A Vulnerability in 5G Authentication Protocols and Its Countermeasure

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

SUMMARY 5G network will serve billions of people worldwide in the near future and protecting human privacy from being violated is one of its most important goals. In this paper, we carefully studied the 5G authentication protocols (namely 5G AKA and EAP-AKA’) and a location sniffing attack exploiting 5G authentication protocols vulnerability is found. The attack can be implemented by an attacker through inexpensive devices. To cover this vulnerability, a fix scheme based on the existing PKI mechanism of 5G is proposed to enhance the authentication protocols. The proposed scheme is successfully verified with formal methods and automatic verification tool TAMARIN. Finally, the communication overhead, computational cost and storage overhead of the scheme are analyzed. The results show that the security of the fixed authentication protocol is greatly improved by just adding a little calculation and communication overhead.

key words: 5G network, authentication protocols, security, formal methods

1. Introduction

5G networks have begun commercial deployment around the world. Whether it is human life (such as smart home, smart city) or manufacturing industry (such as smart factory), it will be deeply connected with 5G network. Hence, 5G will contain a variety of information whether it’s personal or industrial, and 5G security has never been more important than it is now.

As the first line of defense for mobile communication network, authentication protocol is one of the most important fields in mobile network security research. Myrto et al. [1] found a linkability attack in 3G authentication protocol, which can be used by attacker to determine whether a target subscriber is in a specific cell. They also proposed a scheme to cover this problem, which utilizes the PKI mechanism to encrypt subscriber identity information, authentication result, random number and the synchronization sequence number with public key of network. This scheme enhances the security of 3G authentication protocol and the linkability attack is fixed. However, the communication overhead, calculation overhead and storage overhead required by the scheme are large. Ravishankar et al. [2] found a logic vulnerability for the AKA protocols, which exploits XOR operation in AUTS calculation to crack the subscribers’ synchronization sequence number value. The attacker can calculate the SQN value bit by bit through a set of AUTSs caused by the same authentication vector sent to the target subscriber. The attack may be used to track user location and analyze user communication behavior. To fix the attack, they proposed three potential solutions. Changhee et al. [3] discovered a linkability attack in LTE network and proposed an effective solution for it. The communication, computational and storage overhead of the scheme are small. However, the scheme only solves the linkability attack and additional signalling is required to realize synchronization failure recovery in LTE system. Hu et al. [4] disclosed an attack that exploits the target user registration request message to identify target subscriber’s presence. They proposed a systemic solution, but the solution required a major change to the 5G key hierarchy. B. David et al. [5] presented a comprehensive formal analysis of 5G authentication protocol with TAMARIN prover and found some design flaws in terms of Lowe authentication security. However, they didn’t give detailed fix scheme and correspondingly it’s impossible to provide security and efficiency analysis of the security recommendations.

Inspired by previous research, we have discovered a linkability attack in the newest 5G system that can be used to determine the location of a legitimate subscriber. In order to fix the discovered vulnerabilities, we took advantage of the security architecture of the 5G system and proposed a possible solution without adding additional keys. Our contributions are listed as follows:

A novel linkability attack of 5G authentication protocols is found.

A countermeasure is proposed to solve the discovered attack.

The security of the proposed solution is formally verified, and the communication overhead, computational cost and storage overhead of the proposed scheme are analyzed as well.

2. Background

In this section, the background of the problem is introduced. First, we give a general introduction of 5G network. Then two authentication protocols of 5G, namely 5G AKA and EAP-AKA’, are introduced.

2.1 5G Network

Similar to the 4G LTE network, 5G is mainly composed of user equipment (including ME, USIM card), access network, and core network (including serving network and
home network). The 5G network is said to have enhanced large bandwidth, Massive Machine Type of Communication, Ultra-reliable and Low Latency Communication according to ITU. In order to achieve this, a service-based architecture as well as network function virtualization technology are adopted within the 5G core network, which provide support for flexible scheduling and network slice for different vertical industries. Correspondingly, the air interface also adopts many new technologies, such as massive MIMO, Polar and LDPC codes. At the security level, 3GPP has put forward higher requirements for 5G than LTE. 5G has stronger security architecture, more network security layers, more stringent network border control, and user identity information is also asymmetrically encrypted in the air interface.

