第34卷 第20期 计 算 机 工 程 2008年10月
Vol.34 No.20 Computer Engineering October 2008
·安全技术· 文章编号：1000—3428(2008)20—0149—02 文献标识码：A 中图分类号：TP393.08

基于混合密码的增强型3G终端入网认证方案

刘 莹，陆松年，杨树堂
(上海交通大学现代通信技术研究所，上海 200240)

摘 要：针对3G入网认证中存在的安全漏洞，利用PKI的密钥验证协议管理方便的特点，提出适用于B3G环境下的安全分层管理体系结构。同时结合此体系，采用椭圆曲线算法将对称和非对称加密有机结合，提高了协议的安全性，防止了用户身份的泄漏。通过与Zheng Yu、Georgios Kambourakis等人提出的方案进行比较，证明了相较于前者该方案虽增加了1次哈希计算，却减少了3次对称加密，而相较于后者不仅没有给终端带来计算负担，还减少了6次以上空中接口通信。

关键词：PKI体系；用户身份标识；混合密码；密钥验证协议；3G入网认证

Enhanced Access Authentication Scheme in 3G Network Based on Hybrid Encryption

LIU Ying, LU Song-nian, YANG Shu-tang
(Modern Communication Technology Researching Institute, Shanghai Jiaotong University, Shanghai 200240)

【Abstract】 To solve security bugs of access authentication in 3G and take advantage of convenience of Authentication and Key Agreement(AKA) in PKI, a new certificate authority chain is introduced, which can well satisfy B3G hierarchical security. Based on this chain and elliptic curve cryptography, symmetric and asymmetric cryptography is properly combined which successfully prevents disclosure of user's identity. Through comparing with schemes suggested by Zheng Yu, Georgios Kambourakis, et al, it is proved that for the former, this scheme has reduced three computations of asymmetric cryptography although adding one Hash. And as to the latter, it has decreased more than six times of transmission in the air but does not bring computation burdens to terminal.

【Key words】 PKI system; International Mobile Subscriber Identification(IMSI); hybrid encryption; Authentication and Key Agreement(AKA); 3G access authentication

1 概述

1.1 安全漏洞

3G终端入网认证及其密钥分配协议中存在的安全漏洞如下：

(1)以明文的形式传输IMSI用户永久身份会出现的情况有：1)用户第一次注册入网或者在移动终端(MS)长时间没有入网；2)由于SGSN(Serving GPRS Supporting Node)的数据库工作不正常或因在切换过程中，不能从P-TMSI(Packet-Temporary Mobile Subscriber Identity)中获得相应的IMSI。如在切换过程中，(IMSI, P-TMSI)从一个SGSN传到另一个SGSN，而新的SGSN不能解析老的SGSN的IP地址[1]。在文献[2]中，采取秘密分享机制来防止泄漏IMSI，方法是在入网时提前计算PID_M(用户身份分割后的信息)以代替ID的传输，使ID信息的获取不仅通过终端而且网络端也必须参与。在以后的认证中，ID不会在传输中出现，但这意味着存储PID_M和N_M对应关系的HLR数据库必须永远不被破坏或工作正常。

(2)VLR, HLR之间消息传输缺乏保密性。在3G入网认证标准中，VLR和HLR之间采用明文传输，尽管两者之间用有线连接，但还是存在危险，尤其在IMSI没有受到保护的情况下。

(3)缺少MS以及HLR对VLR的认证，导致攻击者有可能假冒合法VLR，在用户传送IMSI时获取永久身份标识或进行中间人攻击。在3G中，MS $\xrightarrow{\text{IMSI}}$ VLR $\xrightarrow{\text{IMSI}}$ HLR。存在的危险：MS $\xrightarrow{\text{IMSI}}$ VLR' $\xrightarrow{\text{IMSI}}$ VLR $\xrightarrow{\text{IMSI}}$ HLR。

1.2 局限性

现有WPKI存在的局限性如下：

(1)移动终端获取自己和服务器的证书都必须通过无线信道向CA(Certificate Authority)索取，所以需额外占用有限的频谱资源。

(2)WPKI体系作为解决移动通信网安全的措施，体系中的CA与移动通信网中的鉴权HLR/AuC是独立的，造成资源浪费。

(3)由于有线网和无线网通信模式、设备存储空间以及计算能力不同，WPKI提供的数字证书和PKI也不同。Internet中数字证书一般采用X.509格式，而WPKI则使用其缩减版本，这导致在今后的异构网络中，证书转换不灵活，存在证书解析转换问题。

