

# IMS 接入认证机制的优化方法

陈志奎 马菲

(大连理工大学 软件学院, 辽宁 大连 116621)

**摘要:** 本文描述了 IMS 安全框架及接入过程中可能出现的安全隐患, 给出一种专门针 UMTS 终端接入 IMS 系统时认证机制的优化方法, 首先借助 AKA 机制对 USIM 的 IMSI 进行 PS 域接入认证结果, 然后采取 UICC 和 HSS 共享一个新参数 IMPIID, P-CSCF 和 S-CSCF 之间共享密钥为 K1i 的方法, 达到一定的防范功效, 在某种程度上不增加计算量的前提下提高了安全性, 并简化了信令流程。

**关键词:** IP 多媒体子系统; 认证和密钥协商; 接入认证机制

## An Optimized Method of IMS Access Authentication Mechanism

CHEN Zhi-kui MA Fei

(Software School, Dalian University of Technology, Dalian Liaoning 116621, China)

**Abstract:** This paper describes the IMS access security framework and the security risks that may arise, then gives an optimized authentication mechanism IMS for UMTS accessing the IMS system. First of all, the optimized method is by virtue of the PS domain access authentication results using USIM IMSI, and then adds a new parameter IMPIID between HSS and UICC, and sets the shared key K1i between P-CSCF and S-CSCF. To a certain extent, it improves security and simplifies signaling flow without increasing the computation.

**Keywords:** IMS; AKA; access authentication mechanism

### 1 引言

IP 多媒体子系统 (IMS) 是 3GPP 在 R5 规范中提出的, 旨在建立一个与接入无关、基于开放的 SIP/IP 协议及支持多种多媒体业务类型的平台来提供丰富的业务。它将蜂窝移动通信网络技术、传统固定网络技术和互联网技术有机结合起来, 为未来的基于全 IP 网络多媒体应用提供了一个通用的业务智能平台, 也为未来网络发展过程中的网络融合提供了技术基础。在网络演进和融合的过程中, IMS 的安全显得尤为重要。本文对 IMS 的接入安全机制进行了分析研究, 针对原来的认证协议加以优化, 增强了认证的安全性, 并简化认证流程。

### 2 3GPP IMS 安全体系介绍

3GPP IMS 安全主要涉及 IMS 的接入安全 (3GPP TS33.203), 包括用户和网络认证以保护 IMS 终端和

网络间的业务; 以及 IMS 的网络安全 (3GPP TS33.210)<sup>0</sup>, 处理属于同一运营商或不同运营商网络节点之间的业务保护。除此之外, 还有对用户终端设备和通用集成电路卡/IP 多媒体业务身份识别模块 (UICC/ISIM) 安全问题。3GPP IMS 的安全框架<sup>0</sup>如图 1 所示。

图 1 显示了 5 个不同的安全层面, 它们将用于 IMS 安全保护中不同的需求, 并分别被标注为 (1)、(2)、(3)、(4) 和 (5)。(1)、(2) 被称为 IMS 接入网的安全, 而 (3)、(4)、(5) 则是网络域内功能模块的安全。功能如下: (1) 提供用户和网络之间的双向身份认证。(2) 为 UE 和 P-CSCF 间的通信提供一个安全连接, 用以保护 Gm 参考点的安全。其中, 包括加密和完整性保护。(3) 提供网络域内 CSCF 和 HSS 之间的安全。(4) 为不同网络间 CSCF 提供安全。(5) 为网络内部 CSCF 提供安全。

