

一种安全增强型无线认证与密钥协商协议

许名松, 李谢华, 曹基宏, 高春鸣

(湖南大学计算机与通信学院, 长沙 410082)

摘要: 针对当前 3G 网络身份认证与密钥协商方案存在扩展性差、用户身份信息易泄露的问题, 提出一种基于无线公钥体制的安全增强型无线认证与密钥协商协议, 实现实体间的双向身份认证, 保护空中接口及有线通信链路, 防止用户和接入网络身份标识泄露。该方案支持数字签名, 可提供不可否认性业务。形式化方法验证分析表明, 该协议能够满足安全需求。

关键词: 无线公钥基础设施; 认证与密钥协商协议; 认证测试; 协议分析

Security-enhanced Wireless Authentication and Key Agreement Protocol

XU Ming-song, LI Xie-hua, CAO Ji-hong, GAO Chun-ming

(School of Computer and Communications, Hunan University, Changsha 410082, China)

【Abstract】 In view of some defects existing in current 3G authentication and key agreement protocols, a Security-enhanced Evolved Packet System-Authentication and Key Agreement(SE-EPS AKA) protocol is put forward based on Wireless Public Key Infrastructure(WPKI). The enhanced scheme realizes bidirectional authentication between the entities, protects the air interfaces and wired links, and resolves the problem of the user and access networks identity leakage. Meanwhile, the scheme can support digital signature to provide non-repudiation services. The formal verification result shows that the proposed protocol can satisfy the security requirements.

【Key words】 Wireless Public Key Infrastructure(WPKI); Authentication and Key Agreement(AKA) protocol; authentication test; protocol analysis
DOI: 10.3969/j.issn.1000-3428.2011.17.038

1 概述

由于无线接口的开放性以及用户移动的随机性, 移动通信系统的安全问题一直备受关注。而身份认证与密钥协商(Authentication and Key Agreement, AKA)协议作为系统的关键性安全机制之一, 自其被引入移动通信系统以来一直是研究的热点。随着移动通信系统的不断演进, 相继出现了 2G AKA、3G AKA、演进分组系统(Evolved Packet System, EPS) AKA^[1]。其中, 3G AKA 是第三代合作伙伴计划(Third Generation Partnership Project, 3GPP)在 2G 安全的基础上, 结合 3G 系统的新特性提出的安全保护机制, 它是对 2G AKA 的继承和发展。但由于处理机制及密钥体制方面的原因, 协议存在多方面的不足^[2], 不能满足下一代全 IP 化无线网络的安全需求。

针对 3G 系统存在和潜在的安全缺陷, 3GPP 着手研究适用于下一代全 IP 化移动通信系统的认证与密钥协商协议。其中, 最新发布系统架构演进(System Architecture Evolution, SAE)Release 8 标准中定义的 EPS AKA 就是其初步的研究成果。但文献[3]的研究表明, EPS AKA 协议仍然存在扩展性差、用户身份信息易泄露、网络实体间的有线链路缺乏必要保护等问题。

本文在研究 3G AKA 及其改进协议的基础上, 针对 EPS AKA 存在的一些安全漏洞提出了一种基于无线公钥体制的增强型演进分组系统认证与密钥协商协议——SE-EPS AKA (Security-enhanced Evolved Packet System-Authentication and Key Agreement), 该方案继承了现有 3G AKA 的认证体制, 在不改变现有移动通信系统体系结构的基础上, 通过引入公钥体制, 增强了系统的安全性和可扩展性, 简化了密钥的管理, 为移动通信实体提供了一个实用的安全可信交互环境。

2 EPS AKA 协议分析

EPS AKA 从 3G AKA 发展而来, 其沿用了以往协议“挑战/应答”的实现方式。协议在用户终端(User Equipment, UE)、移动性管理实体(Mobility Management Entity, MME)和本地用户服务器(Home Subscriber Server, HSS)三者相互成功认证的前提下, 完成了用户与服务网络(Service Network, SN)之间的会话密钥协商。协议的具体实现见文献[1]。

与传统的 3G AKA 相比, EPS AKA 能有效抵御伪基站攻击, 密钥安全强度高, 并且可以避免因序列号 SQN 伪同步失败^[4]而带来的系统开销。然而, EPS AKA 在一些重要方面仍然存在漏洞:

(1)当用户首次注册入网或 SN 无法从用户临时身份标识 S-TMSI(S-Temporary Mobile Subscriber Identity)恢复出用户永久身份标识 IMSI(International Mobile Subscriber Identity)时, SN 要求用户以明文形式传送 IMSI, 这样 IMSI 就存在泄漏的危险, 从而可能遭致用户定位、业务追踪及中间人攻击。