2 对现有PKI证书颁发体系的改进

为解决WPKI体系中的CA与移动通信网中的AuC(鉴权中心)独立而造成资源浪费的问题，将其合并，即移动网中的

基金项目：国家“863”计划基金资助项目“信息安全增值服务平台”(2005AA145110)

作者简介：刘 莹(1984－)，女，硕士研究生，主研方向：通信安全；陆松年，教授；杨树堂，副教授

收稿日期：2007-11-24 **E-mail：**snlu@sjtu.edu.cn

HLR/AuC 具有颁发、存储和吊销其下一级数字证书的能力，HLR 的数字证书由移动网络运营商颁发，运营商的数字证书由不同构网络共同信任的 CA 颁发。图 1 所示为整个证书链体系结构，除空中接口部分，证书传送都在有线环境下进行。

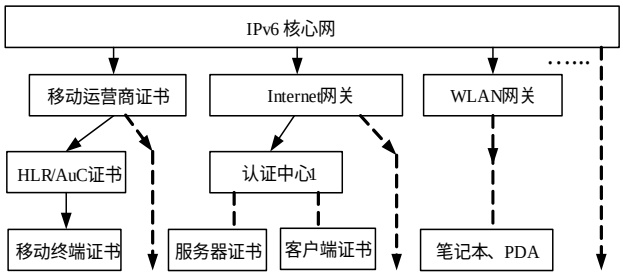

图 1　网络证书链

在图 1 中核心网下每一条支链代表每个异构网络的证书链，各网络由 IPv6 骨干网通过安全网关互连。根据移动 IPv6 技术，注册网络属于 home network，终端在陌生分支(foreign network)中移动时，证书可用于两网之间的相互认证或对敏感信息的保密。此外由于除无线网接入部分证书需无线传输外，其他都是有线传输，因此有线网全网建议统一使用 X.509 证书来简化证书解析认证过程。空中接口部分公钥的传输同文献[3]采用 PKBP(Public Key Broadcast Protocol)。

3　改进后的 3G 终端用户入网认证过程

3.1　初始化阶段

假设：安全椭圆曲线参数为$T=(p, a, b, G, n, h)$。其中，G为椭圆曲线基点。k_HG为Q_H，k_TG为Q_T，E为加密算法，SQN_H为HLR为每个用户设置的跟踪计数器，SQN_T为SIM卡中所存储的最高消息序列号。

(1)HLR/AuC存储其上一级CA发给它的公私钥对(k_H, k_HG)和其管辖范围内所有移动终端的数字证书。

用户数字证书的产生过程：用户到营业厅办理入网手续，首先移动终端选取一个 160 bit的随机数$k_T\in[1,n-1]$存入SIM卡中，作为MS的私钥。然后终端计算相应的公钥$k_TG((k_T, k_TG)$，不仅用于入网身份验证，还用于移动商务中终端身份证明)。营业厅通过安全通道将k_TG传给HLR，HLR制作包含有k_TG的用户证书并用自己的私钥k_H对证书签名，并存储用户证书。同时在用户的SIM卡内，存有一个与HLR/AuC共享的密钥K_c。由于在相同安全强度下，ECC比RSA具有节省存储空间的优点，且私钥选择非常方便，在无线领域大范围采用的可能性很大，因此手机可通过内置、外设或升级来具备计算ECC的能力。

(2)由于VLR和HLR之间通过有线连接，因此安全性比较高。加密速度是考虑的主要原因，采用共享密钥K_L，既达到对信息的加密，又达到HLR, VLR之间的互认证。

3.2　改进后的认证阶段

基于PKBP，HLR的公钥Q_H通过本小区和相邻小区基站的BCCH(广播控制信道)以联合形式发送。各BS不仅发送自己HLR的公钥，同时也发送其相邻BS的HLR的公钥。要入网的移动终端首先接收Q_H。以下是入网认证过程：

Message 1：$M\rightarrow V$: MS使用Q_H加密IMSI || SQN_T，并发送 E_{Q_H}(IMSI || SQN_T)，采用椭圆加密算法。

Message 2：$V\rightarrow H$: VLR用K_L加密 E_{Q_H}(IMSI || SQN_T)，向HLR/AuC发送 E_{K_L}(E_{Q_H}(IMSI, SQN_T))。

