doi: 10.7690/bgzdh.2013.01.006

基于 S/MIME 的 IMS 文件安全传输方案

冯剑川[1,2]，严承华[1]，杜轶焜[1]，廖巍[1]
（1. 海军工程大学信息安全系，武汉 430033；2. 海军蚌埠士官学校信息技术系，安徽 蚌埠 233012）

摘要：针对现有 IMS 网络中文件传输时仅能保护 SIP 信令层，缺乏面向媒体层的有效安全机制的问题，提出一种基于 S/MIME 的文件安全传输方案。通过分析 IPsec、TLS 等安全机制的适用范围和在文件传输时的安全缺陷，依托 MSRP 协议实现 IMS 中文件传输，基于 S/MIME 实现端到端传输安全。仿真测试结果表明：该方案能有效保护传输过程中的文件实体，避免了通过 IMS 中各呼叫会话控制实体带来的延时，实现了 IMS 网络中的文件安全传输。

关键词：IP 多媒体子系统；消息会话中继协议；安全邮件协议；安全传输；媒体层安全
中图分类号：TP393.08　　**文献标志码**：A

IMS File Security Transmission Scheme Based on S/MIME

Feng Jianchuan[1,2], Yan Chenghua[1], Du Yikun[1], Liao Wei[1]
(1. *Department of Information Security, Naval University of Engineering, Wuhan* 430033, *China*;
2. *Department of Information Technology, Petty Officer Academy of PLA Navy, Bengbu* 233012, *China*)

Abstract: The existing IP multimedia subsystem (IMS) network security mechanism mainly focus on the SIP signaling plane protection and lack effective security mechanism for media plane. According to the characteristics of file transferring in IMS and potential security threats, this paper proposes a file safety transmission method based on secure/multipurpose Internet mail extensions (S/MIME). The scheme uses message session relay protocol (MSRP) to realize the IMS file transfer and achieves end-to-end security by S/MIME. It can effectively protect the transmission file entity and decrease the delay by avoiding traverse each call session control function in the IMS. Simulation results prove that the scheme can realize file safety transmission in the IMS network.

Key words: IMS; MSRP; S/MIME; security transmission; media layer security

0　引言

作为分组交换网络、有线和无线基础设施相结合的整体解决方案，IP 多媒体子系统（IP multimedia subsystem，IMS）提供了标准化的信息服务接口。IMS 概念在 3GPP R5 中提出并逐步完善，且得到 3GPP2、ETSI、ITU 等标准化组织和制造商的广泛支持，被视为下一代网络全 IP 环境下融合电信技术、无线和有线网络，提供扩展性更好、实时性更高、交互性更强的多媒体服务的最佳选择[1]。

现有的 IP 网络中存在大量攻击行为，IMS 作为全 IP 网络自然不可避免地面临各种安全威胁。目前最主要的有固网——移动融合（fixed-mobile convergence，FMC）安全、媒体层安全和 IP 电话垃圾信息 3 种[2]。文件传输是现有网络中用户经常使用的功能，由于 IMS 是控制层和承载层分离的网络，3GPP 在定义时仅对信令层的安全做了相应的规定，而对媒体层的安全主要依托承载层实现；因此，笔者分析、研究了 IMS 中文件安全传输的功能和特点，结合文献[3]对 MSRP 安全机制的建议，提出基于 S/MIME[4]实现 IMS 中文件的安全传输方案。

1　基本原理

文献[5]指出，IMS 中的文件传输属于即时消息（instant message，IM）的范畴，依托消息会话中继协议（message session relay protocol，MSRP）[3]与会话初始化协议（session initiation protocol，SIP）协同实现。IMS 网络采用基于 SIP/IP 核心网络的分层式网络架构，即时消息可分为 2 种通信模式：

1) 页面模式（pager mode）。

页面模式下的即时消息通过 SIP MESSAGE 方法完成消息的递送过程。此模式下的即时消息要求不超过最大传输单元（maximum transmission unit，MTU）减 200 字节，若未限定 MTU，一般不超过 1 300 字节。此模式仅适合于少量文本消息的传递，不适合大型文件传输。

