IMS 中的一种跨域信任机制

王晓雷,郭云飞,胡金萍
WANG Xiao-lei,GUO Yun-fei,HU Jin-ping

国家数字交换系统工程技术研究中心,郑州 450002
National Digital Switching System Engineering & Technological Research Center,Zhengzhou 450002,China

WANG Xiao-lei,GUO Yun-fei,HU Jin-ping.Cross-Domain trust mechanism in IMS.Computer Engineering and Applications,2008,44(32):101-104.

Abstract: Analyzed the authorization mechanism of media layer,control layer and application layer in IMS.To the problem of overhead of Cross-Domain authorization when UE roaming in IMS,proposed a Cross-Domain trust mechanism of the control layer in IMS.The Cross-Domain trust mechanism added four functional modules which are trust certificate database,certificate directory, assertion generator and tag extractor.The trust mechanism realized the single-authorization strategy to UE,and reduced the cost of repeat authorization.Using Open SER realized the function of each entity in IMS and built a simple simulation network,and then did simulation of Cross-Domain trust mechanism in the network.The simulation result shows that the Cross-Domain trust mechanism reduces 0.417 7 s of time cost.

Key words: IP Multimedia Subsystem(IMS);Cross-Domain security;trust mechanism;cost

摘 要:分析了 IMS 中媒体层、控制层和应用层的认证机制,针对 IMS 用户漫游时跨域认证造成开销过大的问题,在 IMS 控制层提出了一种跨域信任机制。该机制通过在 HSS 和 S-CSCF 中增加信任证书数据库、证书目录、声明发生器和标签提取器四个功能模块,实现了用户漫游时的单次认证策略,减小了因重复认证造成的开销。利用 Open SER 实现了 IMS 中各个实体的功能,搭建了简易的 IMS 仿真环境,然后在仿真网络中对跨域信任机制进行验证。仿真结果表明,跨域信任机制减少了 0.417 7 s 的时间开销。

关键词:IP 多媒体子系统;跨域认证;信任机制;开销
DOI:10.3778/j.issn.1002-8331.2008.32.030 **文章编号**:1002-8331(2008)32-0101-04 **文献标识码**:A **中图分类号**:TP181

3G 网络被分为3 个不同的域,分别是:电路交换域、分组交换域和 IP 多媒体子系统域(IP Multimedia Subsystem,IMS)。电路交换域的职能是采用电路交换技术继续提供第二代移动通信系统所具有的语音和多媒体服务;分组交换域为终端提供 Internet 的接入, 它主要被视为一种接入技术;IMS 是 3G 中最重要的域,IMS 采用 SIP 作为主要的信令协议向用户提供多媒体服务。未来网络融合的趋势是 IMS 逐渐融合电路域和分组域,并把固定网络纳入 IMS 管理的范围内。

因此,在 IMS 中用户可以采用多种方式接入 IMS 网络,例如 3G、xDSL、GPRS、WLAN、Internet 等。IMS 在融合各个接入网络的同时, 也引起人们对 IMS 多个域之间信任协商问题的关注。特别是终端在移动过程中需要频繁与很多位置、功能都不同的服务单元进行交互,造成了完成一次会话需要认证多次的现象。这对于当前的相对静态独立的身份认证机制提出新的研究方向,需要一种比较灵活的标准机制来使 IMS 服务实现单次认证的策略。

1 IMS 中的认证机制

IMS 是一个分层的网络体系,它包含三个彼此独立的网络层面,分别为媒体层、控制层和应用层。媒体层基于各个接入网传送媒体数据流;控制层对用户的呼叫会话进行控制,是整个 IMS 的核心; 应用层为用户提供多种服务。一个用户从接入 IMS 网络到使用各种业务,需要在 IMS 的三个层次中分别进行认证[1]。

1.1 IMS 媒体层认证

用户在 IMS 媒体层的认证取决于各个接入网,是用户接入 IMS 网络的先决条件,不同的接入网络有着各自不同的认证机制。比如在 GPRS 中,其认证机制和 GSM 中的类似,采用单向身份认证,无法防止伪造网络设备的攻击。这种情况在 3G 中得到了改进,采用了 AKA 认证机制,使网络和用户进行双向认证。IMS 在控制层中把 AKA 机制和 SIP 中的 Http Digest 机制相结合[2],具体的 AKA 机制将在控制层认证中进行介绍。

