3G模拟网络终端接入测试研究

李春梅[1]　宫云战[2]
(北京邮电大学 1. 信息工程学院; 2. 计算机科学与技术学院, 北京　100876)

摘　要: 借助 CMU200 模拟 3G网络, Motorola 3G终端, Gemplus USIM Card 以及 GemXplore Admin 应用软件, 对 3G核心技术 ——鉴权做了详细分析, 对终端接入 3G模拟网络进行研究, 并成功接入 3G网络。

关键词: 3G; USIM Card; Key file; IMSI; 接入
中图分类号: TP311.5

引　言

随着移动用户对数据业务需求的急剧增加, 3G业务, 无论是终端对业务的支持情况, 还是与网络的适配性, 或者在不同设备之间的互连互通测试, 在3G网络部署前和部署后都是一个迫切的工作。而前提条件, 3G终端必须得以接入 3G网络。目前, 国内暂时还没有商用的 3G网络部署, 因此, 3G终端的测试, 不得不借助于模拟网络。

CMU200 是 R&S 公司第 3 代 RF 测试与测量平台, 可以提供处理 3G、2.5G以及包括模在内的前一代测试应用所必须的硬件和软件。在 3G手机生产方面, R&S 的手机综合测试仪 CMU200 已经被国际、国内众多手机厂商所采用。CMU200 支持包括 WCDMA/ HSDPA 在内的各种移动通信标准。

在 3G系统的核心, 通用移动通信系统(Universal Mobile Telecommunication System, UMTS)中的用户服务识别模块 USIM (Universal Subscriber Identity Module) 是实现通信服务最关键的因素。USIM 是用户获得 3G服务的关键, 是安全性的保障, 就如同 GSM 网络中的个人身份识别模同样重要的功能。它能安全地存储用户私人信息, 并执行加密算法。USIM 拥有与 SIM 卡相同的物理特性。它必须最少支持一个 USIM 卡上的网络应用。所不同的是, 在 3G系统里, 一张 USIM 卡可以拥有用户的一套或多套信息(就像一卡两号那样); 并且, 对于特定的卡片信息可以实施安全的空中管理。

收稿日期: 2007-05-15
第一作者: 女, 1978 年生, 硕士生
E-mail: e7156c@motorola.com

目前, Gemplus 公司提供了 Single Verification Capable UICC Card 和 Multiple Verification Capable UICC Card。Single Verification Capable UICC Card 只有一个帐号。Multiple Verification Capable UICC Card 有多个帐号, 不同帐号可以代表不同的运营商网络, 用户可以自由选择。本文将会对 2 种 USIM 卡的接入网络情况进行环境搭建和测试研究。

1　鉴权原理

在 3G网络的接入过程中, 采用双鉴权机制。就是说, 不仅网络端要对 USIM 进行鉴权, 终端 USIM 也会对网络进行鉴权。

相互鉴权的基本思想是服务网络通过盘问响应技术对用户识别符进行校验, 同时终端检验归属网络是否授权服务网络做这些事。鉴权的后一个过程相对 GSM 而言是 UMTS 的新特性, 通过它用户可以检验是否连接到合法的网络。

在 3G鉴权中, 鉴权五元组代替了 GSM 的三元组, 3G鉴权向量的 5 个参数分别是 RAND、期望响应(XRES)、加密密钥(CK)、完整性密钥(IK)、鉴权令牌(AUTN)。与 GSM 相比, 增加了 IK 和 AUTN 两个参数, 其中完整性密钥提供了接入链路信令数据的完整性保护, 鉴权令牌增强了用户对网络侧合法性的鉴权。UMTS 鉴权认证过程如图 1 所示。

(1) 鉴权中心 AuC 为每个用户生成基于序列号的鉴权向量组(RAND、XRES、CK、IK、AUTN), 并且按照序列号排序。

(2) 当鉴权中心收到 VLR/ SGSN 的认证请求后, 发送 n 个鉴权向量组给 VLR/ SGSN。在 VLR/ SGSN 中, 每个用户的 n 个认证向量组, 按照"先入先出"(FIFO)的规则发送给移动台, 用于鉴权认证。

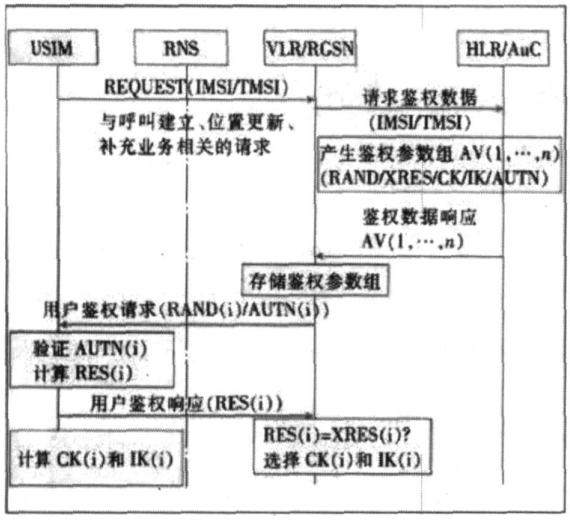

图 1 UMTS 鉴权认证过程

Fig. 1 UMTS authentication process

(3) VLR/SGSN 初始化的一个鉴权过程为选择一个鉴权向量组,发送其中的 RAND 和 AUTN 给用户。用户收到 RAND ‖AUTN 后,在 USIM 侧进行鉴权处理,处理的原理如图 2 所示。

