基于 AKA 的 IMS 接入认证机制

摘要：IP 多媒体子系统(IMS)作为 3G 网络的核心控制平台，其安全问题正面临着严峻的挑战。IMS 的接入认 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。基于认证和密钥协商(AKA)的 IMS 接入认证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。此机制基于“提问/回答”模式实现对用户的认证和会话密钥的分发，由携带 AKA 参数的 SIP 消息在用户设备(UE)和 IMS 网络认证实体之间进行交互，按照 AKA 机制进行传输和协商，从而实现用户和网络之间的双向认证，并协商出后续通信所需的安全性密钥对。

关键词：IP 多媒体子系统；认证和密钥协商；会话初始协议；接入认证机制

Abstract:IPMultimediaSubsystem(IMS) has been accepted as the core control platform of the 3G network. Its security problems are facing severe challenges now. The implementation of IMS access authentication mechanism, which is considered to be the first step of the whole IMS security plan, is the key to the IMS system security access. The Authentication and Key Agreement (AKA)-based IMS access authentication mechanism is developed by the Internet Engineering Task Force (IETF) organization and adopted by the 3GPP organization, and is widely used in 3G wireless network authentication mechanism. It is based on the “challenge/response” mode to achieve the bidirectional authentication and session key distribution. The Session Initiation Protocol (SIP) messages, which are carried with AKA parameters, are transmitted through the User Equipment (UE) and IMS core functional entities according to the AKA mechanism for consultation, thus realizing the two-way authentication between user and network, as well as the security key pair for later communications.

Keywords:IMS;AKA;SIP; access authentication mechanism

移动通信的 安全问题正越来越多地受到关注。2G 网络主要传输语音业务，采用的是单向的用户认证方案，即网络能够验证用户身份是否合法，而用户无法确认其所连接的网络 服务是否可靠。然而，3G 网络将会演变成一个覆盖全球的集有线、蜂窝和卫星通信于一体的全网，不仅支持传统的语音和数据业务，还支持交互式和分布式的业 务，如多媒体业务、电子商务、网上银行等。随着各种信息服务的蓬勃开展，各种机密性、敏感性、隐私性的数据的传输会大大增加，这对网络的安全性提出了更高 的要求。

IP 多媒体子系统(IMS)是 3G 网络的核心控制平台，具有基于会话初始协议(SIP)的全 IP 架构，IP 协议固有的缺陷和安全漏洞使 IMS 很容易遭受攻击。另外，IMS 对开放性接入的支持也对其网络安全提出挑战。如何保证用户安全地接入网络，保证 IMS 网络的可靠部署进而走向商用，成为了重中之重的问题。因此，研究 IMS 网络的安全接入认证机制有着十分重要的现实意义。

3GPP 已经成立了专门的工作组 SA WG3 负责 3G 网络安全方面的标准化工作，已经发布的 IMS 安全标准主要有：3GPP TS33.102: 3G 网络安全架构[1]、3GPP TS33.203: IMS 接入网络的安全机制[2]、3GPP TS33.210: IMS 核心网络的安全机制[3]。

1 IMS 的安全体系结构

作为相对独立的安全体系，IMS 要求所有的用户在使用 IMS 服务之前都必须进行鉴权(认证和授权)，协商建立安全的接入通道。用户和网络实体之间以及网络 实体之间的通信必须时刻处于安全保护之中。IMS 安全体系的整体思想是使用因特网协议安全(IPSec)的安全特性为 IMS 系统提供安全保护。IMS 安全 体系架构[2] 如图 1 所示，分为 5 个安全层面。