(2)网络实体之间的有线链路缺乏必要保护, 在 HSS、MME 之间以明文形式传输的认证向量 AV 易遭截获。

(3)协议仍然采用基于共享密钥 K 的方式实现 HSS 与 UE 间相互认证, 以生成会话密钥。而长期共享的密钥其安全性依赖于网络, 容易泄露。一旦共享密钥泄露, 本地通信就会受到安全威胁, 整个协议再无安全可言。

(4)协议忽视了对服务网络身份标识(Service Network

基金项目: 中央高校基本科研业务费专项基金资助项目

作者简介: 许名松(1984—), 男, 硕士, 主研方向: 无线通信, 移动通信安全; 李谢华, 博士; 曹基宏, 硕士; 高春鸣, 教授、博士

收稿日期: 2011-02-15 **E-mail:** xmssy@126.com

Identity, SNID)的保护。无论是在空中接口还是在有线链路上均存在 SNID 以明文形式传输的现象,攻击者很容易通过窃取合法 SNID 的方式主动发起伪基站、网络欺骗等攻击。

(5)协议采用的是单钥密码体制,密钥数量随着接入用户数目的增加快速增长,缺乏必要的可扩展性。同时,该体制不支持数字签名,不能提供不可否认性业务,很难满足下一代网络高可靠性和灵活性的安全需求。

3 SE-EPS AKA 协议

3.1 符号说明

UE: 用户终端;

MME: 移动性管理实体;

HSS: 本地用户服务器;

CA(Certification Agency): 证书管理机构,主要负责为网络实体 UE、MME、HSS 颁发、更新、验证、废除证书并实现对密钥的管理;

K : 会话根密钥,预先存在 UE 和网络运营商的 HSS 中;

PK_h, PK_m, PK_u : 分别为 UE、MME 和 HSS 的公钥;

SK_h, SK_m, SK_u : 分别为 UE、MME 和 HSS 的私钥;

f_3, f_4, s_{10} : 密钥生成函数;

$f_3K(m), f_4K(m), s_{10}K(m)$: 分别表示由 f_3 、 f_4 、 s_{10} 、密钥 K 及参数 m 生成密钥;

K_{ASME} : 中间密钥,用于衍生后继会话密钥;

K_{SASME} : MME 为 K_{ASME} 分配的唯一密钥标识,用于鉴别 K_{ASME} ;

$\{m\}_K$: 用密钥 K 对消息 m 进行加密运算;

$\{m\}_{sig}$: 对消息 m 进行签名;

\oplus : 按位异或运算;