1.2 IMS 控制层认证

IMS 控制层中的认证基于 UE 和 HSS 之间的共享参数。以

基金项目:国家高技术研究发展计划(863)(the National High-Tech Research and Development Plan of China under Grant No.2007AA01Z434)。
作者简介:王晓雷(1982-),男,硕士研究生,主要研究方向为无线通信安全;郭云飞(1963-),男,教授,博士生导师,主要研究方向为下一代网络体系架构,863 通信主题专家组组长;胡金萍(1982-),女,助理工程师,主要研究方向为电信网络安全。
收稿日期:2007-12-10 **修回日期**:2008-03-25

UE 使用 ISIM 为例,ISIM 和 HSS 共享的参数有 *IMPU*(公共身份标识)、*IMPI*(私有身份标识)、用户归属网络的域名、IMS 域内的 *SQN* 序列号、认证密钥 *key*。认证通过一个 SIP REGISTER 请求来完成,共有两次往返过程[3-4],如图 1 所示。

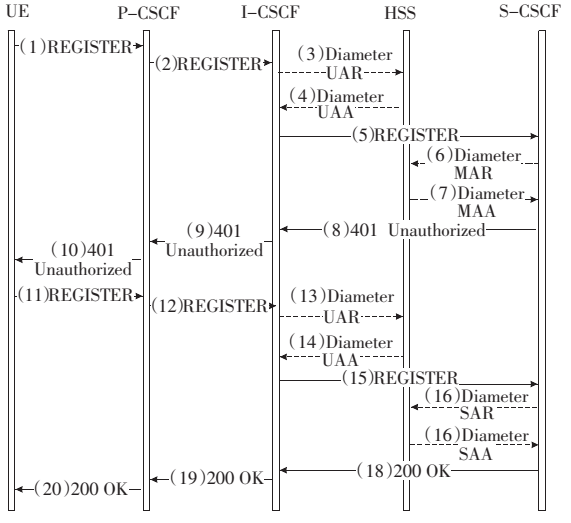

图 1　在 IMS 控制层的认证流程

1.2.1　认证向量的分发

假设用户 user 向域名为 sip:home.net 的归属网络注册。则(1)REGISTER 消息的简要格式如下:

```
REGISTER sip:home.net SIP/2.0
From:<sip:user@home.net>;tag=s8732n
To:<sip:user@home.net>
Contact:<sip:[1080::8:800:200C:417A];comp=sigcomp>
Authorization:Digest username="user_private@home.net"
                realm="home.net",nonce="  "
                uri="sip:home.net",response="  "
Security-Client:ipsec-3gpp;alg=hmac-sha-1-96;
                 spi-c=23456789;spi-s=12345678;
                 port-c=2468;port-s=1357
```

(1)REGISTER 消息没有进行任何安全性保护。Authorization 字段包含了 *IMPI*、归属网络域名,其中 *nonce* 和 *response* 用来进行认证,此时值为空。Security-Client 字段用于建立 SA。

P-CSCF 通过执行 DNS 流程[5]定位 I-CSCF,并把 REGISTER 消息发送到 I-CSCF。I-CSCF 在收到注册消息后向 HSS 发送包含 *IMPU*、*IMPI*、拜访网络标识的 Diameter 用户认证请求。HSS 根据参数内容做出应答,并返回一组 S-CSCF 的性能。I-CSCF 根据 S-CSCF 的性能为用户选择一个合适的 S-CSCF,并把 REGISTER 消息发向 S-CSCF。

