A Call Conference Room Interception Attack and its Detection

Nikos Vrakas[1], Dimitris Geneiatakis[2] and Costas Lambrinoudakis[1]

[1]Department of Digital Systems, University of Piraeus
150 Androutsou St., Piraeus 18532 Greece
Email: {nvra,clam}@unipi.gr

[2]Dept. of Telecommunications Science and Technology, University of Peloponnese
End of Karaiskaki St., GR-22100, Tripolis, Greece
Email: dgen@uop.gr

Abstract. The IP Multimedia Subsystem (IMS) infrastructure is currently considered to be the main core of Next Generation Networks (NGNs), integrating IP and other network types under one common infrastructure. Consequently, IMS inherits security flaws and vulnerabilities residing in all those technologies. Besides, the protection against unauthorized access in NGN services is of great importance. In this paper we present a call conference room interception attack and we propose a new cross layer architecture to shield IMS against it.

Keywords: SIP, IMS, Interception, Spoofing Detection, VoIP.

1 Introduction

The Session Initiation Protocol (SIP) [1] is an application layer protocol responsible for handling multimedia sessions and conferences in Next Generation Networks (NGNs). Although various protocols have been proposed for the administration of call sessions like H323 [2], SIP is considered the predominant one since 3GPP proposes its utilization in IP Multimedia Subsystem (IMS) [3].

Various researchers [4, 5] have focused their research on the identification of security vulnerabilities of SIP-based voice services offered over the Internet (VoIP). Similar security flaws are exhibited by any infrastructure that deploys the SIP protocol. Consequently, IMS services are subjected to attacks like SIP flooding, SIP malformed messages and SIP signaling attacks. In the latter case, a malicious user exploits the lack of the appropriate authentication and integrity protection mechanisms in SIP [4] and IMS correspondingly, in order to (illegally) "modify" a session in progress. Under this context, in this paper we demonstrate a call conference interception attack that could be launched against IMS services. Specifically, an internal user may act maliciously (Internal Attack – IA), as a man in the middle during a multimedia conference, in order to join the conference by exploiting the SIP REFER method. At this point one might argue that such security flaws could be prevented through the deployment of the appropriate integrity mechanisms [6, 7],

however, such mechanisms require the modification of the IMS client side. Furthermore, those solutions have not taken into consideration IMS client side's limited resource capabilities. Besides, it should be noted that in IMS deployments where User's Equipment (UE) lacks IP Multimedia Service Identity Module / Universal Subscriber Identity Module (ISIM/USIM), the IP Security (IPSec) Authentication and Key Agreement (AKA) [8] cannot be utilized. Consequently, the UE should use alternative solutions proposed in IMS specifications [9] like SIP Digest [8], NIBA [10] or GIBA [11]. Note that such mechanisms do not provide integrity protection to signaling messages, allowing a malicious user to participate in an unauthorized way in a multimedia conference. To this end, we propose a transparent server side cross-layer mechanism towards the detection of spoofing and man in the middle attacks in order to deter such behaviors.

The rest of this paper is structured as follows. In section 2 an interception attack, utilizing the SIP REFER method, which can be implemented in an IMS infrastructure is described. Section 3 presents a cross-layer framework capable to detect such behaviors and other more general spoofing attacks, like ARP poisoning, which could compromise a VoIP channel. Finally we conclude the paper with some pointers for future work.

2 Call Interception Attack Utilizing REFER Requests

The SIP REFER method is a non default request described in RFC 3515 [12]. Particularly, SIP REFER is used by an authorized entity (referrer) in order to request some other entity to access a resource on behalf of the "referrer". Fig. 1 depicts a multimedia conference invitation in an IMS architecture. Note that the resource, to be accessed, is identified by the corresponding Uniform Resource Indicator (URI) included in the SIP Refer-To header and can be any type of existing URIs such as SIP and HTTP [13]. This method extends existing multimedia service capabilities providing extra functionality like call transfer, conference rooms etc. However, a malicious user can avail of this request by inviting itself or another UE of his choice in order to participate (illegally) in the session. In this case the attacker spoofs a legitimate REFER request of a valid user by adding his UE URI/public ID in the "Refer-To" or "To" header depending the type of conference invitation.

