Long-term Identity Privacy In Cellular Networks

October 13, 2017

1 Abstract

Long-term identity privacy is an old problem that has persisted in 2G, 3G, and even in 4G networks. The use of temporary identity called TMSI or GUTI has been effective only against the passive attackers who listens to the radio channel. However, the active attackers who impersonate a legitimate serving network can still trick a user equipment and obtain its long-term identity. Even though the weakness is known since the time of 2G networks, no solution has been adopted due to the additional complexity. Use of public key cryptography is one of the promising solutions. Another promising solution is to use a one time identity known as pseudonym that is recognized by the user's home network. The public key approach is simple but more expensive. It can only be implemented in the future networks like 5G and can not provide the privacy in the legacy networks. A pseudonym based solution appears to be more complex but less expensive. It can be implemented in the future networks and can provide the privacy even in the presence of a legacy network. However, vulnerabilities in the pseudonym based solutions have been published in the recent publications. Even though fixes of those vulnerabilities have been provided, confidence in pseudonym based solution is not yet enough. In 3GPP, a solution based on public key cryptography is being adopted for the first phase of 5G specification. However, there still may have opportunities of using a pseudonym based solution in the coming phases of 5G specification.