第 34 卷 第 8 期 计 算 机 工 程 2008 年 4 月
Vol.34 No.8 Computer Engineering April 2008
·安全技术· 文章编号：1000—3428(2008)08—0198—02 文献标识码：A 中图分类号：TP393.08

UMTS 系统鉴权和密钥分配机制的改进

叶敦范，宁 涛
(中国地质大学机械与电子工程学院，武汉 430074)

摘 要：为防止用户的永久身份信息不被窃取，研究第三代移动通信系统的安全结构。通过对 UMTS 系统接入安全机制，即鉴权和密钥分配机制进行分析，提出一种终端用户安全鉴权的方案。利用 USIM 对鉴权随机参数 RAND 进行验证，如果验证失败则给出错误的鉴权结果，反之给出正确的鉴权结果。该方案能最大限度地保证用户的身份信息不被监听窃取，同时提高身份的机密性，且实施周期短。
关键词：鉴权；随机数 RAND；密钥；安全

Improvement for Authentication and Key Agreement Mechanism in UMTS System

YE Dun-fan, NING Tao
(School of Mechanical and Electronical Engineering, China University of Geosciences, Wuhan 430074)

【Abstract】 In order to prevent the permanent information of a user from being identified by a rogue, the 3G security architecture is researched. By analyzing the mechanism of access security of UMTS systems, especially authentication and key agreement, this paper finds a method for authentication. The main idea of the method is to verify the random parameter RAND for authentication by USIM. If the process is not successful, USIM will respond fault result parameter; otherwise will respond correct result parameter. This method can ensure the identification information not been listened easily and improve the level of confidentiality the furthest. The period of putting in practice for the method is short.
【Key words】 authentication; random parameter RAND; key; security

第三代移动通信系统的安全体系主要是为了防止通信过程中用户身份的泄露，保护无线传输业务数据不被窃听。为了满足第三代移动通信安全体系的要求，必须采取一定的实现机制，实现对用户身份的保密和通信过程中数据和信令的保护。

WCDMA作为第三代移动通信系统，比第二代移动通信系统具有更多的业务、更快的速率。因此，对第三代移动通信系统中的安全体系也提出了更高的要求，而其中的鉴权和密钥分配机制是实现安全通信的重要保证[1]。但是在鉴权和密钥分配机制中，由于网络在对用户终端进行鉴权的过程中，用到的随机参数RAND是没有限制的，这样对于不法分子通过伪造网络来窃取用户的身份信息是非常有利的。因此，对于通信的信息特别是用户的身份信息，必须提供更加严密的保护措施。

1 鉴权和密钥分配机制的分析

在第三代移动通信系统中，对移动终端用户的身份验证，网络通过UMTS鉴权算法对存放在USIM卡中的用户信息进行认证实现。UMTS系统进行身份验证的原理是鉴权和密钥分配机制。当USIM和UMTS网络运营商签约进行注册登记时，需要被分配一个移动用户号码(MSISDN)和一个移动用户身份识别号码(IMSI)，同时还要产生一个与IMSI对应的移动用户鉴权密钥K。鉴权算法和鉴权密钥K分别存放在网络端的鉴权中心AuC和终端用户的USIM中。鉴权和密钥分配机制主要完成终端用户和网络之间的相互鉴权和密钥分配，同时也完成用户和网络之间通过密钥K进行的相互鉴权，以及完成加密密钥和完整性保护密钥的分配[2]。鉴权和密钥分配过程主要包括 2 个过程，如图 1 所示。