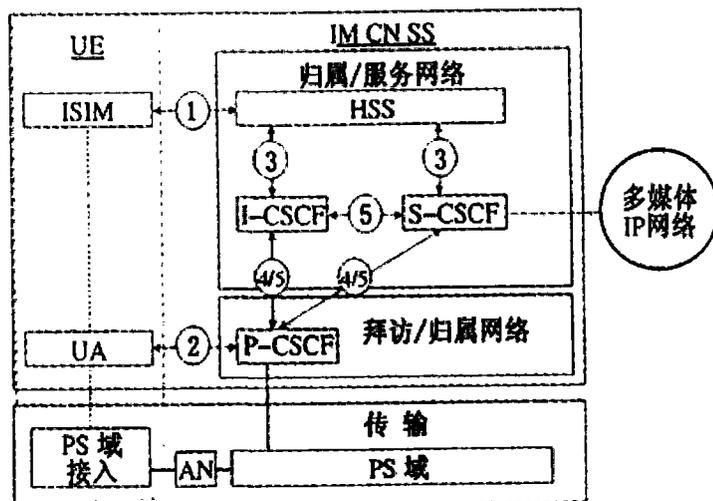


图 1 IMS 安全框架图

### 3 IMS 接入认证机制

IMS 接入认证机制的实现作为整个 IMS 安全方案实施的第一步, 是保证 IMS 系统安全的关键。IMS 的接入安全机制承担两大任务, 一是对接入用户的鉴权 (包括认证和授权); 二是鉴权结束后, UE 和 P-CSCF 之间建立 IPSec SA (即 IPSec 安全关联), 为后续 SIP 信令提供安全保护。

AKA 机制是由因特网工程任务组 (IETF) 制定、并被 3GPP 采用广泛应用于 3G 无线网络的鉴权机制。IMS 的鉴权机制沿用了这种机制的原理和核心算法, 故称之为 IMS AKA 机制<sup>[3]</sup>。IMS AKA 机制是对 HTTP 摘要认证机制的扩展, 主要用于用户的认证和会话密钥的分发, 它的实现基于一个长期共享密钥 (Key) 和一个序列号 (SQN), 它们仅在 HSS 的认证中心模块 (AuC) 和 UE 的 ISIM 中可见。

IMS 的鉴权机制采用鉴权和密钥协商 (AKA) 机制来实现的, 需要协商安全密钥建立 IPSec SA。实际上 AKA 机制的运行和 IPSec SA 的建立都是结合到 SIP 消息中。在 IMS 的注册过程中, 携带 AKA 参数的 SIP 信令在 UE 和 IMS 网络认证实体之间进行交互, 按照 AKA 机制来传输和协商 AKA 参数, 从而实现接入认证和密钥协商的过程。可以这么认为, 整个 IMS 的接入安全机制的建立是通过 IMS 的注册过程来完成的。IMS AKA 接入认证的具体流程<sup>0</sup>如图 2 所示。

### 4 IMS AKA 接入认证机制的安全隐患及优化方法

对于 UMTS 移动接入, IMS 是叠加在分组域 (PS) 之上的, 应用 PS 域来进行多媒体信号的承载和传输, 首先使用 AKA 机制对 USIM 的 IMSI 进行 PS 域接入认证, 再对 ISIM 的 IMPI 进行 IMS 认证。在 IMS 应用中, 类似认证过程前后进行, 会造成不必要的信令开销增加网络负担。

