A new tunnelled EAP based authentication method for WiMAX networks

ABSTRACT

Despite well-defined and commercially viable security standards for WiMAX networks, vulnerability in current system design and other inherent characteristics expose the network to various types of security attacks. These attacks are commonly related to network access security, authentication of users, validation of data transmission, and confidentiality issues. In order to provide better protection to WiMAX users, several improvements in the security mechanism have been provided. One notable solution is by using a more secure protocol, namely the Privacy Key Management (PKM), which later being revised into PKMv2 (PKM version 2). In this protocol, authentication (as well as mutual authentication) plays an important role since it must be completed in order to establish a secure connection between the network entities. PKMv2 uses either RSA-based or EAP-based authentication modes. While there are variations of authentication modes exist in the literature, some of them prone to man-in-the-middle (MITM) attack and significant overheads. This paper proposes a new method called EAP-TTLS-ISRP which embeds the transmission of security messages in a secure tunnel. This authentication method is proposed for a single EAP based authentication to achieve both user and device authentications between Mobile Station (MS) and Authentication Server (AS) by using strong and fast authentication methods. The proposed method outperforms other methods in the number of messages exchanged and thus it has less overhead cost, it also satisfies the EAP requirement for secure and efficient data exchange, as well as robust to MITM attacks. Automated Validation of Internet Security Protocols and Applications (AVISPA) verification tools are used to verify the security performance of the proposed EAP-TTLS-ISRP method.

Keyword: WiMAX; PKMv2; Authentication; TTLS; SRP