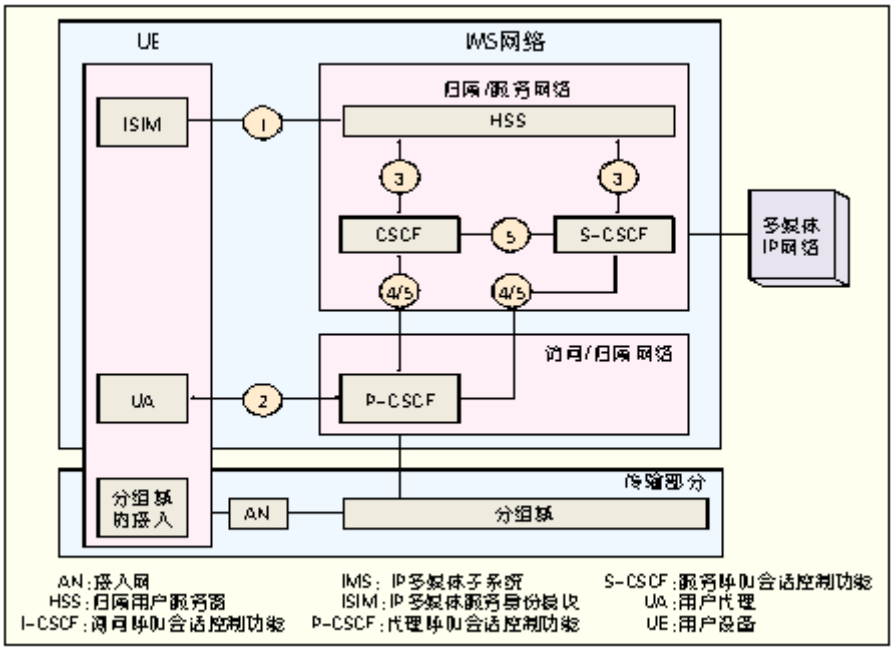


图1 IMS的安全体系架构图

IMS 安全架构的 5 个安全层面应用于 IMS 安全保护中不同的需求：

安全层面 1 提供用户和网络之间的双向身份认证。归属用户服务器(HSS)负责产生认证数据，并且委托服务呼叫会话控制功能(S-CSCF)执行用户认证的操作。认证基于由 IP 多媒体服务身份模块(ISIM)和 HSS 共享的密钥和算法。

安全层面 2 为用户设备(UE)和代理呼叫会话控制功能(P-CSCF)之间的通信提供安全关联，包括加密和完整性保护，并通过 IPSec 提供接入安全保护。

安全层面 3 提供网络域内呼叫会话控制功能(CSCF)和 HSS 之间的安全关联。

安全层面 4 为不同网络间的 CSCF 提供安全保护，适合于 P-CSCF 位于访问网络的情况。

安全层面 5 在网络内部的不同 CSCF 间提供安全保护，适合于 P-CSCF 位于归属网络的情况。

图 1 中的安全层面 1 和安全层面 2 属于 IMS 接入安全机制。IMS 的接入安全机制承担着两大任务：一是对接入用户的鉴权；二是在鉴权结束之后，在 UE 和 P-CSCF 之间建立 IPSec 安全关联(IPSec SA)，为后续 SIP 信令的交互提供安全保护。本文主要对基于认证和密钥协商(AKA)机制的 IMS 安全接入认证机制进行研究。