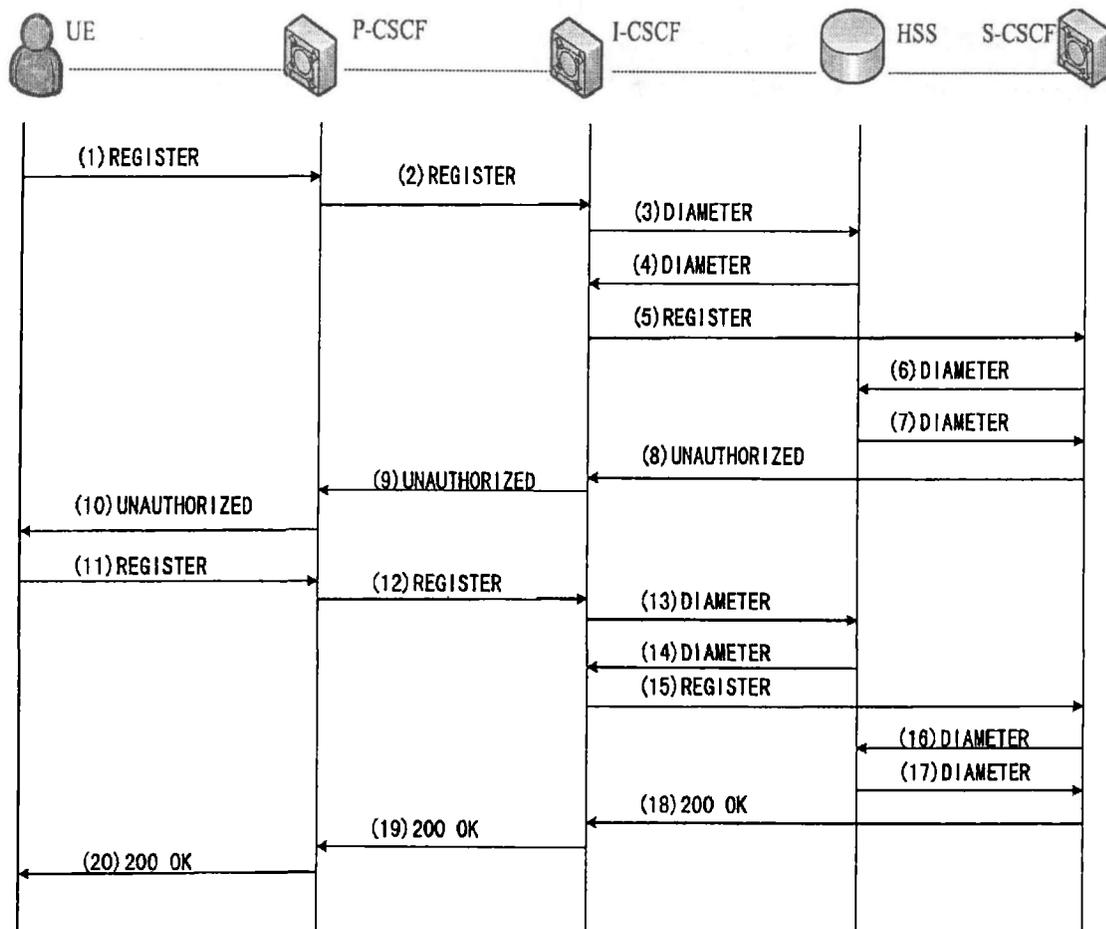


图2 基于AKA的IMS接入认证流程图

通过对IMS AKA协议过程分析发现，移动终端基于IMS AKA机制在注册过程中存在的如下安全隐患。

(1) 虽然UE和P-CSCF之间可以通过AKA机制协商的安全性密钥对SIP信令进行加密性和完整性保护，但是初始注册请求REGISTER消息却是在安全密钥尚未协商的时候发送的，故该消息没有受到任何安全保护而且是用明文发送的，造成IMPI仍然暴露给访问网络，攻击者可以轻而易举地获取用户的注册信息，从而造成用户隐私泄密。

(2) UE并没有对IMS核心网络的接入点P-CSCF进行身份认证，会给攻击者提供冒充中间人实施攻击的机会。UE在P-CSCF成功注册后，恶意UE可能尝试直接向S-CSCF发SIP消息，造成UE免费通话或破坏其他用户通话等问题。

#### 4.1 优化的AKA认证与密钥分配协议方法

为防止上述可能攻击，并简化认证流程，提出针对移动终端的接入认证优化方法（只考虑同一运营商情况），改进前后流程图如图3所示。

总而言之，在用户端和HSS端各新加入参数IMPIID代替原IMPI的传递；并且在不同地理位置的P-CSCF和S-CSCF间设立共享密钥K1i；借助PS域认证结果，初次注册时传递TMSI，完成网络对用户的认证，从而省略认证响应（XRES）参数计算和传递。