Message 3：$H\rightarrow V$: HLR解密 E_{K_L}(E_{Q_H}(IMSI, SQN_T)，得到IMSI, SQN_T，然后检查SQN_T是否在SQN_H的正确范围。 (1)若不在，则失败重发；(2)若在，则调整$SQN_H=SQN_T$。HLR 计算 $K_{HT}=H$(IMSI,K_c)，认证向量$\boldsymbol{AUTN}=E_{K_{HT}}$(Rand||$SQN_T$||$AMF$), $RES=H$(RAND, K_c), CK, IK。发送 E_{K_L}(RES|| CK|| IK|| $\boldsymbol{AUTN}$)||$Sign_H$ ($\boldsymbol{AUTH}$)。其中，CK是加密密钥；IK是完整性密钥；AMF是认证管理域；$Sign_H$ ($\boldsymbol{AUTH}$)是HLR对认证向量的ECC签名。

Message 4：$V\rightarrow M$: VLR解密 E_{K_L} (RES||CK||IK||$\boldsymbol{AUTH}$)，得到RES,CK,IK，将它们存起来，发送$Sign_H$ ($\boldsymbol{AUTH}$)|| $\boldsymbol{AUTH}$给MS。

Message 5：$M\rightarrow V$: MS验证$Sign_H$ ($\boldsymbol{AUTH}$)是否由HLR发送。(1)若不是，则失败；(2)若是，则完成对网络端验证。然后检查 SQN_T是否等于入网前的SQN'_T：(1)若不是，则同步失败，将失败消息传给MSC(Mobile Switching Centre)； (2)若是，则MS计算$K_{HT}=H$(IMSI, K_c)，解密$\boldsymbol{AUTH}$并发送$XRES=H$(RAND, K_c)。

Message 6：$V\rightarrow M$: VLR 对比 $XRES$ 和 RES，检查两者是否相等。(1)若是，则完成对终端的验证；(2)若否，则失败。

整个验证过程由于采用公钥密码体制进行加密，因此原 f5 和 f5* 产生匿名密钥的算法可以去掉。同时对网络端认证已采用HLR数字签名，可以减掉一个异或器和 f1, f1* 算法(这 4 个算法并没有被 3Gpp 具体规定，可由运营商和设备商协商解决，具有可行性)。

4　安全性分析

(1)用户私钥在本地产生。用户用于入网认证以及在后续阶段用于移动电子商务的私钥，由用户在自己的终端中产生并存在 SIM 卡内，用户上一级 CA 即 HLR 无法获取私钥，它的作用只是对用户的公钥进行签名，以证明公钥的合法性。

(2)保护了用户永久身份。IMSI 在整个传输过程中，都处于保密状态，只有 HLR 用自己的私钥才可解密出。

(3)终端能够对 VLR 身份进行认证，防止中间人攻击。考虑到以下几个因素：1)减少 HLR 和终端存储 VLR 证书需花费的空间；2)HLR 和 VLR 之间通过有线网进行连接，且属同一网络运营商管理，安全性较无线高。所以采用在 HLR 和 VLR 之间共享加密密钥，既确保了传输信息的秘密性，又增加了 HLR 对 VLR 之间的双向认证。

(4)防止了HLR遭受回放攻击。方案在终端向HLR传送信息时，增加了SQN_T，检查其是否在SQN_H正确范围内，并通过使$SQN_H=SQN_T$进行初步网络、终端同步调整。

(5)采用了PKBP，终端可通过存储一定时间段不同BS发布的相同HLR公钥信息，选取出现次数最大的数作为本小区内HLR的公钥，来增加抵御假冒HLR的可能性，理论基于现实中恶意BS比合法BS少得多[3]。

(6)对Rand进行了保护。3GPP标准Rand以明文形式传送，如果攻击者截获Rand和用户发送的$XRES$，而f2 又是公开的，则有可能采用某些方法破译共享密钥K_c。

(7)提供了全网用户身份唯一性。将移动商务中用户和服务提供者的公私钥对用于入网认证，节省了资源，同时也实现了统一安全问题。

从表 1 看，本方案相对于 3G 标准提供了更高的安全性，弥补了 3G 中存在的漏洞。并从表 2 分析得到，相较于文献[4]

(下转第 153 页)