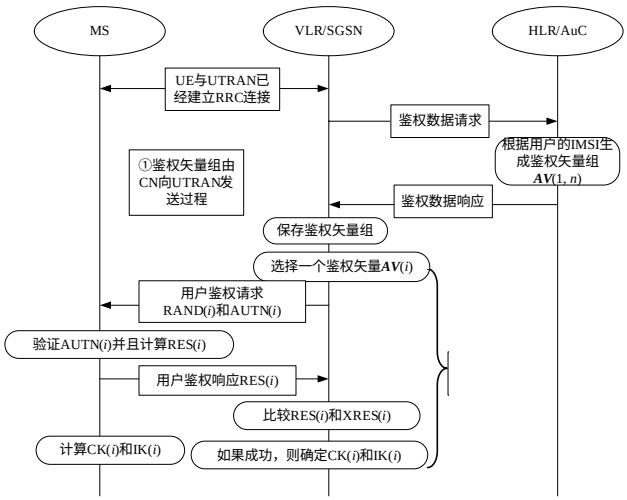

图 1 鉴权和密钥分配过程

(1)当终端用户已经和网络建立RRC连接后，网络根据要求对终端用户进行鉴权，那么SGSN/VLR就会向鉴权中心发送鉴权请求消息以获得鉴权需要的数据。鉴权中心通过一些算法，如$f0$(RAND产生函数)，$f1$(消息认证码编码函数)，$f2$(响应数产生函数)，$f3$(加密密钥CK产生函数)，$f4$(完整性保护密钥产生函数)和$f5$(匿名密钥AK产生函数)[3]等一些算法计算出一组鉴权矢量，然后鉴权中心将发送有序的n个鉴权矢量(鉴权 5 参数组)到SGSN/VLR。每个鉴权矢量包括：一个随机数

作者简介：叶敦范(1956－)，女，教授，主研方向：电子应用；宁 涛，硕士研究生
收稿日期：2007-08-12 **E-mail：**ndg242001@yahoo.com.cn

RAND、一个期望响应数XRES、一个加密密钥CK、一个完整性密钥IK和一个鉴权标识[1]。一个鉴权矢量适用于SGSN/VLR和USIM之间的一次鉴权和密钥分配。

(2)SGSN/VLR获得一组鉴权矢量组后，从中选择一个鉴权矢量，将其中的随机数RAND(*i*)和鉴权标识AUTN(*i*)通过鉴权请求发送给终端用户。终端用户在接收到网络的鉴权请求后，首先通过*f*1*(消息认证码编码函数)等函数验证鉴权标识AUTN(*i*)，以保证网络的鉴权参数是有效的，如果验证通过那么将计算的RES(*i*)发送给网络。网络接收到终端用户的响应数RES(*i*)后，通过和网络中存储的XRES(*i*)进行比较来判断鉴权是否成功。如果成功，网络将确定出用于该终端用户的CK(*i*)和IK(*i*)，同时终端用户也会根据相应的算法计算出CK(*i*)和IK(*i*)[1-2]。

从以上分析可以总结出一旦网络对用户的鉴权过程通过，那么该终端用户就被认为是合法用户。网络对终端用户鉴权所用的 5 参数组中的随机数RAND是最为重要的，但是网络对可用的随机参数没有进行限制。一些不法分子利用各种技术手段伪装成一个网络，通过对终端用户进行鉴权来试图破解认证机制，根据认证后的完整结果SRES, CK和IK推算出USIM卡的密钥K等一些重要隐私参数，从而可以冒充该合法用户。这样给合法用户和运营商都带来巨大的损失，同时也破坏了正常的通信秩序，可能对通信安全和社会安定造成不利的影响和危害[4]。而采用全面更新鉴权算法，对复杂网络结构的核心网来说，技术实现难度极高。因此，期望能有一种验证方法，在现有的安全机制基础上，采用简单而有效的措施弥补现有安全机制的缺陷。

2 改进方案

结合鉴权和密钥分配机制在鉴权中心 AuC 中对用于鉴权的参数 RAND 进行有条件的选择。如果终端用户接收到的随机参数 RAND 不符合条件，那么 USIM 不正确响应接收到的可能引起“攻击”的随机参数，从而扰乱整个解密算法，使其不能进行正确的解密，达到保护用户身份的目的。