2.2 Authentication Protocols

When a UE tries to accesses the mobile network, mutual authentication with the network is required. Thus, UE and network have to run an authentication protocol which generally works in a challenge/response manner. At first, the network needs to calculate an authentication vector that only the corresponding UE can decrypt it with the shared key between network. After receiving the challenge, the UE decrypts the challenge with its own key and performs verification of the message authenticity and freshness. If the check passes, the UE responds to the challenge with a success message. Then the network will respond to the UE with authentication result. Authentication protocols exist in all generations of mobile communication networks. With the evolution of mobile communication networks, the authentication protocols are also evolving and their security and efficiency are increasing. In 5G network, 3GPP specifies two authentication protocols, namely 5G AKA and EAP AKA', that the network must support [6], [7]. As shown in Fig. 1, 5G AKA protocol runs as follows:

1. HN → SN: AV (RAND, AUTN, HXRES*, K_AUSF)
2. SN → UE: RAND, AUTN, ngKSI, ABBA
3. UE → SN: If SQN_SN and MAC are both verified successfully, return RES*.
   If the SQN_SN check fails, UE returns Syn_failure. If the MAC check fails, it returns Mac_failure.
4. SN → HN: RES*, Syn_failure or Mac_failure.

5. HN → SN: Authentication_result, SUPI.

The EAP-AKA' protocol is similar to 5G AKA. It also relies on the challenge/response mechanism based on a shared root key to authenticate each other as well as synchronization sequence number to prevent replay attacks. The SQN, MAC check mechanism and synchronization failure recovery procedure are identical. The main difference between them is that some signalling messages and key derivation functions are different. The problems discussed in this paper are located in SQN, MAC verification mechanism, and synchronization failure recovery procedure. Therefore, the attack discovered and countermeasure proposed in 5G AKA suit EAP AKA' as well.

3. Location Sniffing Attack

In this section, we detail the discovered vulnerability and the attack implementation steps. In short, the vulnerability is that the authentication responses of the AKA protocols in 5G network are transmitted in plaintext in the air interface. The attacker can easily determine whether the authentication is successful or failed and even the fail reason through passive eavesdropping. This vulnerability can be exploited by an attacker to determine a target subscriber’s presence in a cell.

The assumption of implementing the attack is that the attacker has to build up a cellular network signal transmitting and receiving device (denoted by malicious gNodeB), such as USRP with gNodeB protocol stack, which could be used to collect the authentication request message of the target user as well as eavesdrop the authentication response on the air interface. As shown in Fig. 2, the entire attack steps are as follows:

1. Firstly, the attacker places the sniffing tool near the target UE and eavesdrops on the plaintext authentication request message of the target UE from the air interface. This message contains RAND and AUTN, and the attacker saves the message locally.
2. Next, the attacker builds an authentication request message using the RAND and AUTN captured in step 1. Then, he broadcasts the fabricated authentication request message anywhere the target subscriber may appear. All
UEs in vicinity of the malicious gNodeB will receive the authentication request message.

3. After receiving the message, the UEs will make message authentication code check and sequence number check. After the verification is completed, the UE returns the authentication response in clear text as the key agreement procedure has not been completed. The MAC check can be successful only when the xMAC obtained from the AUTN and the MAC recalculated using SQNHN are equal. When performing the SQN check, the UE will determine whether the SQNHN is in the correct range. If SQNHN > SQNUE, the SQN check will succeed. When both of the above checks are successful, the UE will return RES∗ = Response (K, RAND, SNN), where Response() represents a complex key derivation function and SNN represents serving network name. If MAC and xMAC are not equal, the UE will respond to the network with MAC verification failure. If the MAC check succeeds and the SQNHN is not in the correct range, the UE will respond to the network with synchronization failure. Therefore, the replayed authentication request message received in step 2 will pass the MAC check of target UE. However, the SQN check will not pass as SQNHN < SQNUE. Finally, the authentication between UE and malicious gNodeB will fail and the target UE will respond to the attacker with Synchronization failure message. Other UEs will fail the authentication due to the MAC verification failure and respond to the attacker with MAC failure message. According to the received response messages, the attacker can make the following judgment. If there is a synchronization failure message, the target UE is nearby. If all the received messages are MAC failure, the target UE is not nearby. The attack above can be implemented in EAP-AKA’ as well.

Attackers may use this vulnerability to determine the presence of certain important target users (such as national leaders, ambassadors etc.). For example, if the attack is implemented in the vicinity of the office area, home, or large-scale event site that the target user may appear, the current user’s specific location can be judged without being perceived by him or her.

4. Countermeasure and Analysis

In this section, we discuss the countermeasure for the above attack. Since the attack found in the previous section apply to both 5G AKA and EAP AKA’, our improvements are also designed for both of them. At last, the safety and efficiency of the fix scheme are analyzed.

4.1 Proposed Scheme

To fix the vulnerability disclosed in Sect. 3, the two kinds of authentication failure messages must be indistinguishable from the attacker’s perspective. So, we redesign the authentication response message and encrypt it utilizing the existing PKI scheme in 5G network. The proposed countermeasure is shown in Fig. 3.