\parallel : 消息的级联。

3.2 SE-EPS AKA 协议过程

在 WPKI 体制下,UE、MME 和 HSS 在通信之前首先通过 CA 获取会话过程中所需的数字证书,并从中得到公钥。数字证书的获取过程见文献[5]。

SE-EPS AKA 的具体过程如图 1 所示。

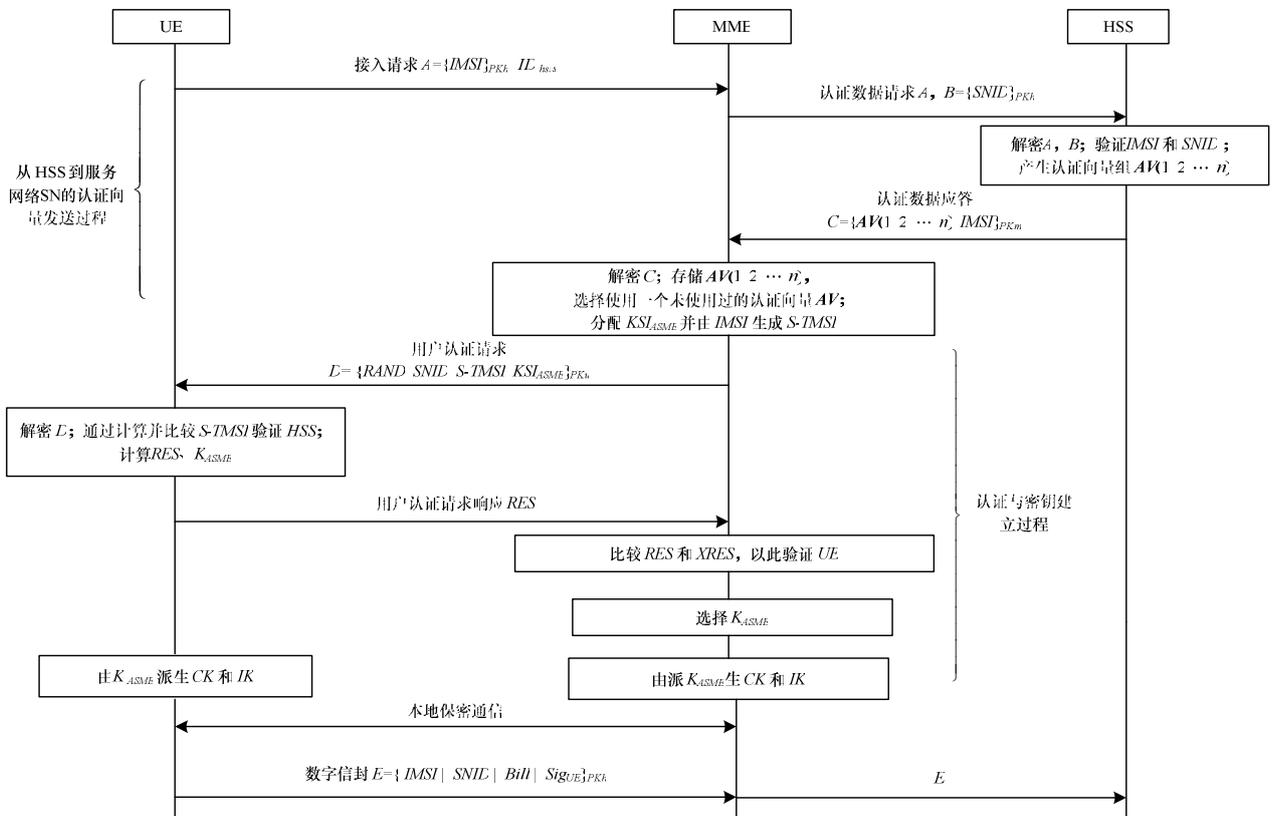


图 1 SE-EPS AKA 的认证与密钥协商过程

由图 1 可见,SE-EPS AKA 协议仍沿用现有 AKA 体制的认证流程。协议的详细描述如下:

(1) UE → MME: $A = \{IMSI\}_{PK_h} || ID_{hss}$

用户发起接入请求:首先,在 UE 中利用 HSS 的公钥 PK_h 加密 $IMSI$ 计算出 A ,然后,UE 将 A 以及用户归属服务器 HSS 的标识 ID_{hss} 一并包含在接入请求中发送给 MME。

(2) MME → HSS: $A, B = \{SNID\}_{PK_h}$

MME 接收到用户的接入请求后,利用 HSS 的公钥 PK_h 加密自身的网络身份标识 $SNID$,得到加密信息,并将 A 、 B 作为认证数据请求传送给 HSS。

(3) HSS → MME: $C = \{AV_1, AV_2, \dots, AV_n, IMSI\}_{PK_m}$

在接收到 MME 的认证数据请求后,HSS 首先利用自己

的私钥 SK_h 解密 A 、 B ,还原出 $IMSI$ 与 $SNID$;然后,根据 $IMSI$ 、 $SNID$ 分别查找在其数据库中维护的合法注册用户列表和授权服务网络列表,以实现 UE 及服务网络的验证。若验证通过,HSS 将产生随机数组 $RAND_1, RAND_2, \dots, RAND_n$,并由 $RAND(1, 2, \dots, n)$ 、 $SNID$ 、密钥生成函数 f_3, f_4, s_{10} 及根密钥 K 计算出认证向量组 AV_1, AV_2, \dots, AV_n 。图 2 给出 AV_1, AV_2, \dots, AV_n 的详细产生过程,根据图中的描述,SE-EPS AKA 协议认证向量的生成需要计算以下参数:

$$X = f_3K(RAND)$$

$$Y = f_4K(RAND)$$

$$K_{ASME} = s_{10}K(X, Y, SNID)$$

$$XRES = RAND \oplus SNID$$

$$AV = RAND \parallel SNID \parallel K_{ASME} \parallel XRES$$

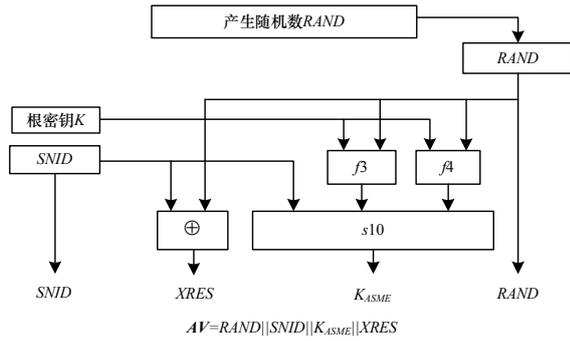


图2 SE-EPS AKA 中认证向量的产生过程

随后, HSS 利用 MME 的公钥 PK_m 对认证向量组 AV_1, AV_2, \dots, AV_n 以及用户的 $IMSI$ 加密, 产生加密信息 C , 并将 C 作为认证数据应答发送给 MME。