2) 会话模式（session mode）。

会话模式下的即时消息通过 SIP/MSRP 结合的方式完成消息的交互过程，即通过 SIP INVITE 方法

收稿日期：2012-07-02；**修回日期**：2012-07-23
基金项目：全军军事学研究生课题（2010JY0698-403）；中国博士后基金特别项目（201003757）；大学自然科学基金项目（HGDYDJJ11008）
作者简介：冯剑川（1982—），男，四川人，硕士，讲师，从事网络安全研究。

建立 MSRP 会话，协商 MSRP 底层参数，调用 MSRP SEND 方法传输消息内容，通过 SIP BYE 方法释放会话。与页面模式相比，会话模式下通过 MSRP 协议进行多次即时消息交互过程，直到通信方决定结束即时消息通信，再完成会话的释放过程。会话模式适用于聊天室、会议等持续一段时间的即时消息交互方式，亦可用于包含多媒体内容的大消息传输、延迟消息的传输和文件传输等多种功能的实现[6]。

MSRP 是一个基于文本、面向连接的协议，可承载基于 MIME 编码的媒体信息。与处于信令层的 SIP 不同，MSRP 处于媒体层，即 MSRP 消息不需像 SIP MESSAGE 消息那样通过 SIP 代理服务器。传统的安全机制主要是针对 IMS 中 SIP 消息进行保护，并不能对 MSRP 提供可靠的保护，MSRP 的安全主要依托下层网络实现。根据注册过程中所选安全机制的不同有 3 种解决方案：基于 IPsec、基于 TLS 和基于 S/MIME。

如图 1 所示，在基于 IPsec 的方案中，客户端(user equipment，UE)注册 IMS 核心网后，信令层和媒体层均受到 IPsec 安全关联的保护，文献[7]指出，此时媒体流将通过 IMS 中各呼叫会话控制实体 P-CSCF、S-CSCF 等节点逐跳加密。基于页面模式的小文件传输若采用 IPsec 实现安全性保障，从理论上是可行的，但 SIP MESSAGE 不超过 1 300 字节的限制使其仅限于传递少量文本信息。尤其是消息经过各节点时还存在被恶意监听的风险[8]。基于会话模式的大文件传输需要 MSRP 实现，由于 MSRP 消息不经过 IMS 中各 CSCF，因此 IPsec 无法对其进行保护。

在基于 TLS 的方案中，文献[7]指出 UE 注册 IMS 核心网后，仅有信令层得到 TLS 安全关联逐跳加密保护。此时进行文件传输仅在 SIP 发出 MSRP 会话请求时消息可得到 TLS 保护，但后续传输过程并未进行保护。