2 IMS 的接入安全机制

2.1IMSAKA 机制概述

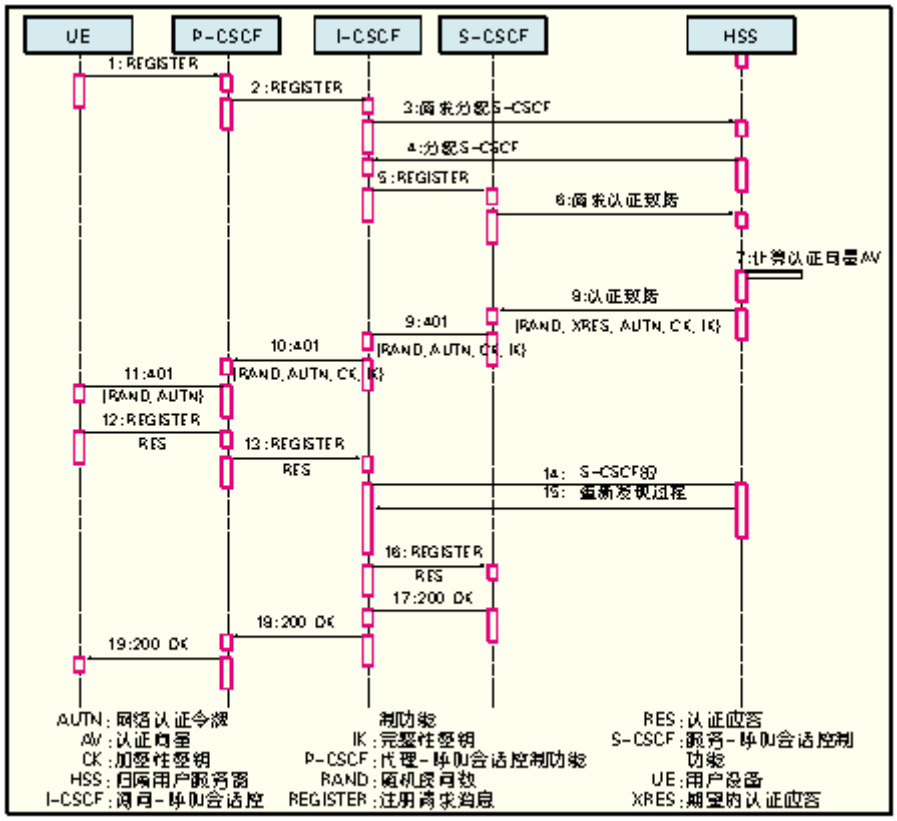
AKA 机制是由因特网工程任务组(IETF)制定、并被 3GPP 采用，广泛应用于 3G 无线网络的鉴权机制。IMS 的鉴权机制沿用了这种机制的原理和核心算法，故称之为 IMS AKA 机制[4]。

IMS AKA 机制是对 HTTP 摘要认证机制[5]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。由于 HSS 不与 UE 直接通信，而是由 S-CSCF 执行认证过程，因此它们不 会将真实的 Key 暴露给外界。

IMS AKA 机制使用“提问/回答”的模式实现用户和网络之间的双向认证，并通过协商产生的密码对(CK, IK)作为 IPSec SA 所需的密钥，为后续的通信提供安全保护。IMS AKA 机制是基于 SIP 协议来实现的。AKA 与 SIP 的结合在 IETF RFC3310 中定义。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。

2.2IMS 接入认证的实现

通过 IMS 注册过程实现基于 AKA 机制的 IMS 接入认证的具体流程[6] 如图 2 所示。



▲图2 基于AKA机制的IMS注册过程的消息序列图

(1) 用户发起注册请求

用户在使用IMS服务之前必须向IMS网络进行注册，注册的目的是将用户的私有身份(IMPI)与用户想要注册的公开身份(IMPU)绑定。每个用户只有一个IMPI，而可拥有多个IMPU，每个IMPU对应相应的服务配置。

UE在初始的注册请求SIP REGISTER消息中发送它的IMPI，该IMPI保存在ISIM应用中，只用于认证和注册过程。这个初始的REGISTER消息的主要头域和参数如图3所示。

```
REGISTER sip:home.mobile.biz SIP/2.0
    Authorization : Digest username="tobias_private@home.mobile.biz",
    realm=" home.mobile.biz",
    nonce="",
    uri=" sip:home.mobile.biz",
    response=""
    ......
```

▲图3 初始REGISTER消息

由于3GPP AKA被映射到HTTP摘要机制，因此认证方案的值被设置为“Digest”，而“response”和“nonce”域的值在初始注册请求消息中都设置 为空。P-CSCF将这个REGISTER消息转发给I-CSCF，I-CSCF联系HSS，以选择为用户提供服务的S-CSCF，然后将REGISTER请求消息转发给选定的S-CSCF。当S-CSCF收到REGISTER消息后，如果发现该用户还没有被认证，则S-CSCF向HSS发 送多媒体认证请求(MAR)消息[7]以请求认证数据。

(2) 计算认证向量

HSS收到MAR消息之后，运行AKA算法，为该用户计算认证向量(AV)，计算过程如下：HSS中的AuC运行AKA机制，首先产生最新的序列号SQN 和一个不可预测的随机提问数(RAND)。然后HSS将根据它与该UE之间的共享密钥Key，以及刚刚产生的SQN和RAND来计算其他的参数，其原理如 图4所示，AKA参数核心算法由3GPP TS35.206[8]提供。