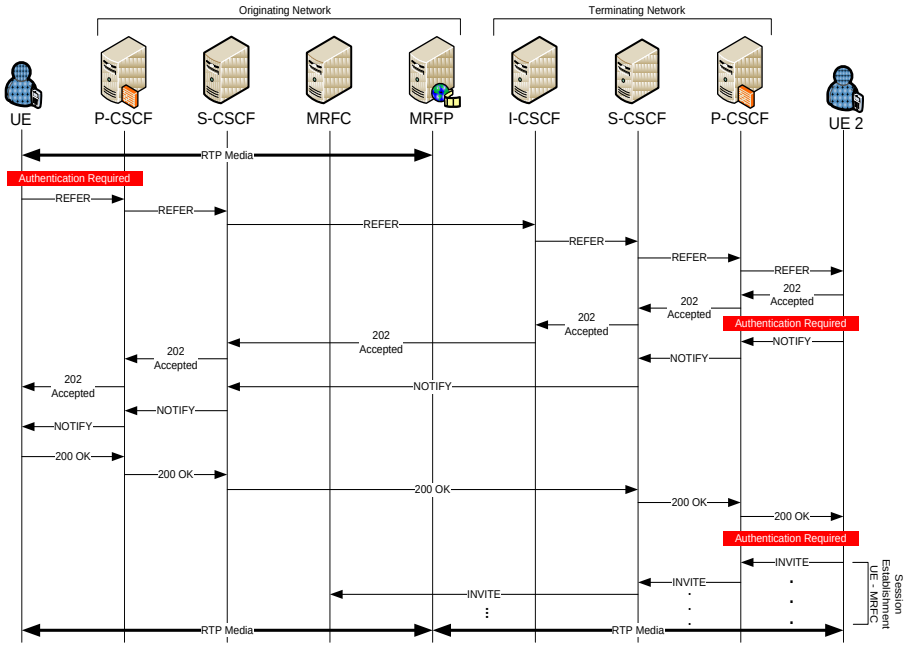

Fig. 1: Successful Invitation to a Call Conference

2.1 Attack Description

In this attack scenario a malicious user acts as an intermediate (Man in the Middle - MitM) between the Proxy Call Session Control Function (P-CSCF) and the UE, utilizing well-known attack techniques such as Domain Name System (DNS) [14, 15] and Address Resolution Protocol (ARP) poisoning [16]. We assume that a legitimate UE has already established a multimedia conference room and would like to invite one more user (UE3) to join. At the very first stages, a malicious user changes DNS binding in order to force the traffic passing through his domain. Consequently, whenever a legitimate UE sends a SIP REFER message, the DNS resolution procedure will force the CSCF components to forward traffic towards the attacker's domain. Afterwards the malicious user poisons the ARP correlating legitimate user's IP with his own MAC address in order to receive the responses directed to a legitimate UE.

As soon as the malicious user catches a SIP REFER, spoofs the "To" header value with his URI/public ID, while the remaining message is retained as is, and forwards it to P-CSCF. Afterwards, the SIP REFER request is processed by the Server-CSCF (S-CSCF), which by its turn sends it to the destination that the "To header" points to, namely the IA. The IA responds with a "202 Accepted" to the S-CSCF as well as the former sends a spoofed "202 Accepted" towards the UE. Subsequently, the IA sends a "legitimate" SIP NOTIFY message to the P-CSCF, while the IA is the "legitimate"

referee. The IA is able to authenticate successfully the NOTIFY request as he holds a valid subscription (considering that the IA is an internal user).

After the successful authentication, the P-CSCF sends a NOTIFY to UE through the IA who acts as MiTM, while the IA spoofs the included headers that points him ("From" and "Contact") with the corresponding of UE3. The UE accepts it by sending a 200 OK response message. In the same way the IA spoofs and forwards it to the P-CSCF. Finally, the IA executes an invitation handshake in order to establish a media session with the MRFP that will enable him to participate as a legitimate user in the conference room. For further information for the rest of the handshake refer to [17]. The whole attack procedure is depicted in Fig. 2. The green color denotes that the IA is able to fulfill the specific request or generally to bypass a security mechanism. Note that an external attacker will not be able to launch such an attack because of lack of valid credentials to authenticate SIP NOTIFY message.

