Computer Communications 31 (2008) 4259–4268

Contents lists available at ScienceDirect

Computer Communications

journal homepage: www.elsevier.com/locate/comcom

An efficient end-to-end security mechanism for IP multimedia subsystem

Chi-Yuan Chen [a], Tin-Yu Wu [b], Yueh-Min Huang [c], Han-Chieh Chao [a,d,*]

[a] Department of Electrical Engineering, National Dong Hwa University, Hualien, Taiwan, ROC
[b] Department of Electrical Engineering, Tamkang University, Taipei, Taiwan, ROC
[c] Department of Engineering Science, National Cheng Kung University, Tainan, Taiwan, ROC
[d] Department of Electronic Engineering and Institute of Computer Science & Information Engineering, National Ilan University, I-Lan, Taiwan, ROC

ARTICLE INFO

Article history:
Available online 6 June 2008

Keywords:
IP multimedia subsystem (IMS)
Key exchange
End-to-end security

ABSTRACT

With the rapid growth of the Internet and wireless communications, people make extensive use of portable wireless devices to access information such as voice, data and multimedia, any time from any place, enjoying ubiquitous services. IP multimedia subsystem (IMS) are regarded as the total solution for packet-switched networks, combining wired and wireless infrastructures, providing a standardized interface for information services. We propose the IMSKAAP key exchange protocol and fit it into the IMS session initiation procedure to achieve media plane end-to-end security. This mechanism also mitigates the impact of spam over IP telephony (SPIT) using mutual authentication, fulfilling the lawful interception requirement. The simulation result shows that the proposed mechanism provides a more secure session key exchange and does not need the additional message exchange cost. The voice call end-to-end delay is also lower than the hop-by-hop security associations defined by 3GPP.

1. Introduction

In next generation communication network technical development most researches focused on the WCDMA/HSDPA, cdma2000 1xEV-DO/DV [1] and other competitive access network technologies like WiMax or WiBro. The bandwidth demands for voice and streaming are growing for future communication networks. It can be expected that the next generation communication network will be an integrated All-IP network. Many research institutes are devoted to finding how to deploy IP protocols in mobile communication core network and services. The IP multimedia subsystem (IMS) is a network subsystem proposed by 3GPP [2]. The IMS concept is to combine telecommunication technology, wireless and wired networks under the All-IP environment to provide a more extensible, real-time, interactive multi-media service in 3G and future 4G networks. IMS can be regarded as the trend for future wireless communication networks.

The IMS offers three main functions [3] in the core network: (1) providing quality of service (QoS) for services; (2) offering the extensible charging mechanisms to services; (3) offering user integrated services, and the standard architecture make the third parties could provide different rich services.

3GPP defined IMS the architecture (such as Fig. 1). The IMS application server can offer the traditional telecommunication services and novel services such as push-to-talk, video streaming, multimedia messaging. This architecture includes numerous logical functions that could roughly be divided into three layers: (1) application server layer; (2) session control layer; (3) transport and endpoint layer.

IMS uses the modified IETF session initiation protocol (SIP) to establish the service session. The main function is to combine circuit-switched and packet-switched domains. The contents are not limited by the access medium but become more extensible to offer more optional services to users. There are several SIP servers in the IMS domain and they are generally called CSCF (call session control function). After integrating the HSS (home subscriber system), CSCF has the ability to transfer any kind of SIP service to another different network.

In the 3GPP IMS architecture, CSCF is the main component responsible to the SIP-based voice and multimedia session control, including the application layer registration and location information exchange with HSS. CSCFs are divided into three kinds: proxy CSCF (P-CSCF), serving CSCF (S-CSCF) and interrogating CSCF (I-CSCF). P-CSCF is the first contact point for user equipment (UE). The UE can obtain the P-CSCF address after registering with the access network. S-CSCF is mainly responsible for call service and session control. I-CSCF is the first connecting point. When requests

[*] Corresponding author. Address: Department of Electronic Engineering & CSIE, National Ilan University, I-Lan, Taiwan, ROC. Tel.: +886 3 9357400; fax: +886 3 9354238.