(4) MME \rightarrow UE:

$$D = \{RAND, SNID, KSI_{ASME}, S-TMSI\}_{PK_u}$$

MME 首先解密 C , 得到认证向量组 AV_1, AV_2, \dots, AV_n 及用户 $IMSI$, 并在数据库中存储认证向量组; 然后, 将从向量组选取未被使用过的一个认证向量 AV , 并抽取其中的随机数 $RAND$ 、服务网络身份标识 $SNID$; 接下来, 给认证向量中的中间密钥 K_{ASME} 分配唯一的密钥标识 KSI_{ASME} , 并利用 $IMSI$ 及 MME、UE 间约定的算法为用户生成一个在再次接入场景下使用的临时身份标识 ($S-TMSI$)。在完成一次认证与密钥协商之后, UE 与 MME 中都将存有 KSI_{ASME} 与 K_{ASME} 的对应关系。如果是再次接入, UE 与 SN 首先考虑根据这一标识验证 K_{ASME} , 从而无须发起认证过程就能实现机密通信^[1]; 最后, 将 $RAND$ 、 $S-TMSI$ 、 $SNID$ 用 UE 的公钥 PK_u 加密生成加密数据 D , 并把 D 包含在用户认证请求中发送给 UE。

(5) UE \rightarrow MME: RES

UE 在收到 MME 发送过来的用户认证请求后, 用自己的私钥解密 D , 还原出 $RAND$ 、 $S-TMSI$ 和 $SNID$, 然后, UE 计算 $S-TMSI$ 并与解密得到的 $S-TMSI$ 进行比较, 以此来对 HSS 的认证, 若两者不等, 表明 HSS 不合法, 则终止协议, 否则, UE 将计算 $RES = RAND \oplus SNID$ 和 $K_{ASME} = s10K(f3K(Rand), f3K(Rand), SNID)$ 并把 RES 作为对用户认证请求的响应发送给 MME。

(6) 将收到的 RES 与原认证向量中的 $XRES$ 进行比较, 若两者一致, 则该用户是合法的。然后, MME 和 UE 将以 K_{ASME} 作为中间密钥, 根据双方商定的密钥生成算法产生用以本地通信的加密密钥 (Cipher Key, CK) 和完整性密钥 (Integrity Key, IK), 否则, 终止整个过程。

(7) UE \rightarrow MME \rightarrow HSS:

$$E = \{\{IMSI \parallel SNID \parallel bill\}_{sig}\}_{PK_h}$$

MME 在自己的数据库中存储 $S-TMSI$ 与 $IMSI$ 、 AV_1 、 AV_2, \dots, AV_n 、 KSI_{ASME} 、 K_{ASME} 、 CK 、 IK 的对应关系。用户则在 UE 中存储 $S-TMSI$ 与 $IMSI$ 、 $SNID$ 、 KSI_{ASME} 、 K_{ASME} 、 CK 、 IK 的对应关系。在用户和服务网络完成业务交互后, 根据业务的需要, UE 还可以利用自己的私钥 SK_u 对用户身份标识 $IMSI$ 、服务网络号 $SNID$ 及业务计费信息 $bill$ 进行签名, 产生计费凭证 $\{IMSI \parallel SNID \parallel bill\}_{sig}$ 。同时, 为防止 $IMSI$ 、 $SNID$ 的泄漏, 再利用 HSS 的公钥 PK_h 对此计费凭证进行加密保护, 生成数字信封 E 。该信息经 MME 转发给 HSS, 可以作为 MME、UE 在场参与业务并产生相关计费关系的凭证。

4 SE-EPS AKA 协议的形式化分析

认证测试方法^[6]是目前身份认证协议验证方法中较完善的一种, 因此, 本文采用该方法对 SE-EPS AKA 协议进行安全性和保密性验证。

认证测试方法的初始定义如下:

UE 的串和轨迹 $UE[IMSI, SNID, ID_{hss}, A, D, RES]$ 定义为: $\langle +\{A, ID_{hss}\}, -\{D\}, +\{RES\} \rangle$ 。

MME 的串和轨迹 $MME[IMSI, SNID, ID_{hss}, A, B, C, D, RES]$ 定义为: $\langle -\{A, ID_{hss}\}, +\{A, B\}, -\{C\}, +\{D\}, -\{RES\} \rangle$ 。