S-CSCF 收到注册消息后从 HSS 下载若干 5 维的认证向量 ***V***。

$$\boldsymbol{V}=(RAND,AUTN,XRES,IK,CK) \tag{1}$$

AUTN 由共享的密钥 *key* 和序列号 *SQN* 生成。S-CSCF 利用第一个认证向量建立 401 未授权响应来传送 *nonce* 值和加密密钥 *CK*、完整性密钥 *IK*。

$$nonce=RAND+AUTN=RAND+key+SQN \tag{2}$$

P-CSCF 收到 401 未授权响应后取出 *CK* 和 *IK* 用来建立 SA,然后把剩下的消息发给用户。此时 401 消息中 Authorization 和 Security-Server 字段为:

```
Authorization:Digest realm="home.net"
                nonce="dcd98b7102dd2f0e8b11d0f600bfb"
                algorithm=AKAv1-MD5
Security-Server:ipsec-3gpp;q=0.1;alg=hmac-sha-1-96;
                 spi-c=98765432;sip-s=87654321;
                 port-c=8642;port-s=7531
```

1.2.2　认证的过程

用户收到 401 消息后,由 *nonce* 推算出 *RAND*、*AUTN*、*CK*、*IK*。用共享的 *key* 和 *SQN* 计算得到一个 *AUTN*,如果它和接收到的 *AUTN* 值一样,则网络通过认证。然后用 *key* 和接收到的 *RAND* 产生响应值 *RES*,并通过(11)REGISTER 消息的 *response* 字段发送给 S-CSCF。S-CSCF 把接收到的 *RES* 值与预期认证向量中的 *XRES* 进行比较,如果匹配,则用户通过认证,并返回一个 200(OK)消息。

经过媒体层和控制层的认证后,用户可以完成在 IMS 中的注册。

1.3　IMS 应用层认证

用户在使用业务前需要与应用服务器间进行相互认证,因此需要定义一套通用的认证框架。通用认证体(Generic Authentication Architecture,GAA) 描述了一个这样的框架。作为 GAA 的一部分,IMS 网络定义了通用引导体系(GBA)[6]、引导服务器功能(BSF)和基于 AKA 协议的相互认证机制。通用的GBA 参考模型如图 2 所示:

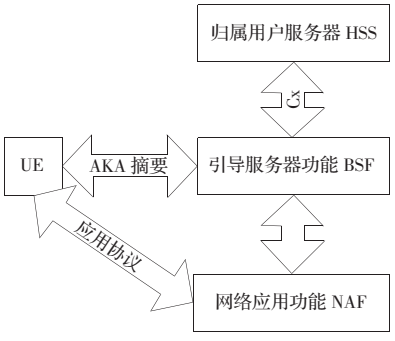

图 2　GBA 参考模型框图

在图 2 中 BSF 和 UE 之间通过 HTTP Digest AKA 协议相互认证,并产生会话密钥,该会话密钥用于保护 UE 和网络应用功能(NAF)之间的数据。BSF 能够从 HSS 上获得用户的安全设置信息。通常 BSF 与 HSS 都位于一个运营商的网络中。其中,NAF 相当于应用服务器。

2　跨域认证造成的问题

IMS 中的跨域通常有两种情况:一是指在媒体层跨越不同的接入网;二是指在控制层跨越不同的安全域。安全域是 IMS 网络域安全中的重要概念, 是一个由独立权威机构管理的网络,具有典型的安全水平和服务。一个安全域可以代表一个归属网络或拜访网络,通常指一个 S-CSCF 负责的区域。IMS 支持用户在不同安全域之间漫游,下面从用户是否漫游的角度分析 IMS 跨域认证的问题。

2.1　用户在归属网络的认证

(1)接入网络认证。根据不同的接入网采用不同的认证方式,设该次认证的信令开销为 T_1。

(2)控制层认证。用户在接入网认证成功后允许接入到 IMS 网络,然后在控制层进行第二次认证,设该次认证的信令开销

为 T_2。

(3)应用层认证。用户在控制层的认证成功后完成了在 IMS 网络的注册，当用户使用 IMS 提供的各种业务时，用户与 IMS 的应用服务器之间进行认证。设该次认证的信令开销为 T_3。