#### 4.2 优化后具体接入认证过程

优化后的具体接入认证过程如图4所示。

(1) UE在初始注册请求SIP REGISTER消息中带参数IMPIID（IMPI）及USIM的TMSI（IMSI）发送到P-CSCF，该IMPIID和相应IMPI存储在ISIM卡中，TMSI则通过SGSN添加到该注册消息里，TMSI传递过程参考文献<sup>0</sup>。

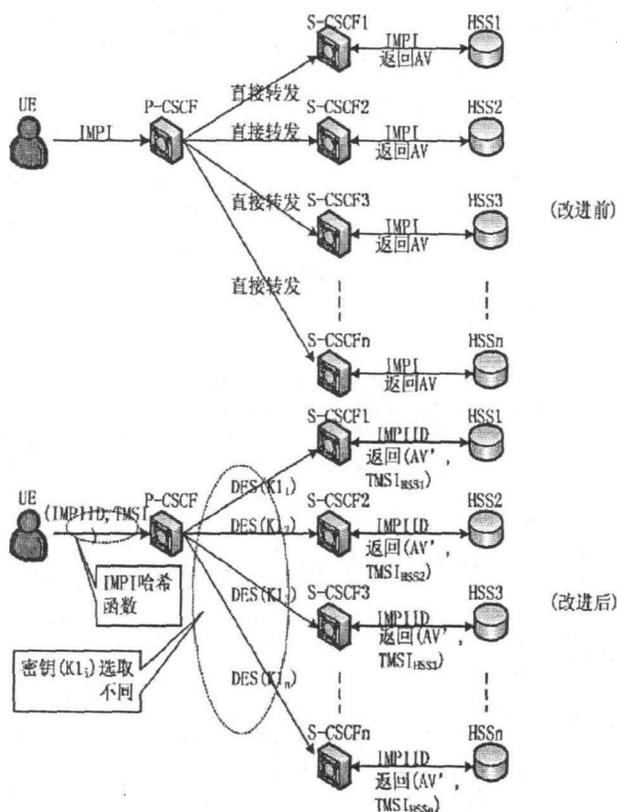


图3 IMS AKA 改进前后接入认证方案

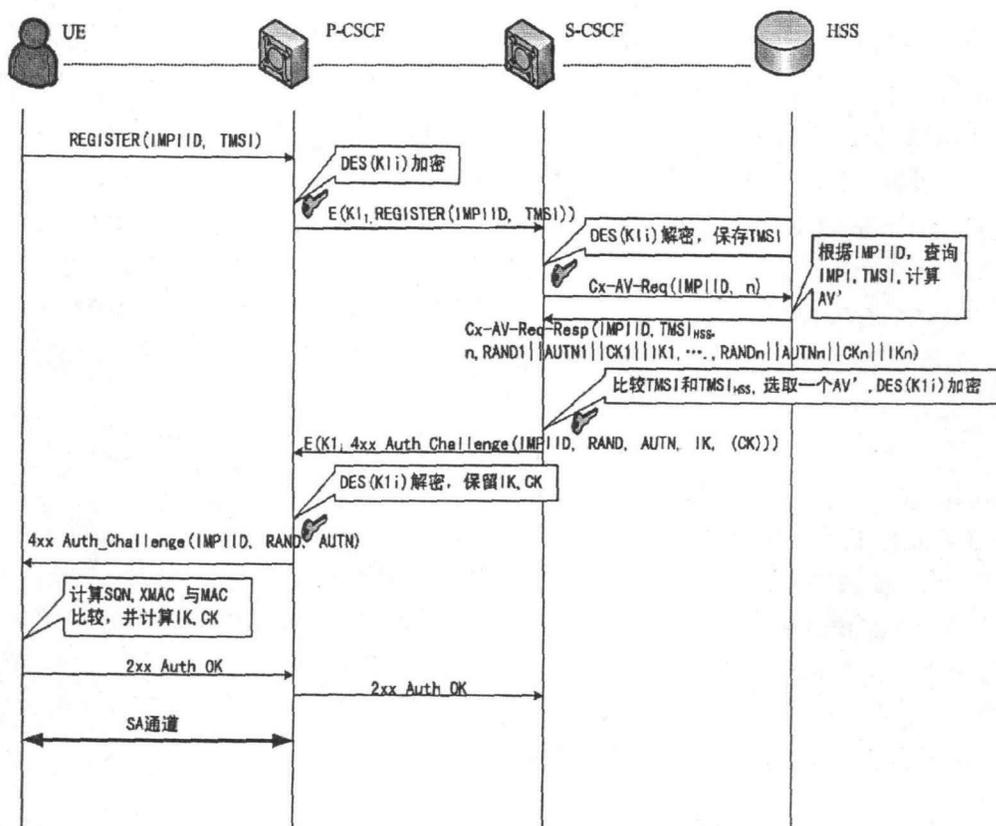


图4 改进后注册流程图

(2) P-CSCF 将接收的 REGISTER 消息经过 DES (k<sub>1i</sub>) 加密后转发选定 S-CSCF (图 4 省略 I-CSCF 部分)。

(3) S-CSCF 将接收到的 REGISTER 消息进行 DES (k<sub>1i</sub>) 解密后, 如果发现该用户还没有被认证, 则

S-CSCF 通过传送参数 IMPIID 向 HSS 请求认证数据, 同时保存接收到的 TMSI。

(4) HSS 通过 IMPIID 查询 IMPI, 得到用户信息包含 TMSI (IMSI), 计算得到一组认证数 AV (RAND||CK||IK||AUTN), 此时不必计算 XRES。HSS 将这些认证数据和 TMSI<sub>HSS</sub> 一起发送给 S-CSCF。

(5) S-CSCF 从 HSS 得到所需的安全相关的参数 AV 及 TMSI<sub>HSS</sub>, 与原先保存的 TMSI 比较: 相同则完成网络对用户的认证。

(6) S-CSCF 将得到的 AV 及 IMPIID 进行 DES ( $k_{1i}$ ) 加密后以 401 应答消息方式发送给 P-CSCF。