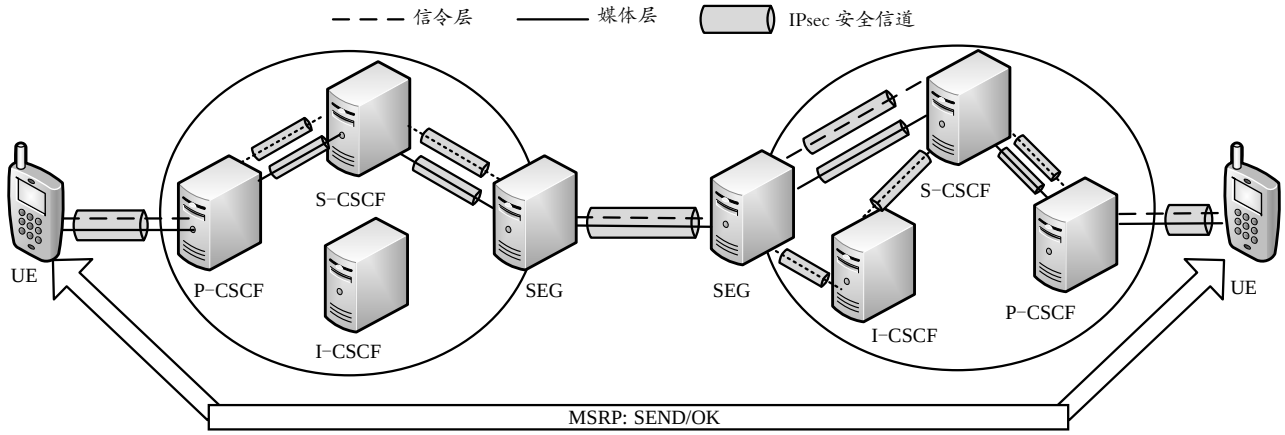


图 1 IMS 中基于 IPsec 的安全机制

与前两者采用逐跳加密不同，基于 S/MIME 的方案可实现端到端的安全加密，提供所有不需要中间节点处理的信息的安全保障，笔者提出的文件安全传输方案即基于 S/MIME 实现。

2 文件安全传输方案设计

文件安全传输方案的设计思想是将 S/MIME 中的签名和加密 2 种功能移植到 UE 中，两端 UE 通过 SIP 的 INVITE 请求建立 MSRP 会话后，发送端 UE 采用 S/MIME 对要传输的文件进行签名和加密，调用 MSRP 的 SEND 方法发送文件，接收端 UE 解密文件并验证签名，从而实现 IMS 中文件的安全传输，整个过程如图 2 所示(因 MSRP 工作在媒体层，故省去中间节点)。

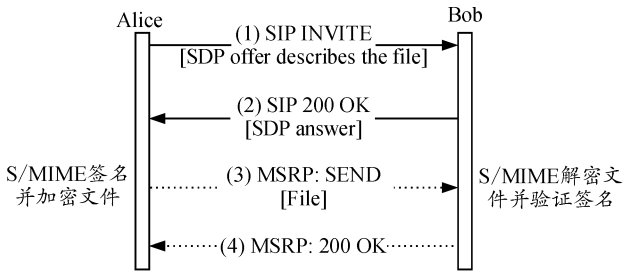
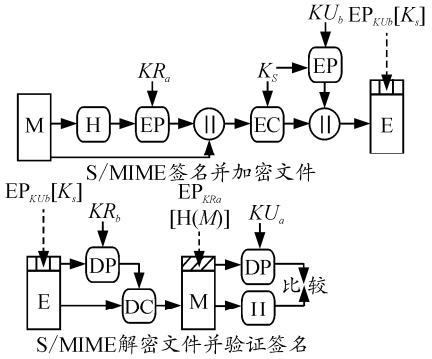


图 2 IMS 文件安全传输过程

S/MIME 对文件进行加解密和数字签名的流程如图 3 所示。



K_s：会话密钥，用于对称加密；H：hash函数；
KR_a，KR_b：用户A、B的私钥；KU_a，Ku_b：用户A、B的公钥；
EP：非对称加密；DP：非对称解密；EC：对称加密；
DC：对称解密；‖：二进制串联接；M，E：明文，密文。

图 3　S/MIME 对文件进行加解密和数字签名流程

3　方案仿真与测试

3.1　仿真测试环境

仿真环境基于 OpenIMSCore 核心平台[9]，采用 myMONSTER TCS[10]软终端形式实现 S/MIME。德国 Fraunhofer 研究院开发的 OpenIMSCore 实现了 IMS 中呼叫会话控制实体 CSCF 及一个小型的 HSS，构成了当前 3GPP 和 TISPAN 等国际组织所定义的 IMS/NGN 下一代核心网的重要组成部分。该研究院同时发布了 myMONSTER TCS 客户端解决方案，使开发人员可针对下一代网络创建多样的客户端通信应用，其基于 JAVA 开发，具有良好的可移植性，笔者选取 BouncyCastle JCE[11]实现 S/MIME。

测试环境如图 4 所示。

1) IMS 服务器：基于 OpenIMSCore 的 IMS 服务器，运行于 Ubuntu8.04 的 Linux 操作系统，可实现呼叫会话控制实体 CSCF 及 HSS 等功能。