由此可见，当用户在归属网络中使用 IMS 业务时，需要进行三次认证，总共的信令开销 T 为：

$$T=T_1+T_2+T_3 \tag{3}$$

2.2　用户漫游到拜访网络的认证

当一个已经在归属网络认证过的用户漫游时，相当于进入了另一个安全域。根据 IMS 网络域安全的要求，用户若要在拜访网络使用 IMS 业务，必须在控制层向归属网络进行重新认证。设在拜访网络中接入认证的开销为 T_1'，在控制层重新认证的开销为 T_2'，则用户从在归属网络中进行认证，到漫游到拜访网络使用 IMS 业务，总共的信令开销 T' 为：

$$T'=T_1+T_2+T_1'+T_2'+T_3 \tag{4}$$

由此可见 $T'>T$。即当用户处于漫游状态时，业务所需的开销大于非漫游状态。

3　IMS 中的跨域信任机制

3.1　设计思想

针对用户漫游时认证开销过大的问题，在控制层提出了一种跨域信任机制，提出了信任标签和信任声明的概念。通过在 HSS 中设置信任证书数据库、证书目录、声明发生器三个模块和在 S-CSCF 中设置标签提取器模块，使用户单次登录即可享受 IMS 服务。

(1)信任证书数据库：存储所有已经通过认证的用户认证信息，称为信任证书。信任证书包括归属 HSS、S-CSCF 的地址，*IMPI*，*IMPU*，同步序列号 *SQN*，以及已经协商好的 *CK* 和 *IK*。同时生成信任证书在数据库中的位置信息。

(2)证书目录：为信任证书生成一个信任标签，信任标签是信任证书的名称。对信任证书在数据库中的位置和信任标签进行绑定，生成一个目录。

(3)声明发生器：按照目录查询信任证书数据库，提取信任证书。然后把信任证书以信任声明(Assertion)的方式发送到标签的源地址。信任声明是信任证书的发送载体。

(4)标签提取器：当 S-CSCF 收到一个注册请求时，判断该注册请求中是否存在信任标签。若存在，则提取出标签并将其发向 HSS 中的证书目录；若没有，则利用 S-CSCF 的原功能完成用户的认证注册。

