{5G AV\}PKSN using SN’s public key and send it to SN.

4. After receiving the \{5G AV\}PKSN, the SN decrypts the 5G AV with PKSN and saves KSEAF, HXRES* locally. Then, SN encrypts \{RAND, AUTN, ABBA, ngKSI\} with Eph.public key and sends it to UE.

5. After receiving the authentication request message, UE decrypt the message with Eph.private key. If UE can’t decrypt the \{RAND, AUTN\}Eph.public key, then abort. If this step succeeds, then execute MAC and SQN check. If both verifications are successful, the calculated RES* is returned to the SN.

6. SN compares SHA256(R, RES*) with HXRES*. If they are equal, SN return RES* to HN.

7. HN determines whether the authentication is successful according to RES* verification result. If it’s successful, HN returns SN authentication result and the encrypted SUPI, namely \{SUPI\}KSEAF.

8. SN sends authentication success message to inform the UE of authentication result.

5. Formal Analysis of the Proposed Scheme

Strand spaces model is a powerful formal analysis tool for cryptographic protocols [4]. We now prove with strand spaces model that our proposed authentication protocol is secure. The proposed protocol can be expressed as below.

\[ \text{UE} \rightarrow \text{SN} : \text{M1} = \{\text{SUCI, Eph.public key}\} \]
SN → HN: M2 = {SUCI, [SNN, Rs]PKHN}
HN → SN: M3 = {[RAND, AUTN, HXRES*, KSEAF]PKSN}
SN → UE: M4 = {[RAND, AUTN, ABBA, ngKSI][Eph.public key]}
UE → SN: M5 = {RES*}
SN → HN: M6 = {RES*}
HN → SN: M7 = {Result, [SUPI]KSEAF}
SN → UE: {“Authentication success”}

The UE strands are [SUCI, Eph.public.key, RAND, AUTN, ABBA, ngKSI, RES*] with tranches: <+1, −M4, +M5>. The SN strands are [SUCI, Eph.public.key, SNN, Rs, RAND, AUTN, HXRES*, KSEAF, ABBA, ngKSI, RES*, SUPI] with tranches: <+−M1, +M2, −M3, +M4, −M5, +M6, −M7>. The HN strands are [SUCI, Eph.public.key, SNN, Rs, RAND, AUTN, HXRES*, KSEAF, RES*, SUPI] with tranches: <+−M2, +M3, −M6, +M7>. In the above definition, SUCI, SNN, Rs, RAND, AUTN, HXRES*, KSEAF, ABBA, ngKSI, RES*, SUPI ∈ T, PKHN, PKHN ∈ K.

Proposition 1: Authentication of SN to UE. Suppose C is a bundle of the protocol’s strand space Σ. RAND is uniquely originating from HN. Kp is the cipher key set controlled by attacker and SKHN, SKSN /∈ Kp. If s ∈ SN [SUCI, SNN, Rs, RAND, AUTN, HXRES*, KSEAF, ABBA, ngKSI, RES*, SUPI] and c-height(s) = 7, then there are regular strands in C, SUE ∈ UE[SUCI, RAND, AUTN, ABBA, ngKSI, RES*], and C-height(SUE) = 3.

Proof: 1. Construct test component. From strand space model, RAND only comes from <s, 4>, and <s, 4> =⇒ +<s, 5> is transformed edge. So, edge <s, 4> =⇒ +<s, 5> is a test for RAND. Suppose t0 = HXRES*, we can conclude t0 is test component of <s, 4> about RAND. Base on the authentication test rules, <s, 4> =⇒ +<s, 5> is an incoming test for RAND in HXRES*.

2. Apply authentication test rule. According to incoming authentication test rule, transforming edge of RAND, m =⇒ +m’ exists in bundle C.

3. Define node m’. From the analysis in step 2, m’ should be a node in one initiator. Suppose initiator strand is SUE’, SUE’ = UE[SUCI’, RAND’, AUTN’, ABBA’, ngKSI’, RES’*], and m’ = <SUE’, 3>, t0 ∈ term(<SUE’, 3>).

4. Compare content of strand. Compare term(<SUE’, 3>) with content in initiator strand, we can conclude SUE = SUE’, m =⇒ +m’ is <SUE’, 3> =⇒ +<SUE’, 3>.

Therefore, normal strand SUE ∈ UE[SUCI, RAND, AUTN, ABBA, ngKSI, RES*] in bundle C, and C-height(SUE) = 3. It can be seen that SN can authenticate the identity of UE through the similar method.

Proposition 2: Authentication of SN to HN. Suppose that s is SN’s strand, SKHN, SKSN /∈ Kp, then SNN is originated uniquely by s.

Proof: 1. Construct test component. SN strand s = SN[SUCI, Eph.public.key, SNN, Rs, RAND, AUTN, HXRES*, KSEAF, ABBA, ngKSI, RES*, SUPI]. As SNN ∈ {SNN, Rs}PKHN is originated uniquely in <s, 2>, {SNN, Rs}PKHN is the test component in <s, 2> about SNN. It can be seen that: <s, 2> =⇒ +<s, 3> is the outgoing test for SNN.

2. Apply the authentication test rule. It has the existence of normal node m, m’ ∈ C, term(m) = {SNN, Rs}PKHN, and m =⇒ +m’ is the transforming edge of SNN.

3. Define the node m. According to the result of step 2, the node m is a negative node. Therefore, m is the node of certain HN strand. Suppose that the initiator strand is s’ and s’ = HN[SUCI’, Eph.public.key’, SNN’, Rs’, RAND’, AUTN’, HXRES*’, KSEAF’, RES*’, SUPI’], m = <s’, 2>, and term(s’, 2) = SUCI’ = {MMC’, MNC’, [SUPI’, Ru’]PKHN}.

4. Compare the contents of strands. By comparing the contents of term <s’, 2> with the related content in HN strand, SUPI = SUPI’, HN = HN’, SNN = SNN’ can be derived. So, it can be seen that SN can authenticate the identity of HN. Through the same method, the authentication of HN to SN can also be validated.

6. Conclusion

The authentication protocols are supposed to ensure the communication security in insecure channels. In this letter, we found an attack in 5G authentication protocol, which is caused by the insecure channel. Then, we propose a security enhanced authentication protocol for 5G network to defend the found attack and other potential attacks. With formal methods, we successfully prove that the proposed scheme can guarantee the communication security in two insecure channels, namely the channel between UE and SN as well as the one between SN and HN.

Acknowledgments

This work was supported by the National Natural Science Fund for Innovative Research Groups (61521003) and the National Natural Science Foundation of China (61801515).

References

[1] 3GPP TS33.501, “Security architecture and procedures for 5G system,” 2019.

[2] D. Basin, J. Dreier, L. Hirschi, S. Radomirovic, R. Sasse, and V. Stettler, “A formal analysis of 5G authentication,” Proc. 2018 ACM SIGSAC Conference on Computer and Communications Security, pp.1383–1396, 2018. doi: 10.1145/3243734.3243846.

[3] R. Borgaonkar, L. Hirschi, S. Park, and A. Shaik, “New privacy threat on 3G, 4G, and upcoming 5G AKA protocols,” Proc. Privacy Enhancing Technologies, vol.2019, no.3, pp.108–127, Stockholm, Sweden, 2019. doi: 10.2478/popets-2019-0039.

[4] T. Fábrega, F. Javier, J.C. Herzog, and J.D. Gutman, “Strand spaces: Proving security protocols correct,” Journal of Computer Security, vol.7, no.2-3, pp.191–230, 1999. doi: 10.3233/JCS-1999-72-304.