Recommendations for Improving 5G Authentication

Kelley Burgin (kburgin@mitre.org)
Paul Rowe (prowe@mitre.org)
Current contact:
Joshua Guttman (guttman@mitre.org)

The MITRE Corporation

Mutual authentication between a 5G subscriber and its home network is critical for 5G communications. The 3rd Generation Partnership Project (3GPP) has standardized numerous protocols to facilitate authentication. This brief document describes security weaknesses in the Authentication and Key Agreement (AKA) family of protocols designed to facilitate the connection of a subscriber device to a serving network in its vicinity which is not part of the device's home network. We focus on EAP-AKA', but the issues and proposed solution appear to apply to other variants in the AKA family as well.

Two Attacks on Privacy

Privacy for the subscriber user equipment (UE) is an important goal for 5G. The 5G architecture should not make it appreciably easier for a malicious actor to locate or track a target device. To this end, EAP-AKA' masks unique identifiers of the UE trying to connect to a serving network (SN) until the UE and its home network can mutually authenticate each other, and the HN can facilitate key agreement between the UE and the SN.

In order for a UE to connect to SN, the UE and its home network (HN) engage in a challenge response protocol with communication mediated by the SN since UE and HN cannot communicate directly. During this phase, the messages between the UE and the SN must be sent in the clear because they do not yet share any cryptographic key material. A malicious actor within range of the SN could therefore receive and record messages for replay later. In particular, a malicious actor can replay an old challenge message sent from the HN to the UE (as relayed by the SN) to break the UE's privacy.

Detecting presence of target device.[1] EAP-AKA' ensures that old messages cannot be replayed to undermine the mutual authentication between UE and HN. However, when an old challenge message targeting a specific UE is replayed, the targeted UE responds with a failure message that differs from the failure messages sent by other devices. The message authentication code (MAC) on the challenge message will properly validate the message only for the targeted UE. All other devices with reply with a MAC failure message, while the targeted UE will reply with a sync failure message. Since these error messages are sent in the clear, the adversary can detect the presence of the targeted UE

[1] Basin, David, et al. "A formal analysis of 5G authentication." Proceedings of the 2018 ACM SIGSAC conference on computer and communications security. 2018.

in the vicinity by determining if any device replied with a sync failure message. If the adversary controls a network of rogue or malicious base stations, they might be able to track the movements of the targeted UE as well.

Revealing usage information of target device.[2] Replaying an old challenge message also opens up the possibility for a malicous actor to learn information about how often the targeted UE has attempted to connect to the network in a given time period. The sync failure message sent by the UE contains the current sequence number used by the UE. This sequence number is masked by being xor'ed with secret information contained in the challenge message. By replaying the *same* challenge message at two points in time, an adversary can analyze the two resulting sync failure messages and begin to infer information about how far the sequence number has advanced between the two times.

Recommended Improvement

The attacks described above hinge on the fact that the UE has no way of tying the challenge message from HN to its original request to connect to the SN. It cannot distinguish replayed challenges from a situation in which the HN's sequence number has gotten out of sync. We therefore recommend that the UE include a unique identifier in its request to connect to SN, and that this identifier be threaded through the challeng-response protocol. This will allow the UE to detect the replayed message and avoid replying with a sync failure message. The unique identifier need not be random, but it must never be reused.

Such a change to the protocol addresses both types of privacy violation described above. Since the targeted UE will no longer send a sync failure in response to a replayed message, it will not inadvertently signal its presence in the vicinity of the adversary. Similarly, it prevents the UE from sending two different sequence numbers xor'ed with the same secret value. This prevents an adversary from learning anything about how often the UE tried to connect.

While different recommended improvements to EAP-AKA' could also address the issues identified above, we believe our proposal has the advantage that it places minimal requirements on the user equipment. Although the 5G architecture design is willing to make stronger assumptions about user equipment, such as its ability to perform some expensive cryptographic functions and to produce sufficiently random values, our proposal makes no new demands on the UE. The UE performs no encryptions and the unique identifier in its connection request need not be random. This makes our proposed improvement suitable for compatibility with 3G and 4G devices which are generally assumed to be less capable than 5G devices.

[2] Borgaonkar, Ravishankar, et al. "New privacy threat on 3G, 4G, and upcoming 5G AKA protocols." Proceedings on Privacy Enhancing Technologies 2019.3 (2019): 108-127.