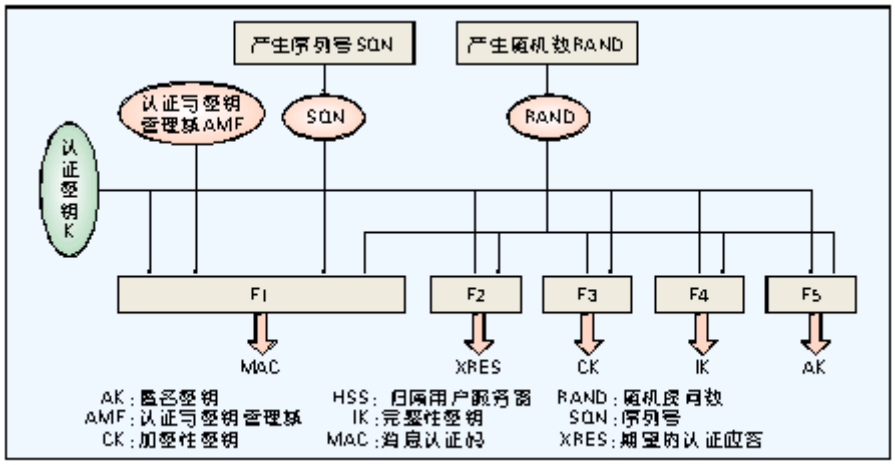


图4 HSS计算AV的原理图

其中，各个参数的计算公式如下(?在表示按位异或，|| 表示串接)：

计算消息认证码(MAC)：MAC=F1K(SQN|| RAND || AMF) ；

计算期望的认证应答(XRES)：XRES=F2K(RAND)；

计算保密性密钥(CK)：CK=F3K(RAND)；

计算完整性密钥(IK)：IK=F4K(RAND)；

匿名密钥(AK)：AK=F5K(RAND)；

网络认证令牌(AUTN)：AUTN=SQN?在AK|| AMF || MAC；

AV：AV=RAND||XRES||CK||IK||AUTN；

AK 用来隐藏 SQN，因为 SQN 可能会暴露用户的位置信息。如果不需要隐藏 SQN，那么 AK 被设置为 0。

(3) 网络向用户提问

HSS 通过上述的计算过程得到了一组 AV，其中每个 AV 都是一个五元组(RAND, XRES, AUTN, CK, IK)，该认证五元组并不包括 Key 和 SQN 本身。然后，HSS 将这些认证数据通过多媒体认证应答(MAA)消息发送给 S-CSCF。

S-CSCF 从 HSS 得到所需的安全相关的参数，即所谓的 AV。这些参数使得 S-CSCF 可以在不需要知道共享密钥 Key 和 SQN 的情况下就可以执行认证过程。

S-CSCF 将剔除 XRES 的 AV 包含在 401 Unauthorized 应答消息的 WWW-Authenticate 头域中向用户提问，401 应答主要的头域和字段如图 5 所示。

```
SIP/2.0 401 Unauthorized
WWW-Authenticate: Digest
realm="RoamingUsers@mobile.biz",
nonce="CjPk9mRqNuT25eRkajM09uTl9nM09uTl9nMzSOX2SPZz==",
algorithm=AKAv1-MD5,
ik="0123456789abcdeedcba9876543210",
ck="9876543210abcdeedcba0123456789"
.....
```

图5 401应答消息

其中，在 nonce 字段填入了将 RAND 和 AUTN 参数串接后进行 Base64 编码后的字符串。在 ik 和 ck 字段加入完整性密钥和保密性密钥。在 algorithm 字段放入值“AKAv1-MD5”，表示使用的是 3GPP AKA 认证机制。

当接收到 S-CSCF 返回的 401 应答消息后，P-CSCF 在将其发往 UE 之前，将其中的完整性密钥

IK 和保密性密钥 CK 保存下来，并将它们从 AV 中删除掉(IK，CK 这两个参数不能暴露，网络认证通过后，UE 的 ISIM 会根据收到的 AV，重新计算出来)。