E-mail addresses: d96921015@ntu.edu.tw (C.-Y. Chen), tyw429@hotmail.com (T.-Y. Wu), huang@mail.ncku.edu.tw (Y.-M. Huang), hcc@niu.edu.tw (H.-C. Chao).

0140-3664/$ - see front matter © 2008 Elsevier B.V. All rights reserved.
doi:10.1016/j.comcom.2008.05.025

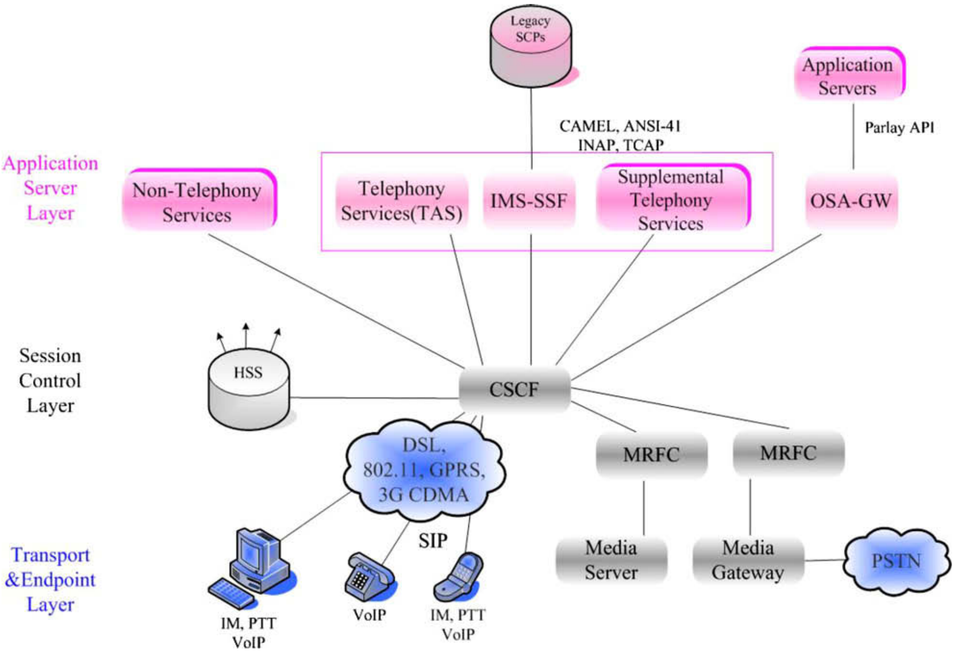

Fig. 1. IMS logical architecture.

enter the serving network I-CSCF is responsible for inquiring with HSS about the user's information and relevant location. I-CSCF has implemented the hiding inter-work gateway (THIG) function to improve security and privacy.

Numerous well-known attacks have been perpetrated on IP networks. Security is the first challenge for communication systems migrating into the All-IP network. Besides various network attacks, the forthcoming problems [4] that IMS would meet:

Fixed-mobile convergence (FMC) Security risks – Both wired networks and wireless networks can be integrated using the IMS architecture. IMS has become the architectural solution for FMC, adopted in many different standardization solutions such as PacketCable and ETSI TISPAN. Because the environmental requirements and hardware for wireless and wired networks are different, the IMS security features may not be directly adopted by the wired networks. It is expected that the IMS core network would be accessed from both wireless and wired networks, making the related security mechanisms are very important.

Media plane security – Currently, the IMS security architecture provides security protection only for SIP signaling messages. The media plane may be protected by the hop-by-hop security associations inside the core network, however, these security mechanisms may be disabled by the provider for performance reasons. Therefore, under the above-mentioned FMC architecture, the media plane security will not be guaranteed.

