A Cross Layer Spoofing Detection Mechanism for Multimedia Communication Services

Nikos Vrakas, University of Piraeus, Greece

Costas Lambrinoudakis, University of Piraeus, Greece

ABSTRACT

The convergence of different network types under the same architecture offers the opportunity for low cost multimedia services. The main objective has been the high quality of the provided services. However, considering that older equipment with limited processing capabilities may be present in such environments, a tradeoff between security and service quality is inevitable. Specifically, low resource enabled devices cannot utilize state of the art security mechanisms, such as IPSec tunnels, integrity mechanisms, etc., and they simply employ HTTP Digest authentication. The lack of integrity mechanisms in particular raises many security concerns for the IMS infrastructures. Attacks such as Man in the Middle (MitM), spoofing, masquerading, and replay that can be launched in IMS environments, have been pinpointed in bibliography by various researchers. Moreover, an internal attacker may utilize his legitimate security tunnels in order to launch spoofing and identity theft attacks. This paper presents a cross-layer spoofing detection mechanism that protects SIP-based infrastructures from the majority of the aforementioned attacks without requiring an additional cryptographic scheme which would inevitably introduce considerable overheads.

Keywords: *Cross Layer, IMS, IP Multimedia Subsystem, Security Mechanism, SIP, Spoofing, VoIP*

1. INTRODUCTION

The provision of multimedia services over cellular and mobile devices is nowadays a necessity and not a special service. The need for better and contemporary services at low cost have forced the providers to widely deploy the IP Multimedia Subsystem (IMS) (3rd Generation Partnership Project, 2008) in order to introduce high quality services to the users of different network architectures. On the other hand, this universal infrastructure has to be flexible enough to cover the participating entities that either come from technologically older network generations or low resource enabled devices. This fact comprises a special feature for the universality of the architecture and at the same time a major drawback for the security. More specifically,

DOI: 10.4018/jitsa.2011070103

in order for all these obsolete devices to be satisfied, the security schemes have to include less resource demanding and eventually weaker encryption and authentication algorithms. Furthermore, the Session Initiation Protocol (SIP) (Rosenberg et al., 2002) is utilized in IMS as the main signaling protocol providing flexibility but also introduces threats as stated in many scientific works (Geneiatakis et al., 2006; Sher, Wu, & Magedanz, 2006; Walsh & Kuhn, 2005).

According to IMS specifications (3rd Generation Partnership Project, 2010) for all User Equipment (UE) that do not utilize a Universal Subscriber Identity Module/IP Multimedia Services Identity Module (USIM/ISIM), the authentication method has to be the SIP Digest (Franks et al., 1999). That implies that there is no integrity protection for the signaling messages or a tunneling between the UE and the Proxy-Call Session Control Function (P-CSCF). This raises many security and privacy concerns and introduces vulnerabilities and entry points to the IMS architecture (Abdelnur, Avanesov, & Rusinowitch, 2009; Hunter, Clark, & Park, 2007; Sher et al., 2006; Sher & Magedanz, 2007; Vrakas, Geneiatakis, & Lambrinoudakis, 2010).

Another important threat in such architectures comes from attacks that can be launched by internal users who have a legitimate subscription to the service. In these cases the attacker may bypass the security mechanism because he is able to authenticate the forged messages. Moreover, such an attacker may utilize his legitimate security tunnel when the AKA with IPSec (Kent & Atkinson, 1998) or TLS (Dierks & Allen, 1999) is employed as authentication method in order to launch identity theft and SIP signaling attacks (3rd Generation Partnership Project, 2010; Sisalem, Kuthan, Abend, Floroiu, & Schulzrinne, 2009).

The heavyweight employed security protocols between IMS core entities does not give the opportunity for another potential additional overhead. Thus, even though the employment of integrity mechanism such as S/MIME (Ramsdell, 1999) cannot deter the internal attacker (IA) from launching attacks, the utilization of public key encryption is rather heavy and resource draining for such devices.

Taking into account the restrictions imposed by the power and bandwidth limitations of UEs; we propose a cross-layer spoofing detection mechanism for VoIP/IMS infrastructures, without the use of any cryptographic protocols that would introduce an additional overhead to the network. The proposed detection method covers the majority of spoofing attacks against VoIP/IMS environments that utilize SIP as their signaling protocol, including MitM, masquerading and SIP signaling attacks from different network layers. It is worth noting that an accurate detection and prevention of spoofing attacks can reduce the need of an integrity mechanism and especially when SIP Digest is employed to reduce the number of required authentications.

The remaining of the paper is structured as follows: Section 2 presents the alternative threats faced by an IMS environment due to spoofing attacks. Section 3, provides a review of the detection mechanism presented by other researchers as well as a comparison, in respect to their efficiency in detecting attacks, with the proposed mechanism, while section 4 provides an extensive description of the proposed detection mechanism. Finally we conclude the paper with case study scenarios and some useful proposals for future work.

2. SPOOFING ATTACKS IN SIP/IMS ENVIRONMENTS

A malicious user can utilize many different techniques in order to hide his real identity. With the term *identity* we refer to either some hardware or to the person/subscriber. As far as the hardware, namely the UE, is concerned the identity can be the IP address in correlation with its unique MAC address. On the other hand, the identity of a user comprises the unique IMS Private Identity (IMPI) and IMS Public Identity (IMPU).