3.2　信任机制的流程及开销分析

3.2.1　跨域信任机制流程

为了方便仅讨论两个域之间用户的信任交互问题。信任机制流程如图 3 所示。

(1)信任标签的分发

用户在归属域 A 进行注册认证时的标签分发流程如图 3 中的实线箭头所示，共有 7 个步骤。

①注册认证消息经过 P-CSCF 转发后到达归属域 A 的 S-CSCF。因为是用户首次注册认证，此时 REGISTER 消息中没有标签。

②标签提取器把没有标签的消息转到 S-CSCF 的原功能模块进行处理。

③经过 IMS 控制层认证机制的两个往返流程后用户通过认证，S-CSCF 向 HSS 发送 SAR 消息存储用户的认证信息。

④HSS 原功能模块把用户的认证信息转存到信任证书数据库中。

⑤信任证书数据库以信任证书的形式存储该用户的认证信息，并把该信任证书在数据库中的位置发送到证书目录。

⑥证书目录收到信任证书在数据库中的位置信息后，生成信任标签和目录。然后向 S-CSCF 发送包含标签的 SAA 消息。

⑦S-CSCF 向用户发送包含标签的 200(OK)响应消息。至此用户在归属域的注册认证过程结束，获得了信任标签 Tag，并在以后的所有注册请求中包含该标签。

(2)信任声明的发布

当用户漫游到拜访域 B 时，跨域信任机制的认证流程如图 3 中的虚线箭头所示，共有 7 个步骤。

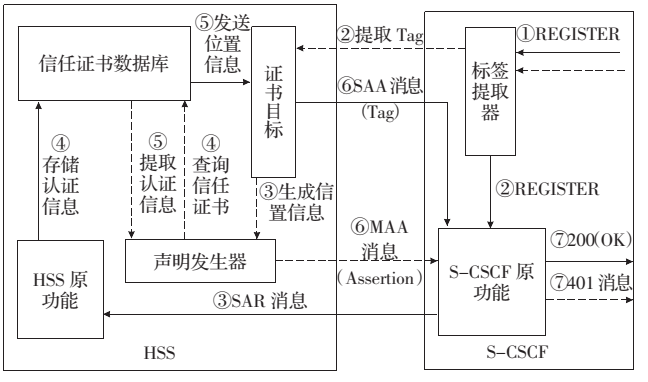

图 3　跨域信任机制流程

①用户在拜访域 B 的认证消息经过转发后到达归属域 A 的 S-CSCF。因为是用户的重新认证，所以此时 REGISTER 消息中含有信任标签 Tag。

②标签提取器把信任标签 Tag 提取出来，然后发向 HSS 中的证书目录。

③证书目录从目录中查询该标签所对应的信任证书在数据库中的位置，然后将位置信息发给声明发生器。

④声明发生器根据收到位置信息，到信任证书数据库中查询该用户的信任证书。

⑤声明发生器提取数据库中信任证书中的用户认证信息。

⑥声明发生器把认证信息封装成信任声明，将其存放在 MAA 消息中发向归属域的 S-CSCF。

⑦归属域的 S-CSCF 向拜访域的 S-CSCF 发送包含声明的 401 消息。当拜访域 B 的 S-CSCF 收到该消息后提取出信任声明，和用户协商建立新的安全联盟。至此 IMS 的跨域信任机制流程结束。

3.2.2　跨域信任机制的开销

从跨域信任机制的流程可以看出，用户在拜访网络控制层的重新认证流程缩短了一半。由原来的两个往返过程减少为一个往返过程。设跨域信任机制的开销为 T_o，则 T_o 的值如下：

$$T_o=T_1+T_2+T_1'+\frac{T_2'}{2}+T_3 \tag{5}$$

由此可见 $T_o<T'$，即跨域信任机制的开销小于原来的认证机制，节省了 $T_2'/2$ 的开销。因为网络在控制层对用户进行重新认证时，需要跨越多个网络实体，所以节约的开销是非常可观的。

3.3　主要数据结构

信任标签和信任声明由 SIP 协议来传送，因此主要给出它

们在 SIP 消息中的结构。

(1)信任标签的数据结构

在 UE 的 REGISTER 消息中,信任标签位于认证字段 Authorization 中,具体 SIP 消息的简要结构如下:

```
REGISTER sip:home.net SIP/2.0
From:<sip:user@home.net>;tag=s8732n
To:<sip:user@home.net>
Contact:<sip:[1080::8:800:200C:417A];comp=sigcomp>
Authorization:Digest username="user_private@home.net"
              realm="home.net",nonce=" "
              uri="sip:home.net",response=" "
              Tag="12345678"
```

(2)信任声明的数据结构

信任声明主要位于 401 消息的 Authorization 字段中,具体 SIP 消息的简要结构如下;

```
Authorization:Digest realm="home.net"
              nonce="dcd98b7102dd2f0e8b11d0f600bfb"
              algorithm=AKAv1-MD5
              Assertion="impi,impu,sqn,ck,ik,ip"
```

4 跨域信任机制的验证

4.1 仿真环境的搭建

4.1.1 利用 Open SER 实现 CSCF 实体的功能

Open SER 是一个成熟且灵活的开源 SIP 服务器,它用途很广,代码量很小,是用纯 C 实现的,其特殊的优化结构保证了高性能[8]。它可以用作注册服务器、位置服务器、代理服务器等多种 SIP 服务器。通过对 Open SER 进行配置,可以实现 IMS 中各个 CSCF 的功能。

(1)P-CSCF、S-CSCF、I-CSCF 功能的实现

下载 openser-1.1.0-tls_src.tar.gz,在 PC 上进行安装。对每台机器上的 openser.cfg 进行配置,主要对 IP 地址及其端口进行指定,通过设置不同消息的接收处理和发送策略,使 PC 分别实现 P-CSCF、S-CSCF 和 I-CSCF 的功能。

(2)HSS 功能实体的实现

在对 openser.cfg 进行地址和端口配置的同时,对 openser.cfg 进行数据库配置。可以通过运行其自带脚本 openser.mysql.sh 完成 Open SER 数据库的创建,然后添加本地用户的各种信息,使 HSS 具有认证与注册的功能。