(4) 用户认证网络身份

接收到网络返回的 401 应答消息后，UE 将接收到的 AKA 参数传递给 ISIM 应用，由 ISIM 模块运行 AKA 算法，执行以下工作：

首先基于 ISIM 中存储的共享密钥 Key 来校验网络认证令牌 AUTN，如果 AUTN 校验成功，网络就被认证通过(即确认认证数据是从归属网络中发来的)。 ISIM 计算 AKA 参数的过程如图 6 所示。UE 中的认证服务模块通过随机数 RAND 计算出匿名密钥 AK，然后使用匿名密钥 AK 来恢复序列号 SQN，接着通 过得到的序列号 SQN、RAND 和 ISIM 中保存的认证管理域 AMF 来计算期望的消息认证码 XMAC。将计算得到的期望的消息认证码 XMAC 和从网络认证 令牌 AUTN 中取得的由 HSS 计算的消息认证码 MAC 相比较。如果这两个参数一致，那么用户认证网络身份成功，接着进行下面的步骤；如果不一致，则用户认 证网络身份失败，UE 向网络发送不携带 response 字段的 REGISTER 消息，以此通知网络提问无效。

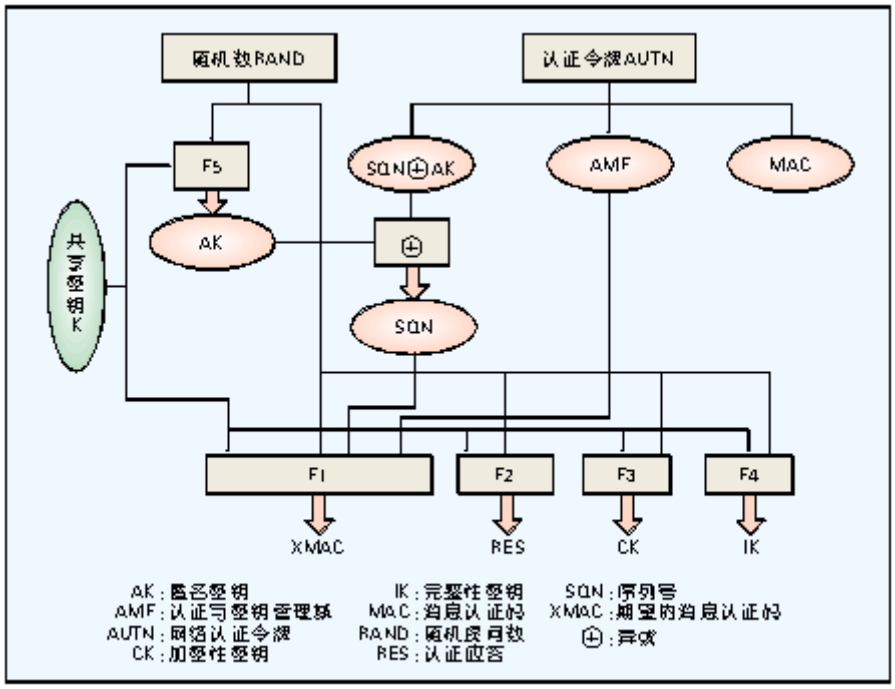


图6 ISIM计算AKA参数示意图

如果用户认证网络身份成功，UE 将接着检查序列号 SQN 是否在正确的范围之内(比较这次提问的序列号 SQN 是否比上次提问时使用的 SQNi 大)。如果 SQN 在正确的范围之内(即 SQN>SQNi，将 SQNi 更新为 SQN，并保存，以备下次使用)，UE 将会计算认证应答(RES)。如果 SQN 不大 于 SQNi，则认为本次提问的 AV 是不新鲜的，UE 与网络失同步，则 UE 计算重同步参数 AUTS，使用携带该重同步参数的 REGISTER 消息重新发起注 册请求。