2) UE 客户端：基于 myMONSTER TCS 开发的软终端(含有 S/MIME 模块的 UEA 和 UEB)，运行于普通 PC 的 WindowsXP 操作系统，已事先各自产生公私钥对并将公钥分发给对方。

3) WireShark 监控端：配置 WireShark 工具进行网络数据采集并分析验证，在交换机上配置端口镜像指向监控端接口。

4) 网络环境：实验室百兆局域网。

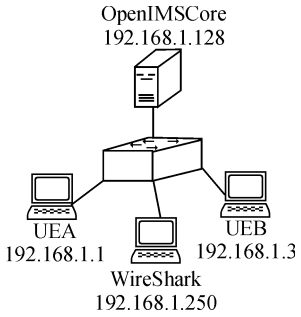


图 4　仿真测试环境

3.2　测试过程

UEA 和 UEB 先向 IMS 服务器注册，成功后 UEA 通过 UEB 的 SIP 地址发起 MSRP 会话请求。会话建立后，UEA 选择要传输的文件，分别采用直接传输和开启 S/MIME 传输 2 种方式将文件发送给 UEB，UEB 接收文件完毕后自动发送成功状态。测试传输功能，并用 WireShark 采集通信数据。

3.3　结果分析

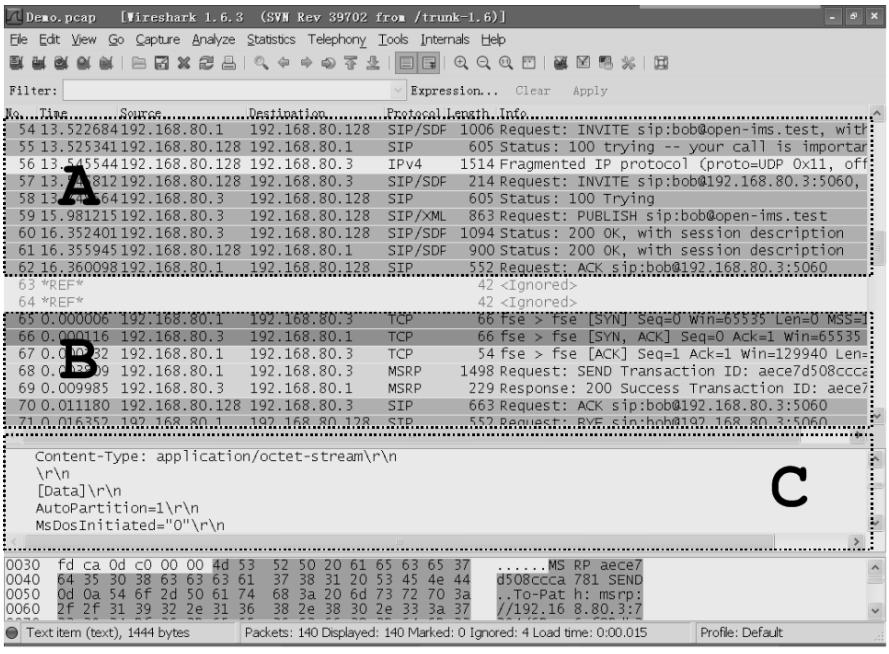


图 5　直接传输抓包结果

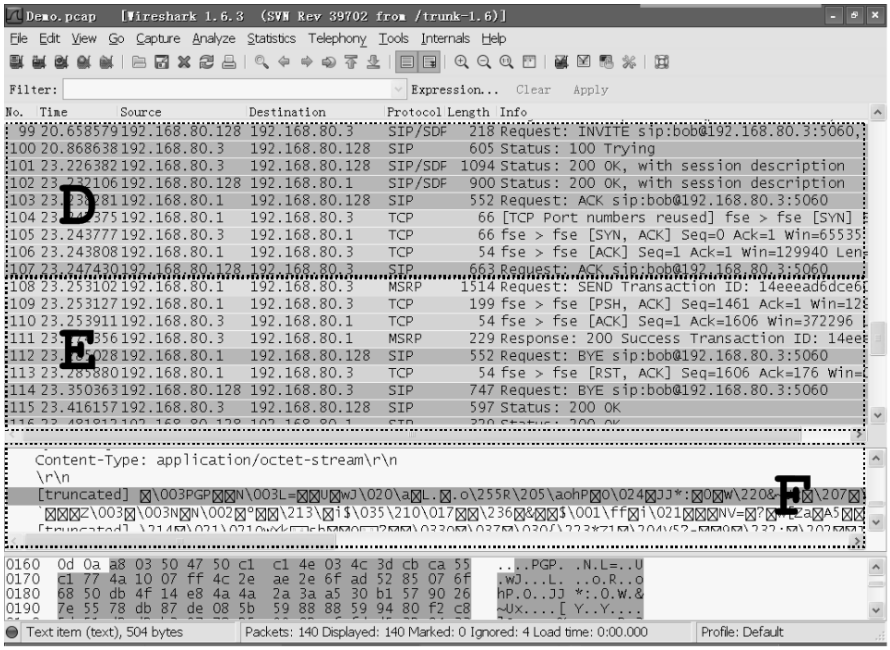


图 6　启用 S/MIME 抓包结果

仿真测试结果如图 5、6 所示。分析图 5 直接传输时 WireShark 采集的数据可看出，当 UEA 注册 IMS 服务器及发起 MSRP 会话请求时，SIP 消息将通过 IMS 中各 CSCF，如 A 区所示，图 6 中 D 区与此类似。但调用 MSRP SEND 方法传输文件时信息不通过 IMS，即第 2 节所述 IPsec 和 TLS 均无法对文件传输进行保护，如 B 区所示，图 6 中 E 区与此类似。C 区为传输的内容，为明文。

分析图 6 启用 S/MIME 时采集的数据，如 F 区所示文件经 S/MIME 加密后成为乱码不可读，文件安全传输得以实现。

4　结束语

仿真测试结果表明：基于 S/MIME 的 IMS 文件安全传输方案可实现文件的端到端安全传输，同时避免了数据通过 IMS 中各呼叫会话控制实体造成的延时。

参考文献：

[1] Third Generation Partnership Project.3GPP TS 23.228 IP Multimedia Subsystem (IMS)(Release 11)[S]. France: Valonne, 2011: 20–21.