Spam over IP telephony – Like the Internet spam problems, the spam over Internet telephony (SPIT) is an urgent problem for VoIP and IMS. A malicious person could send numerous unsolicited voice calls or prerecorded messages to the IMS user. Unlike the spam email problem, the SPIT exists in the real-time services. But the SPIT can be prevented from policy control, completed user authentication and a tight trust model for IMS.

This paper proposes an efficient end-to-end security mechanism that addresses these potential IMS problems. This paper is organized as follows. In Section 2 we review the related technological background and possible mechanisms. In Section 3, we propose the end-to-end security mechanism for IMS. Section 4 discusses the IMSKAAP security analysis. Section 5 presents the simulation result showing the proposed mechanism is efficient and suitable for the IMS architecture. The final section presents our conclusions and future work.

2. Related works

The IMS security mechanism is divided into two parts: access security and network domain security. Access security, specified in 3GPP TS 33.203 [5], includes authentication related mechanisms and traffic protection between the UE and core network. Network domain security, specified in 3GPP TS 33.210 [6], includes traffic protection between network elements and takes into account roaming and non-roaming scenarios.

The IMS security architecture is shown in Fig. 2. The required security associations between the user equipment (UE) and IMS core network are specified. On the UE side, the IMS authentication key and functions are stored on a universal integrated circuit card (UICC) and the IMS subscriber identity module (ISIM) indicates a collection of IMS related security information and UICC functions.

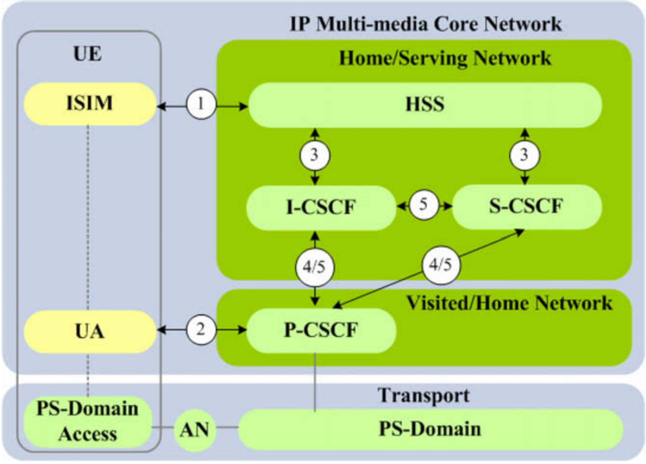

Fig. 2. IMS security architecture [5].

The five security associations for the IMS security architecture numbered in Fig. 2 as:

1. Provides mutual authentication between UE and HSS. The UE must have one user private identity (IMPI) and one or more user public identity (IMPU). The pre-shared long-term key in the ISIM and the authentication center (AuC) of HSS is associated with the IMPI.
2. The Gm reference point provides a security link and corresponding security associations between the UE and the P-CSCF after registered.
3. The Cx-interface provides security association for HSS database.
4. Provides link security for network elements between different network domains. It is specified by TS 33.210, as the Za interface in the Fig. 3. The Za Interface applies the encapsulating security payload (ESP) tunnel mode.
5. Provides link security for network elements within the same network domain. It is specified by TS 33.210, as the Zb interface in the Fig. 3.

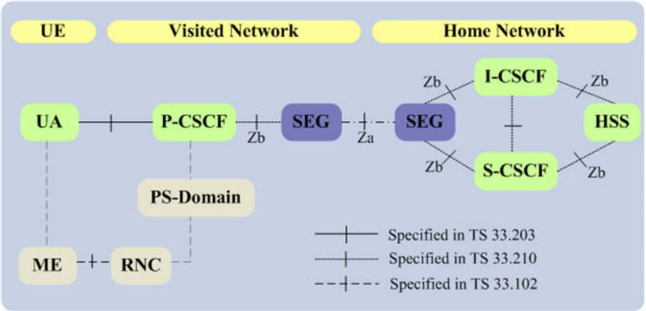

Fig. 3. IMS network domain security [5].