图 2 是终端用户安全鉴权的方案。本方案技术难度小，非常简单易行。

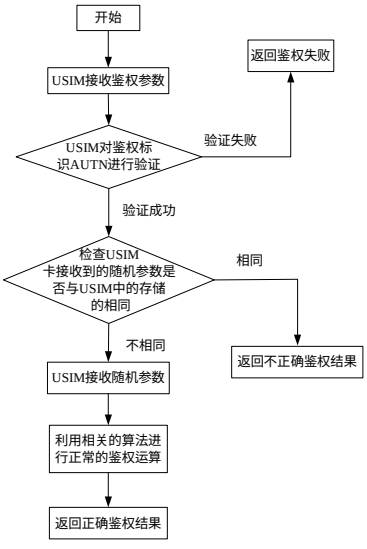

图 2 终端用户安全鉴权方案

本方案提出了一种终端用户安全鉴权方法，采用简单而有效的措施弥补现有鉴权和密钥分配机制的缺陷，提高了 USIM 卡抵抗攻击的能力。具体实施包括如下步骤：

步骤 1 终端用户通过控制信道接收网络的鉴权参数随机参数 RAND 和鉴权标识。

步骤 2 终端 USIM 卡对鉴权标识进行验证，如果验证失败，则直接给网络回复鉴权失败的结果；如果验证成功，那么执行步骤 3。

步骤 3 终端 USIM 卡比较接收到的随机参数 RAND 是否存在于 USIM 卡中保存的随机参数列中；如果存在，则给出错误的鉴权结果；如果不存在，则执行步骤 4。

步骤 4 终端 USIM 卡根据鉴权和密钥分配机制中的相关算法计算鉴权响应参数 RES、加密密钥 CK 和完整性保护密钥 IK，并向网络返回正确的鉴权结果。

本方案中对于存储在USIM中的有“攻击”可能的“随机数参数RAND”，既可以根据不同的密钥K确定不同的USIM卡存储的随机数参数列，也可以通过一定的算法对RAND参数进行限制[3]，这种算法保存在终端用户USIM和鉴权中心AuC中，其中可以通过密钥K来对不同的终端用户进行区别。这些选定的随机数参数将作为该终端用户USIM鉴权运算的例外，给出不正确的鉴权结果。

在进行鉴权过程中，对比移动通信网络发送的鉴权参数随机参数，如果符合终端 USIM 上所存储的“随机数参数”，则返回错误鉴权结果，以避免被攻击。这里错误的鉴权结果可以是给出随机参数，也可以是根据一种不可逆算法来给出错误结果。这样在破解者不了解有可能得出错误鉴权结果的情况下，破解几乎是不可能的；即使破解者知道有可能出现错误鉴权结果，由于他不清楚终端 USIM 卡中存储的随机数的算法，很难得出哪些是错误的鉴权结果，因此，破解者要窃取用户信息也是非常困难的。

在网络的鉴权中心 AuC 中也保存有终端 USIM 卡所存储的“随机数参数”列，用户进行正常的网络身份验证时，如果 AuC 生成的 RAND 在终端 USIM 卡所存储的“随机数参数”列中，那么鉴权中心 AuC 会要求重新产生随机数参数 RAND，保证传递给终端 USIM 卡的随机数参数 RAND 可以返回正确的鉴权加密结果，不会影响用户的正常登录。

3 结束语

本文主要研究了 UMTS 系统中的鉴权与密钥分配机制，对接入安全问题进行了分析和研究，针对存在的缺陷提出了一种终端用户安全鉴权的方案，并通过具体的实施措施对该方案进行了详细说明。提出的终端用户安全鉴权的方案能够有效地解决鉴权和密钥分配机制中的缺陷，也能很大程度上保证用户的正常使用，并且对移动网络透明，实施周期短。

参考文献

[1] 3GPP. 3GPP TS 33.102 3rd Generation Partnership Project. Technical Specification Group Services and System Aspects——3G Security, Security Architecture(Release 5)[Z/OL]. (2005-12-13). http://www. 3gpp.org.

[2] 3GPP. 3GPP TS 35.202 3rd Generation Partnership Project. Technical Specification Group Services and System Aspects——3G Security, Specification of the 3GPP Confidentiality and Integrity Algorithms — — Document 2: KASUMI Specification(Release 5)[Z/OL]. (2005-10-07). http://www.3gpp.org.

[3] 3GPP. 3GPP TS 33.105 3rd Generation Partnership Project. Technical Specification Group Services and System Aspects——3G Security, Cryptographic Algorithm Requirements(Release 4)[Z/OL]. (2004-06-15). http://www.3gpp.org.

[4] 桑 田, 黄连生, 张 磊. 改进的加密协议形式化验证模型和算法[J]. 清华大学学报: 自然科学版, 2002, 42(1): 48-51.