[2] Chakraborty S, Peisa J, Frankkila Tomas, et al. IMS Multimedia Telephony over Cellular Systems[M]. America: Wiley Press, 2007: 10–12.

[3] Campbell B. The Message Session Relay Protocol (MSRP).RFC 4975[S]. America: Internet Engineering Task Force, 2007: 1–10.

[4] Ramsdell B, Turner S. Secure/Multipurpose Internet Mail Extensions (S/MIME) Version 3.2. RFC 5751[S]. America: Internet Engineering Task Force, 2010: 3–8.

[5] Camarillo G, Garcia-Martin M A. The 3G IP Multimedia Subsystem (IMS)[M]. America: Wiley Press, 2008: 453–476.

[6] 关琳，杨维忠，张琳峰. 即时消息——网络融合中的亮点业务[J]. 移动通信, 2008(14): 17–19.

[7] Third Generation Partnership Project. 3GPP TR 33.802 Feasibility study on IMS Security Extensions (Release 7)[S]. France: Valonne, 2011: 11–12.

[8] Chen Chiyuan, Wu Tinyu, Huang Yuehmin. An efficient end-to-end security mechanism for IP multimedia subsystem[J]. Computer Communications, 2008: 1–10.

[9] Fraunhofer Institute FOKUS. Open Source IMS Core[OL]. http: //www.openimscore.org, 2012.

[10] Fraunhofer Institute FOKUS. myMONSTER TCS[OL]. http: //www.monster-the-client.org, 2012.

[11] BouncyCastle. Cryto-147[OL]. http://www.bouncycastle.org, 2012.