(7) P-CSCF 再次进行 DES ( $k_{1i}$ ) 解密, 将 AV 中的完整性密钥 IK 和保密性密钥 CK 保存下来, 并将它们从 AV 中删除掉。继续以 401 应答消息转发 AV 中剩余参数给 UE。

(8) UE 接到该鉴权消息后, 取出 AUTH 和 MAC 计算 IK, CK, XMAC 和接收到的 MAC 比较来完成终端对 IMS 网络认证。保存 IK, CK 为后续通信提供完整性保密性保护。

(9) UE 对 IMS 网络认证成功, 以 2xx Auth-OK 消息通知 P/S-CSCF 认证成功, 以后消息将通过 UE-P-CSCF 之间商定的安全联盟 (SA) 通道传送。

通过上述步骤描述, UE 完成 IMS AKA 接入认证。

### 4.3 优化方法合理性分析

对于移动终端使用 IMS 业务时, UE 首先在通过 PS 域认证后, 再进行 IMS 注册认证和密钥分配。UMTS 用户终端同时携带私有信息 IMSI 和 IMPI。

首先, 经过 PS 域认证与 PDP 上下文激活后, 从 SGSN (GPRS 业务支撑点) 获得唯一 IMSI 值, 为了防止无线链路窃听, 保证移动用户识别的安全性, 在空中接口传递 TMSI 代替 IMSI。SGSN 将移动终端 (MS) 对应的 TMSI 添加到 REGISTER 消息, 发送到 S-CSCF 后将 TMSI 值保存, 然后和从 HSS 处得到的 TMSI<sub>HSS</sub> 比较, 先完成网络对用户的认证, 再完成用户对网络认证, 因此, 原来用于网络对用户认证的参数认证响应 (RES) 则显多余, 省略掉, 减少计算信令开销。而且对比图 2 图 4, 由于使用了 PS 域的认证结果, 使得认证由原来的 2 次“提问-回答”简化为一次, 简化信令流程。