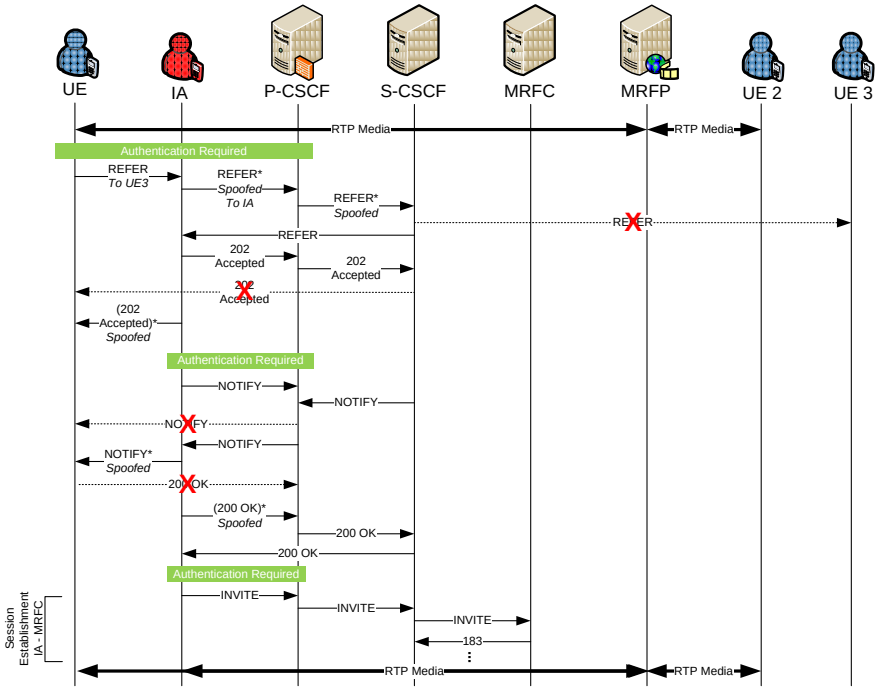

Fig. 2: REFER – Interception Attack

3 Proposed Mechanism

The proposed mechanism relies on the information gathered from messages of different network layers, in order to correlate a specific UE with its MAC, IP, SIP addresses and private/public ID. This mechanism is able to detect IMS spoofed message attacks not only in cases where signaling messages lack authentication or

integrity protection, but also in cases where the user establishes a security tunnel using IPSec [18] or Transport Layer Security (TLS) [19] with the corresponding server. For example an internal malicious user utilizes his legitimate tunnel in order to forward spoofed messages with stolen public IDs to Core Network (CN) [8].

3.1 Mechanism Description

The proposed mechanism monitors the incoming traffic and gathers information related to a specific UE. Particularly, it collects information from all Internet layers (SIP messages), Network (IP packets) and the frames of Data Link layer (MAC Address) relevant to the current UE request. Actually, this information is stored in a *cross layer correlating* table where a tuple denotes UE's specific connection characteristics which are the MAC address, IP addresses retrieved from IP and SIP protocol layers correspondingly, as well as the UE's identities and finally the method of the SIP request.

A stack of collected information is denoted by E_i, where i = {0,…,n} and n is the number of the incoming messages as illustrated in Table 1. For instance, MAC_0 denotes the MAC address of the UE that a user utilized in order to be initially registered to the service while the IP_0 denotes the IP address that the specific UE has been allocated during the same procedure. The SIP_0 and ID_0 come from the application layer denoting the IP address and the ID that have been included in the SIP header fields of the same message (E_0). All the subsequent messages come with a subscript increased by 1.

Table 1: Proposed Mechanism's Cross-Layer Correlation

	UE	IP Address		IMPI/IMPU	Method
E_0	MAC_0	IP_0	SIP_0	ID_0	Register
E_1	MAC_1	IP_1	SIP_1	ID_1	Refer
	Layer 2	**Layer 3**	**Layer 5**		

Every new collected message (E_i) for a specific UE is compared with the existing tuples in order to identify a spoof case. This is also true if the attacker is internal (and thus able to establish a security tunnel through IPSec) and tries to launch an identity theft attack as already described in section 2. For instance, for an incoming SIP message received by an IMS service we extract the following:

$$E_1=\{MAC_1, IP_1, SIP\text{-}IP_1, ID, Method_1\}$$

Furthermore, we define $K = MAC \cup IP \cup SIP\text{-}IP$ denoting a unique correlation with a specific UE. Consequently, for E_1 we compute the corresponding K_1 value. If K_1 matches some K_i (for every tuple in the table the corresponding K value is calculated) the incoming message E_1 has been generated by a legitimate user. Otherwise, the proposed mechanism compares the IP_1 and SIP-IP_1 field values in E_1. If these are different it is deducted that a malicious user has created a spoofed SIP message. Alternatively, it could be that IP_1 and SIP-IP_1 of message E_1 do have the same value,

but there is no match with a record in the cross layer table. In such a case if the collected info (IP_1, SIP-IP_1 and MAC_1) has been extracted from an authenticated SIP REGISTER message, E_0 must be updated (as the legitimate user has been registered through a different UE), otherwise, a malicious user tries to impersonate a legitimate one.

3.2 Protecting Against the Call Interception Attack

Considering the REFER interception attack that has been presented, we are able to detect it, through the conditional tests that detects IP spoofing and ARP poisoning. Specifically, when the IPs of both network (IP) and application layer (SIP) of an incoming message matched with a tuple in the cross layer table, while the corresponding MACs differ, we can deduce that: (a) IPs (network and application layer) or (b) MAC addresses has been spoofed.

