A Vulnerability in 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. We report on a deficiency in the specifications of the Authentication and Key Agreement (AKA) protocols of the Universal Mobile Telecommunications System (UMTS) and Long-Term Evolution (LTE) as well as the specification of the GSM Subscriber Identity Authentication protocol, which are all maintained by the 3rd Generation Partnership Program (3GPP), an international consortium of telecommunications standards bodies. The flaw, although found using the computational prover CryptoVerif, is of symbolic nature and could be exploited by both an outside and an inside attacker in order to violate entity authentication properties. An inside attacker may impersonate an honest user during a run of the protocol and apply the session key to use subsequent wireless services on behalf of the honest user.

Keywords: Applied Cryptography, Vulnerability Assessment, Security Protocols, Authentication, Mobile Network Security, LTE, UMTS.

1 Introduction

The Global System for Mobile communication (GSM) and UMTS mobile networks are a worldwide success with now about 6 billion supscriptions [17], and still growing. New mobile systems are rolled out, including the 3GPP recent developments named 'Long Term Evolution' (LTE) and 'System Architecture Evolution' (SAE), which have become a forerunner for the fourth generation (4G) generation mobile communication system. The new system is called 'Evolved Packet System (EPS), emphasizing the all-IP packet switching design throughout the system onto the user's mobile terminal. [1] As more and more people take advantage of the accelerated internet access through their mobile phones, the recent international concern about securing the cyberspace and critical infrastructures certainly must include mobile networks. There is a multitude of security issues in such large networked systems. Here we will focus on the mobile terminal access security by means of an authentication and key agreement protocol. Weaknesses in this protocol may not only lead to revenue loss to mobile operators but might also facilitate cyber crime.

[1] Although EPS is the proper technical term for this new 3GPP mobile system generation of SAE/LTE, we will use the most well-known name LTE.

I. Kotenko and V. Skormin (Eds.): MMM-ACNS 2012, LNCS 7531, pp. 65–76, 2012.

The LTE AKA protocol 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 GSM Subscriber Identity Authentication (SIA) protocol. With the persistent spread of these mobile network systems, these authentication protocols have become some of the most widely used security protocols today. While there exist formal analyses of UMTS AKA in the *Symbolic Model* of security (also called the *Dolev-Yao* model and inspired by [15]), this is in fact the first analysis of LTE AKA to date.

We report on an intermediate result of an ongoing analysis [19] of UMTS AKA and LTE AKA with the tool CryptoVerif [14] that can prove the security of protocols directly in the computational model. We discover a previously undetected flaw in the specifications of both UMTS AKA and LTE AKA. We note that the specifications of the GSM SIA protocol [9,8] suffer, strictly speaking, from the same vulnerability (cf. Section 3.3). The 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 his behalf without the user being present on the network at that time. 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 (cf. Section 3.1). We propose a simple correction to UMTS/LTE AKA and are working on CryptoVerif proofs of correspondence (*i.e.* authentication) and secrecy properties for the session key.

Related Work. Annex B of the 3GPP technical report in [1] documents a formal analysis of the UMTS AKA protocol using a BAN logic variant. The analysis verifies authentication and secrecy properties. The flaw that we present here is not detected in [1] because strong assumptions (the *prerequisites on SN's side*) are used which already eliminate the weakness in the protocol. The GSM SIA protocol does not provide authentication of the access network to the user and the interoperability of the GSM and UMTS systems perpetuates this attack possibility, reported in [18]. Our analysis is not directed to the problems of interoperability between LTE/UMTS/GSM. A redirection attack on the UMTS AKA is reported in [20], which exploits the observation that the user is not able to authenticate the identity of the *serving* network because this is not included in the authentication vector provided by the home network. The new LTE AKA specification is designed to fix this weakness. A recent paper focuses on the privacy properties of the UMTS AKA protocol [10]. They use the tool ProVerif [12] for a formal analysis, and the paper describes an attack that enables the adversary to track a user. This is done by exploiting different error messages that are returned by UMTS AKA. The analysis models the UMTS AKA as a simplified two-party protocol between a user and the core network. However, by reducing UMTS AKA to a two-party protocol, the weakness uncovered in the present work is concealed.