如果 UE 确认 SQN 在正确的范围之内，则接着计算保密性密钥 CK 和完整性密钥 IK。

至此，UE 和 S-CSCF 都知道了密钥对 CK 和 IK，可以用于进行下面的数据加密。UE 将会保存 CK 和 IK，直到下一次成功执行了 AKA 过程。

最后，UE 在发往 S-CSCF 的第二个 REGISTER 请求中返回认证挑战应答 RES。

(5) 网络认证用户身份

P-CSCF 将这个携带认证应答的 REGISTER 消息转发给 I-CSCF，I-CSCF 重新查询 HSS 以发现 S-CSCF，然后将 REGISTER 消息 转发给 S-CSCF。当 S-CSCF 接收到 REGISTER 消息之后，进行解析并从认证头域 Authorization 中取出相应的参数：

如果 Authorization 头域中的 response 字段为空，再检查重同步参数字段 auts 是否为空：如果 AUTS 参数不为空，说明 UE 检查出了 SQN 同步失败，S-CSCF 使用这个重同步参数 AUTS 重

新向 HSS 请求认证数据，当下载认证数据成功后，再用新的认证向量重新向 UE 提问。如果 AUTS 参数也为空，说明 S-CSCF 的提问无效，S-CSCF 选择下一个认证向量，重新用 401 消息进行提问。如果 S-CSCF 用完了所有的认证向量 后，用户仍然无法确认网络身份，S-CSCF 认为本次认证失败，放弃本次认证过程，并发送 403Forbidden 消息通知用户。

如果 Authorization 头域中的 response 字段不为空，则 S-CSCF 取出其中的认证应答 RES 参数，并将其和保存在 S-CSCF 中的认证 应答 XRES 相比较。如果一致，S-CSCF 就认为用户回答提问正确，认证用户身份成功，允许用户接入网络，同时向 UE 回送 200OK 消息；如果不一 致，S-CSCF 就认为用户回答提问错误，认证用户身份失败，S-CSCF 不允许用户接入网络，那么 S-CSCF 应该发送 403Forbidden 应答消 息给 UE，通知认证失败，并且放弃本次认证过程。

3 IMSAKA 机制的安全性分析

3.1IMSAKA 机制实现的安全能力

从上述对基于 AKA 的 IMS 接入认证机制的原理和实现过程的分析可以看出，IMS AKA 机制实现了以下安全目标。

(1) 用户和网络之间的双向认证

S-CSCF 对 UE 的认证是通过 RES 实现的：如果 UE 合法，它能够正确地计算出 RES，且 RES 等于 XRES；UE 对 S-CSCF 的认证是通过 MAC 实 现的：UE 收到 S-CSCF 转发的 MAC 后，计算期望的消息认证码(XMAC)，如果 MAC 和 XMAC 一致，则认证成功。

(2) UE 和 P-CSCF 之间的密钥协商分配

P-CSCF 收到的来自 HSS 的 AV 中包含了保密性密钥(CKHSS)和完整性密钥(IKHSS)。合法的用户在收到正确的 RAND 之后，能正确地产生 CKUE 和 IKUE，且 CKHSS 等于 CKUE，IKHSS 等于 IKUE。CK 和 IK 用于其后的保密通信，而 CK 和 IK 并没有在空中接口中传输，确保了密 钥的安全性。

(3) UE 与 S-CSCF 间密钥的新鲜性

由于每次通信前的认证选择了不同的 AV，保证了每次通信采用的 CK 和 IK 都是由不同的 RAND 计算得到的。而每次使用的 MAC 是由不断递增的 SQN 作为输入变量之一，从而确保了密钥的新鲜性，有效地防止了重放攻击。

(4) 认证应答 RES 的安全

当 UE 计算出认证应答 RES 之后，使用名为“AKAv1-MD5”的摘要算法(实际上就是一个单向的哈希函数)来计算 RES 的摘要，然后将该摘要发送到 S-CSCF。S-CSCF 也使用同样的方法计算出期望的认证应答(XRES)的摘要值，通过比较这两个摘要值是否一致来认证用户的身份。通过这样的方法，即使攻击者窃听到 RES 的值，但是由于摘要算法是单向的哈希函数，根本无法反推出 RES 的值，因此不能危害网络安全。

由上面的分析，可以看到 IMS AKA 机制具有相当强大的安全能力来实现用户和服务网络之间的双向认证以及密钥协商，并且能够保证协商的保密性密钥和完整性密钥的新鲜性。因此，AKA 机制在 3G 网络的接入认证机制的实现中得到了相当广泛的应用。

