Computational Analysis of the UMTS and LTE Authentication and Key Agreement Protocols

Joe-Kai Tsay and Stig F. Mjølsnes

Department of Telematics
Norwegian University of Sciences and Technology, NTNU
{joe.k.tsay | sfm}@item.ntnu.no

Abstract. One of the forerunners and main candidates for the fourth generation (4G) mobile communication systems is commonly known under the name Long-Term Evolution (LTE) and its standard is produced and maintained by the 3rd Generation Partnership Program (3GPP), an international consortium of telecommunications standards bodies. The LTE Authentication and Key Agreement (AKA) protocol design is based on the Universal Mobile Telecommunications System (UMTS) AKA protocol, which is widely used today for third generation (3G) wireless networks, and which itself is the successor of the Subscriber Identity Authentication (SIA) protocol of the Global System for Mobile Communication (GSM). With the persistent spread of these mobile network systems, their authentication protocols have become one of the the most widely used security protocols today. We present a computational security analysis of the Authentication and Key Agreement (AKA) protocols of the Universal Mobile Telecommunications System (UMTS) and the Long-Term Evolution (LTE) system. We mainly consider the technical specifications ts33.102, ts33.401, ts33.210, ts33.310, ts33.200, ts29.002, ts42.009 and ts43.020, which are produced by the 3GPP. This work constitutes the first analysis of LTE AKA to date and the first computationally sound analysis of UMTS AKA. We conduct our analysis of UMTS AKA and LTE AKA with the tool CryptoVerif that can prove the security of protocols and cryptographic primitives directly in the computational model.

Using CryptoVerif, we discover a previously undetected vulnerability in the specifications of both UMTS AKA and LTE AKA. The flaw itself is of symbolic nature but we found the attack by interpreting the last game in a sequence of game transformations performed by CryptoVerif. It is the same flaw that is present in the specifications of both UMTS AKA and LTE AKA. We note that, strictly speaking, the specifications of the GSM SIA protocol (ts43.020, ts42.009) also suffer from the same vulnerability. This vulnerability can be exploited by both outside and inside attackers in order to break authentication of a user to a serving network. Furthermore, inside attackers may impersonate an honest user and use wireless services on her/his behalf without the user being present on the network at that time. The attacks are possible because of a misbinding of the responses sent by the so-called home network, which acts as a trusted third party in the UMTS/LTE security architecture. If the intended receiver of those responses, the serving network is running concurrent sessions, then an adversary, who is in full control of the network, can force a session mixup attack by redirecting the responses to different sessions of the serving network. This attack is not prevented by the specifications, which (in some cases) protect the connection between the home and the serving network using IPsec or MAPsec. We reported the vulnerability to the 3GPP, where the issue is currently under investigation. We have not tested current implementations for susceptibility to these attacks.

We propose simple corrections to UMTS/LTE AKA (and GSM SIA) and use CryptoVerif to proof correspondence (i.e. authentication) and session key secrecy properties for the corrected UMTS and LTE AKA protocols. In our proofs, we model the cryptographic primitives following the 3GPP MILENAGE sample algorithms set (ts.35.206), where we use a pseudo-random permutation block cipher, an IND-CPA symmetric-key encryption scheme, a WUF-CMA secure message authentication code, and a pseudo-random function. All these cryptographic primitives are already modeled and ready-to-use in CryptoVerif. Our proofs were mostly not conducted fully automatically but concluded by inspection of the last games in the sequences of CryptoVerif transformations.