Taking as an example the attack illustrated in Fig. 2, we assume that UE has the MAC AAA, UE2 the BBB and the attacker CCC (or a MAC of his choice but note that in order to achieve an ARP poison he must broadcast his real MAC). UE1 and UE2 have been registered and the corresponding E_i tuples have been generated in the cross layer table (E_0 and E_1). Afterwards, the IA gathers the UE's REFER and forwards it to the server (E_2). As depicted in Table 2, the E_2 K value does not match with any E_i K_i value in the table. Although, IP addresses (network and application level) have the same values, the E_2 record has been generated from a non-authenticated SIP REGISTER, consequently the incoming message is a spoofed one.

Table 2: An Instance During the Detection of Refer Attack

	UE	IP Address		IMPI/IMPU	Method
E_0	AAA	111	111	User1	Register
E_1	BBB	333	333	User3	Register
E_2	CCC	111	111	User1	Refer
	Layer 2	**Layer 3**	**Layer 5**		

4 Conclusions

NGNs infrastructures merge different network technologies under the umbrella of Internet architecture, constituting them vulnerable to similar threats and attacks residing in it. As IMS is the core of NGN it will attract the attention of malicious users who will try to identify new vulnerabilities or exploit existing ones. Under this context, in this paper we present a case of a signaling attack in IMS namely "A Call Conference Interception Attack", exploiting the lack of appropriate integrity protection mechanisms in SIP.

Furthermore, we propose a cross layer server based mechanism to detect illegal modifications in IMS signaling messages and consequently in established sessions.

Such a method does not require any modification in client side as would be the case for an Integrity mechanism.

Currently, we focus on the evaluation of the proposed mechanism and we also investigate the case of broaden it in order to shield IMS infrastructure not only against signaling but also resource consumption attacks using a centralizing architecture.

References

1. J. Rosenberg, H. Schulzrinne, G. Camarillo *et al.*, *RFC 3261: SIP: Session Initiation Protocol*, 2002.
2. I. T. Union, "H323 Packet Based Multimedia Communications Systems," Telecommunication Standardization Sector of ITU, 1998.
3. 3GPP, "TS 23.228: IP Multimedia Subsystems (IMS)," Third Generation Partnership Project, Technical Specification Group Services and System Aspects, 2008.
4. D. Geneiatakis, A. Dagiouklas, G. Kambourakis *et al.*, "Survey of security vulnerabilities in Session Initiation Protocol," *IEEE Communications Surveys and Tutorials*, vol. 8, pp. 68-81, 2006.
5. D. Sisalem, J. Kuthan, S. Ehlert *et al.*, "Denial of Service Attacks Targeting a SIP VoIP Infrastructure: Attack Scenarios and Prevention Mechanisms," *IEEE NETWORK*, vol. 20, no. 5, pp. 26, 2006.
6. D. Geneiatakis, and C. Lambrinoudakis, "A lightweight protection mechanism against signaling attacks in a SIP-based VoIP environment," *Telecommunication Systems*, vol. 36, no. 4, pp. 153-159, 2007.
7. B. Ramsdell, "RFC 2633: S/MIME version 3 message specification," 1999.
8. 3GPP, "TS 33.203: 3G security; Access security for IP-based services (Release 9)," Third Generation Partnership Project, Technical Specification Group Services and System Aspects, 2009.
9. 3GPP, "TS 24.229: IP Multimedia Call Control Based on SIP and SDP," Techincal Specification Group Core Network and Terminals, 2009.
10. 3GPP, "TR 33.978 Security aspects of early IP Multimedia Subsystem (IMS)," Third Generation Partnership Project, Technical Specification Group Services and System Aspects, 2008.
11. ETSI, "TS 187 003: Telecommunications and Internet converged Services and Protocols for Advanced Networking (TISPAN): Security Architecture," 2008.
12. R. Sparks, *RFC 3515: The Session Initiation Protocol (SIP) Refer Method*, 2003.
13. A. B. Johnston, *SIP: Understanding the Session Initiation Protocol*: Artech House, 2004.
14. A. Klein. "BIND 9 DNS cache poisoning," http://www.trusteer.com/docs/bind9dns.html.
15. R. Zhang, X. Wang, R. Farley *et al.*, "On the feasibility of launching the man-in-the-middle attacks on VoIP from remote attackers." pp. 61-69.
16. R. Wagner, "Address resolution protocol spoofing and man-in-the-middle attacks," *The SANS Institute*, 2001.
17. 3GPP, "TS 24.147: Conferencing using the IP Multimedia (IM) Core Network (CN) subsystem," Technical Specification Group Core Network and Terminals, 2009.
18. S. Kent, and R. Atkinson, "RFC 2401: Security Architecture for the Internet Protocol," *Network Working Group*, 1998.
19. T. Dierks, and C. Allen, *RFC 2246: The TLS Protocol Version 1.0*, RFC Editor, 1999.