与此同时, 设置 UICC 和 HSS 共享一个新参数 IMPIID,  $IMPIID=F(IMPI)$  (单向哈希函数), IMPIID 事先已由运营商分配好, UE 端和 HSS 端只需查询, 不会增加计算量 (考虑到用户数量增加, HSS 侧可根据区域建立同类型多个用户表避免查询复杂)。在初次注册过程时, UE 端传送 IMPISID 代替 IMPI, 在 HSS 端只需查询 IMPIID 和 IMPI 的对应关系表后, 即可得到对应的 IMPI 的用户资料, 即使有中间人攻击, 得到 IPMIID 值, 但由于是单向哈希函数加密也无法得到相应的 IMPI, 只要保证了用户卡和 HSS 的安全, 就能有效地保证了用户身份的安全性, 这样能够防止假冒者的攻击和偷窃。

其次, UE 漫游时, P-CSCF 和 S-CSCF 之间处于不同的地理位置, 有可能受到伪装攻击, 可采取 P-CSCF 和 S-CSCF 之间对称加密 DES 算法, 共享密钥为  $K_{1i}$ , 其中参数  $K_{1i}$  的选择: 同一运营商内可根据地域给每个 P-CSCF 编号, 每 2 个 P-CSCF 共享一个  $K_{1i}$ , 其对应关系只有运营商知道 (例如大连-北京的密钥为  $K_{11}$ , 大连-上海的密钥为  $K_{12}$ ),  $K_{1i}$  可以按固定时间统一调整防止密钥  $K_{1i}$  泄露。P-CSCF 和 S-CSCF 之间传送的 SIP 消息采用对称密钥 ( $K_{1i}$ ) DES 加密解密方式, P-CSCF 和 S-CSCF 之间设置新的密钥  $K_{1i}$ , 若不知准确的 P-CSCF 和 S-CSCF 的对应关系, 即便获得对称密钥 ( $K_{1i}$ ), 也无法长期伪装 P-CSCF 发送 SIP 消息, 使得通信更加安全, 并且能够完成相互鉴权的作用, 从而一定程度上也解决了 UE 绕过 P-CSCF 和 S-CSCF 直接发送 SIP 消息的问题。

## 5 结束语

本文通过对 IMS 用户接入认证机制的研究分析, 专门针对 UMTS 移动终端的 IMS 接入认证机制加以优化。优化方法在保持原协议安全性的基础上, 不增加 UE 端计算复杂度的前提下, 有效地防止了攻击, 增

强了安全性，并且简化了认证流程。

### 参考文献

- [1] 3GPP TS 33.210v7.2.0.3G security; Network Domain Security; IP network layer security (Release 7) [S]. 13-15
- [2] 3GPP TS 33.203 V5.1.0.3rd Generation Partnership Project; Technical Specification Group Services and System Aspects; 3G Security; Access security for IP-based services [S]: 8-12
- [3] NIEMI A, ARKKO J, TORVINEN V, et al. Hypertext transfer protocols (HTTP) digest Authentication using authentication and key agreement (AKA) [R]. RFC3310, IETF. 2002
- [4] ChungMing Huang and Jian Wei Li. One-Pass Authentication and Key Agreement Procedure in IP Multimedia Subsystem for UMTS [R]. 21st International Conference on Advanced Networking and Applications (AINA'07) 0-7695-2846-5/07 2007IEEE

### 作者简介

陈志奎，男，1968年生，四川阆中市，大连理工大学教授，研究生导师，主要研究方向为网络通信理论与技术，无线传感器理论与应用等；

马菲，女，1979年生，河北辛集市，研究生，主要研究方向为无线网络通信理论与技术。