1. After receiving the authentication request message (RAND, AUTN), the UE verifies the MAC and SQN. If both pass, then UE shall compute RES → f2(K, R) and compute RES’ from RES according to A.4 in 33.501. Otherwise the UE generates a new random number rand and goes to step 2.

2. If the MAC check succeeds but the SQN check fails, let fail_reason = Syn_failure, MACS = f1K(SQNUE∥rand), then

\[
RES’ = [\text{fail_reason}, \text{SQNUE}, \text{rand}]_{\text{PbN}} || \text{MAC-S} = ["\text{Syn_failure"}, \text{SQNUE}, \text{rand}]_{\text{PbN}} || f1K(\text{SQNUE || rand})
\]

where “||” represents the concatenation of two operands.

3. If the MAC check fails, let fail_reason = Mac_failure, MACS = f1K(SQNUE || rand), then

\[
RES’ = [\text{fail_reason}, \text{rand}]_{\text{PbN}} || \text{MAC-S} = ["\text{Mac_failure"}, \text{rand}]_{\text{PbN}} || f1K(\text{SQNUE || rand})
\]

4. Send RES’ to the SN/HN.

In the above solution, the MACS is included in the authentication failure message to prove that the message originates from the real UE. The new rand rand is used in the MACS computation to prevent a possible link attack: If the RAND in the AV is used, the attacker replays the same authentication request twice in a short time (the SQNUE has not changed). Then, the same MACS is captured twice and the target subscriber is captured according to this. Besides, random number rand is used to encrypt SQNUE with public key to prevent rainbow table attack.

4.2 Security and Efficiency Analysis

To prove that our scheme will not leak subscriber’s location information, we use TAMARIN prover [8] for formal verification. Observational Equivalence properties in TAMARIN reason about two systems by showing that an intruder cannot distinguish these two systems. If observational equivalence of authentication response message is satisfied, it is not possible for an attacker to determine a subscriber’s location information.

Table 1 shows the formal description of our proposed
scheme, where the rule describes the encryption of authentication failure message with network public key pk_HN. To prove the observational equivalence, we use the \texttt{diff} ( , ) operator in TAMARIN. Lemma demonstrates the property we want to prove. The result of the verification is shown in Fig. 4. It can be seen that an attacker cannot distinguish between two types of error messages, which proves the security of the proposed countermeasure.

In addition to the security property, we also analyze the efficiency of the proposed solution, including communication overhead, storage overhead, and computational overhead. The analysis results are shown in Table 2. We can see that the 3GPP solution and our scheme both have pluses and minuses. The communication overhead indicates the length of data that UE needs to transmit by radio. It can be seen that our solution requires slightly more overhead than the 3GPP’s. In terms of computational overhead, 5G AKA needs to run 6 times pseudo-random function, while our scheme needs 5 as well as 1 asymmetric encryption. In terms of storage overhead, our solution is smaller than 5G AKA.

5. Conclusion

In this paper, we found a security vulnerability in 5G network authentication protocols. With this vulnerability, an attacker can track a target subscriber’s location with cheap hardware.

To fix the vulnerability, we propose a countermeasure that leverages the existing PKI mechanism of 5G network without adding keys. The failure messages of authentication are redesigned. Next, the security, communication, computation and storage overhead of the scheme are analyzed. The analysis results show that our proposed scheme greatly increases the communication security and reduces the storage overhead while only adding little communication overhead and computation overhead.

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] M. Arapinis, L. Mancini, E. Ritter, M. Ryan, N. Golde, K. Redon, and R. Borgaonkar, “New privacy issues in mobile telephony: fix and verification,” Proc. 2012 ACM conference on computer and communications security, pp.205–216, North Carolina, USA, 2012. doi: 10.1145/2382196.2382221.

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

[3] C. Hahn, H. Kwon, D. Kim, K. Kang, and J. Hur, “A privacy threat in 4th generation mobile telephony and its countermeasure,” Proc. International Conference on Wireless Algorithms, Systems, and Applications, vol.8491, pp.624–635, Harbin, China, 2014. doi: 10.1007/978-3-319-07782-6_56.

[4] X. Hu, C. Liu, S. Liu, W. You, Y. Li, and Y. Zhao, “A Systematic Analysis Method for 5G Non-Access Stratum Signalling Security,” IEEE Access, vol.7, pp.125424–125441, 2019. doi: 10.1109/ACCESS.2019.2937997.

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

[6] 3GPP TS33.501, “Security architecture and procedures for 5G system,” 2019.

[7] 3GPP TS33.102, “5G Security; Security architecture,” 2018.

[8] M. Simon, S. Benedikt, C. Cas, and B. David, “The TAMARIN prover for the symbolic analysis of security protocols,” International Conference on Computer Aided Verification, vol.9044, pp.696–701, Saint Petersburg, Russia, 2013. doi: 10.1007/978-3-642-39799-8_48.