3.2IMSAKA 机制的安全隐患及解决方案

在实际应用中，IMS AKA 机制的一些安全漏洞渐渐暴露出来。下面将对 IMS AKA 机制在注册过程中存在的一些安全隐患及现有的解决方案进行介绍。

(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，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。

SIP 协议对此进行了安全扩展：对 SIP 消息取摘要值，并且由 SIP 消息携带这个摘要值一同发送。在接收端对收到的 SIP 消息计算摘要值，如果和原摘要值 一致，说明这个 SIP 消息没有被修改过，受到了完整性保护。虽然即便是这样，还是不能杜绝攻击者窃听 SIP 消息，可是至少攻击者无法偷偷修改

消息内容，这 样对 SIP 消息的安全性能有一定程度的提高。

(2) 向 IMS 网络注册时，至少需要发送两次 REGISTER 请求，用户与网络之间的 SIP 交互过于繁琐，并且 SIP 消息携带的认证头域(如 Authorization 头域和 WWW-Authenticate 头域)带有众多 AKA 参数，导致 SIP 消息长度大幅增加。由于网络带宽的限制，传输延 迟将会十分明显，用户通过注册接入网络的耗时将会比较长，影响用户的使用感受。可以采用压缩 SIP 消息[9]的方法来在一定程度上改善服务质量，特别是在 无线环境下能大大缩短呼叫建立的时间。

(3) 在基于 AKA 的接入认证过程中，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。参考文献 [10]中提出的基于传输层安全协议(TLS)的 IMS 接入认证机制能对这一缺陷进行改进，但也仅仅是在理论阶段，还没有接受实际应用的考证。

4 结束语

IMS 作为下一代网络的发展方向，作为移动网络和固定网络的融合平台，为用户提供端到端的 IP 多媒体业务，这种基于 SIP 的全 IP 的开放网络特性给 IMS 网络的安全带来了极大的挑战。如何保证用户安全地接入网络是整个 IMS 安全方案实施的第一步，只有实现安全的接入认证机制，才能保证 IMS 网络的可靠部 署，进而走向商用。

IMS AKA 机制虽然被广泛地应用，但正如没有任何一种技术是 十全十美的道理一样，IMS AKA 机制本身也存在一些不太合理的地方，目前也有许多的组织和个人对 IMS AKA 机制提出了许多增强和完善的建议，但除了 SIP 的安全扩展机制以外，还没有哪一种改进方案被标准化采用。但无疑正是这种不断的推陈出新，使得网络的 安全性越来越高。IMS AKA 机制中仍有一些有待改进的开放性问题，希望在以后的研究工作中能对其进行改进：

(1) 通过使用序列号，用户可以保证认证信息(如 RAND 和 AUTN)是没有被攻击者或者是被服务网络使用过的。服务网络通过检验用户认证应答 RES 来判断用户 是否知道他和网络之间的共享密钥，以此来认证用户身份。然而，用户却仅仅只能检测出认证向量是否由归属网络产生，也就是说，用户不能判断收到的认证向量是 否是他请求服务的服务网络所申请的，因为任何服务网络都可以向归属网络请求认证向量。这种安全漏洞也会给攻击者提供机会。

(2) SQN 重同步的过程也并不很合理，因为只要 UE 检查出来 SQN 不在正常的范围之内，它就会发起重同步过程，而不关心 SQN 同步失败的真实原因。但是事实上 即使序列号不在正确的范围内，也并不代表 HSS 中的计数器 SQN_HN 发生了同步失败，有可能是恶意的攻击者重放提问引起的。UE 不关心真实的原因，不断 进行重同步过程，这必然会加大服务网络和归属网络之间的通信负荷，严重延迟用户接入网络的时间，甚至最后无法接入网络，严重影响用户的使用感受。但是这个 问题的改进可能要涉及到对 IMS AKA 机制的改进。本文主要研究安全接入认证机制，当实现用户的安全接入之后，如何建立 IPSec SC 的过程暂不涉及，将在以后的工作中进一步研究。