HSS 的串和轨迹 $HSS[IMSI, SNID, ID_{hss}, A, B, C]$ 定义为: $\langle -\{A, B\}, +\{C\} \rangle$ 。

4.1 UE 对 MME 的验证

前提假设: 令 s 为 UE 串, K_P 为攻击者掌握的密钥集合, 且 $PK_u, PK_h \notin K_P$, $IMSI$ 由 s 唯一产生。

证明:

(1) 构造测试分量。发起者串 $s = UE[A, ID_{hss}, D, RES]$, $IMSI$ 唯一产生于结点 $\langle s, 1 \rangle$, 因此, $\{IMSI\}_{PK_u}$ 是 $IMSI$ 在 $\langle s, 1 \rangle$ 中的测试分量, 从图 1 可以得到, 由于 $S-TMSI$ 是由 $IMSI$ 产生的, 因此 $S-TMSI \subset IMSI$, $\langle s, 1 \rangle \Rightarrow^+ \langle s, 2 \rangle$ 是 $IMSI$ 在 $\{IMSI\}_{PK_u}$ 中的出测试。

(2) 认证测试规则 1^[6]。得到正常结点 m , $m' \in C$, $term(m) = \{IMSI\}_{PK_u}$, 并且 $m \Rightarrow^+ m'$ 是 $IMSI$ 的转换边。

(3) 结点 m 。由(2)的结果可得, m 为负结点。假设 m 为某 MME 串 s' 中的结点, $s' = MME[A', ID_{hss}, B', C', D', RES]$, $m = \langle s', 1 \rangle$, $term(\langle s', 1 \rangle) = \{IMSI\}_{PK_u}$ 。

(4) 串的内容。比较 $term(\langle s', 1 \rangle)$ 和 MME 串中的相应分量, 可以得到 $A = A'$, $ID_{hss} = ID'_{hss}$, $HSS = HSS'$ 。

(5) $SNID = SNID'$ 。使用认证测试方法的第 2 部分, 将 $t_1 = D = \{RAND, SNID, KSI_{ASME}, S-TMSI\}_{PK_u}$ 作为测试分量, 且 $PK_u^{-1} \notin K_P$ 。因此, 得到正常结点 m , m 为负, $term(m) = t_1$ 。

(6) 结点 m 。假设 m 为某个发起者 s'' 串中的结点, $m = \langle s'', 2 \rangle$, $sign(\langle s'', 2 \rangle) = -$, $term(\langle s'', 2 \rangle) = \{RAND, SNID, KSI_{ASME}, S-TMSI\}$ 。

(7) 串 s 和 s'' 的内容。由于 $IMSI$ 唯一产生于初始者串 s , 且 $PK_u \notin K_P$ 因此可得到 $s = s''$ 。由于 $-\{RAND, SNID, KSI_{ASME}, S-TMSI\}_{PK_u} = term(\langle s, 2 \rangle)$, 因此最终得到 $SNID = SNID'$ 。由此可见, UE 能够对 MME 的身份进行认证。

4.2 MME 对 HSS 的身份认证

前提假设: 令 s 为 MME 串, $PK_m^{-1}, PK_h^{-1} \notin K_P$, 且 $SNID$ 是由 s 唯一产生的。

证明:

(1) 构造测试分量。MME 串 $s = MME[A, ID_{hss}, B, C, D, RES]$, 由于 $SNID \in B$ 唯一产生于 $\langle s, 2 \rangle$, 因此 $B = \{SNID\}_{PK_u}$ 是 $SNID$ 在 $\langle s, 2 \rangle$ 中的测试分量, 从图 1 中可以看出: $\langle s, 2 \rangle \Rightarrow^+ \langle s, 3 \rangle$ 是 $SNID$ 的出测试。

(2) 认证测试规则 1^[6]。得到正常结点 m , $m' \in C$, $term(m) = \{SNID\}_{PK_u}$, 并且 $m \Rightarrow^+ m'$ 是 $SNID$ 的转换边。

(3) 结点 m 。由(2)的结果可得, 结点 m 为负结点, 因此, m 为某 HSS 串的结点, 假设该初始者串为 s' , $s' = HSS[IMSI', SNID', A, B, C, D, ID'_{hss}]$, $m = \langle s', 2 \rangle$, 则 $term(\langle s', 2 \rangle) = \{IMSI\}_{PK_u}, \{PK_u\}, ID_{hss}, \{SNID\}_{PK_u}$ 。

(4) 串的内容。通过比较 $term(\langle s', 2 \rangle)$ 和 HSS 串中的内容 (下转第 135 页)