Under the IMS domain, a UE must register before being authorized to access the IMS services. Fig. 4 shows the IMS authentication procedure during registration.

First, UE sends the REGISTER the IMPU and IMPI requests to P-CSCF. In order to achieve the security mechanism agreement, the request also includes a security-client header field which contains a list of supported integrity and encryption algorithms, the security parameter index (SPI) values and selected port numbers. Upon receiving the request, P-CSCFS removes the security-client header field before forwarding the request to S-CSCF. S-CSCF then fetches authentication vectors (AVs) from the HSS via Cx interface (modified diameter protocol). The AVs are used in Universal mobile telecommunications system (UMTS) authentication and key agreement (AKA). S-CSCF then sends authentication token (AUTN), random number (RAND), confidentiality key (CK) and integrity key (IK) in the 401 unauthorized response message. After receiving the 401 message, P-CSCF removes the CK and IK, and adds a security–server header field. The security–server header field contains P-CSCF supported integrity and encryption algorithms, SPI values and selected port numbers.

After the UE receives the 401 message, UE uses ISIM to verify the AUTN challenge. If the verification procedure succeeds, the IMS core network is authenticated to the UE. The ISIM also produces the Response (RES) for UE. UE then selects integrity and encryption algorithms from the security–server header field to complete the security mechanism agreement procedure. After this procedure, UE establishes security associations (SAs) with P-CSCF. The UE sends an authentication response in the second REGISTER request via the SAs. Upon receiving the request, S-CSCF compares the RES with expected response (XRES). If the verification procedure succeeds, the UE is authenticated to S-CSCF. S-CSCF then sends a 200 OK message to indicate that the UE identity is registered in the IMS domain.

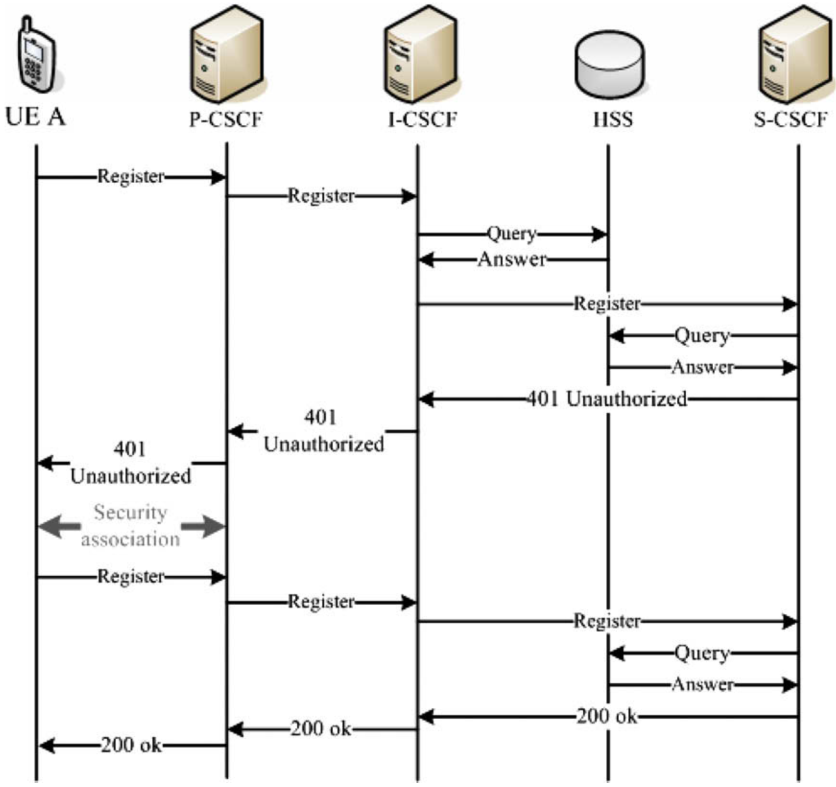

Fig. 4. IMS authentication procedure.