A Session Mix-up Attack on the UMTS/LTE Authentication and Key Agreement Protocols

Short talk at IEEE Computer Security Foundations Symposium
Cambridge MA, June 26, 2012

Stig F. Mjølsnes

Department of Telematics
Norwegian University of Science and Technology
sfm@item.ntnu.no

We have detected a protocol-level security vulnerability in the specifications of the Authentication and Key Agreement (AKA) protocols. These kind of cryptoprotocols are used globally now in the 3G Universal Mobile Telecommunications System (UMTS) mobile networks, and in the 4G Long-Term Evolution (LTE) mobile system currently being deployed worldwide. The attack, which will violate the entity authentication security, was found during our work on establishing a computational security analysis using the tool CryptoVerif. We distinguish two possible attack scenarios; an outsider attack and an insider attack. An insider (a subscriber) can impersonate another user by establishing a mixed up shared key with the serving network, which allows the attacker subsequent use of the wireless access charged to the victim's subscription. We propose simple, but important corrections to UMTS/LTE AKA. In the paper presented at FCC 2012 [1], we prove authenticity and secrecy properties for the session keys in *the corrected* UMTS and LTE AKA protocols.

References

[1] Tsay and Mjølsnes. *Computational Analysis of the UMTS and LTE Authentication and Key Agreement Protocols*. Eighth Workshop on Formal and Computational Cryptography (FCC), June 27-28, 2012.