(3)终端 UE 的实现

用开源的 SIP communicator 作为测试终端,它支持 Authentication、Path 和 Service-Route 等字段。

4.1.2 仿真网络架构及设置

为了简化实验过程节省开发时间,在仿真网络中省去 I-CSCF、HSS 和 DNS,把 HSS 中授权认证的功能集成在 S-CSCF 中实现。具体仿真网络结构如图 4 所示。

(1)信任标签的实现

在 UE 所有注册消息的 Authorization 字段中增加一个 Tag 状态标志来代替信任标签的功能,UE 认证注册成功之后 Tag 标志设置为 1,其余情况设置为 0。

(2)新增四个功能实体的实现

省去证书目录和声明发生器模块,在 S-CSCF(2)中设置一个缓存空间完成信任证书数据库的功能,当收到的注册消息中 Tag=1 时,S-CSCF(2)从缓存中提取 UE 的认证信息并发向标

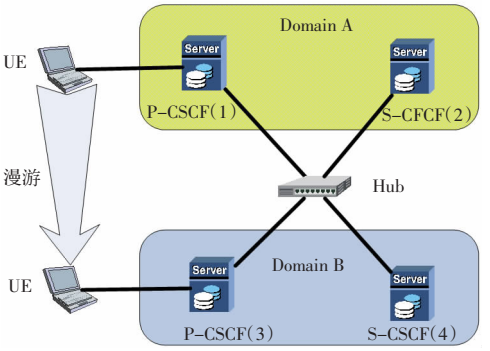

图 4 跨域信任仿真网络结构

签的源 S-CSCF 地址;当 Tag=0 时,S-CSCF(2)按照正常的认证流程对 UE 进行认证。

(2)消息路由的设置

设 UE 的首跳地址为 P-CSCF,P-CSCF 的下一跳地址为 S-CSCF,简化了 P-CSCF 和 S-CSCF 的发现流程。

(3)跨域信任机制的流程实现

首先,UE 在归属域 Domain A 中经过 P-CSCF(1)和 S-CSCF(2)完成注册认证流程,在 S-CSCF(2)的缓存中保存 UE 的认证信息。

然后 UE 在拜访域 Domain B 中重新进行注册认证,设置消息中 Tag=1。认证消息经过 P-CSCF(1)后到达 S-CSCF(4),S-CSCF(4)按照原来的跨域认证机制把 UE 的 REGISTER 消息转发到 S-CSCF(2),并在 S-CSCF(2)中对消息中的 Tag 值进行判断。按照信任机制提取缓存中 UE 的认证信息,把信息存放在 401 消息中的声明字段 Assertion 中发回给 S-CSCF(4)。然后 S-CSCF(4)利用收到的认证信息完成对 UE 的认证,跨域信任流程结束。

4.2 仿真验证结果

未采用跨域信任机制时,使 UE 首先在归属域 Domain A中注册,然后在拜访域 Domain B 中发起跨域认证请求。测试从发送 REGISTER 消息到认证成功时收到 200(OK)消息的响应时间 t_1。重复进行 30 次测试,可以得到时间 t_1 的一个统计值,如图 5 中圆圈所示。

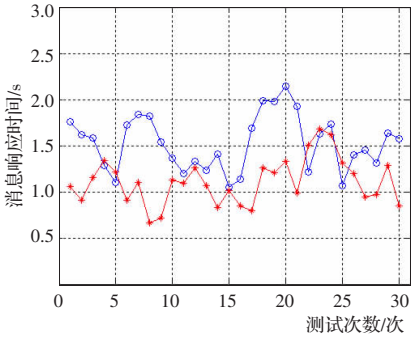

图 5 消息响应时间对比图

应用跨域信任机制,同样使用户 UE 首先在归属域 Domain A 中注册,然后在拜访域 Domain B 中发起跨域认证请求。测试从发送 REGISTER 消息到认证成功时收到 401 消息的响应时间 t_2。重复进行 30 次测试,可以得到时间 t_2 的一个统计值,如图 5 中星号所示。

(下转 122 页)