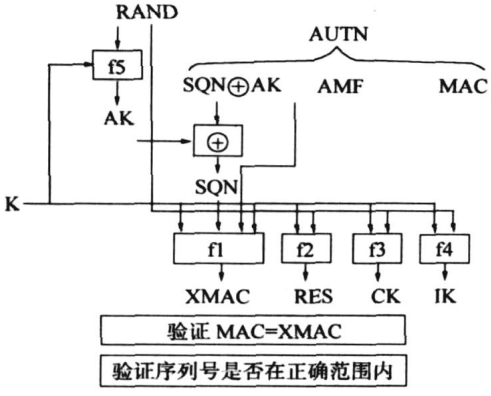

图 2 USIM 中的鉴权处理原理

Fig. 2 UMTS Authentication Process Principle

首先计算 AK,并从 AUTN 中将序列号恢复出来,SQN = (SQN ⊕AK) ⊕AK; USIM 计算出 XMAC,将它与 AUTN 中的 MAC 值进行比较。如果不同,用户发送一个"用户认证拒绝"信息给 VLR/SGSN,放弃该鉴权过程。在这种情况下,VLR/SGSN 向 HLR 发起一个"鉴权失败报告"过程,然后由 VLR/SGSN 决定是否重新向用户发起一个鉴权认证过程。

同时,用户还要验证接收到的序列号 SQN 是否在有效的范围内,若不在,MS 向 VLR 发送同步失败消息,并放弃该过程。

如果 XMAC 和 SQN 的验证都通过,那么 USIM 计算出 RES,发送给 VLR/SGSN,比较 RES 是否等于 XRES,如果相等,网络就认证了用户的身份。

最后,用户计算出 CK 和 IK。

所以,达到 USIM 的密钥和 CMU200 的 Security Code 一致,成为成功接入 3G 模拟网络的关键。

2 测试方案

对于 Single Verification Capable UICC Card,只有一个应用(或账号),所有对于卡的参数要求都可以在这个唯一的应用中实现。对于 Multiple Verification Capable UICC Card,根据 3gpp 规范规定,最多有 8 个应用,所有对于卡的参数要求都应该在所选定的应用中实现。以下的测试方案,都默认卡的具体应用已经确认。

方案一

获得 USIM 卡的密钥,修改 CMU200 网络端密钥与之保持一致。

在 CMU200 的 Network 设置中,密钥和 IMSI 都是可以获取和修改的。所以,如果一张 USIM 的密钥和 IMSI 是已知的,那么可以直接修改 CMU200 的网络配置,使之与 USIM 的信息保持一致。

因此,如果可能的话,可以定制特定密钥和 IMSI 的 USIM 卡,使之与 CMU200 保持一致。这样可以避免由于不正当操作对 USIM 产生破坏性损伤。或者是要求 USIM 的制造商提供卡的密钥和 IMSI,是 CMU200 的对应参数与之保持一致。这是目前各大手机制造商普遍采用的方法。

在这里,可以得知 USIM 卡的密钥和 IMSI,于是在 CMU200 的网络设置中,设置了 Secret Key Part 1 和 Secret Key Part 2,使之加起来为:00 01 02 03 04 05 06 07 08 09 0A 0B 0C 0D 0E 0F(这个 Code 是一个任意的 32 位 Code),与得到的 USIM 的密钥保持了一致,如图 3 所示。

同时,IMSI(International Mobile Subscriber Identity)也需要保持号段一致。IMSI 由三部分组成,即:MCC(Mobile Country Code)、MNC(Mobile Network Code)和 MSIN(Mobile Subscriber Id Number)。在这里,本文将 MCC 定义为 001,MNC 定义为 01,MSIN 定义为 0123456789(这个 15 位号段也是任意制定的),与 CMU200 网络端保持一致。

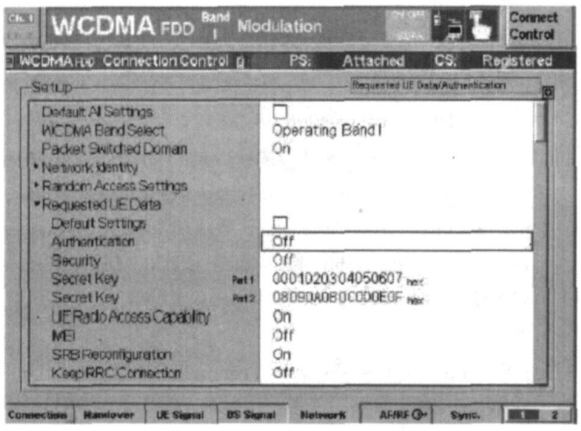

图 3　CMU200 密钥修改

Fig. 3　CMU200 secret key value update

对于射频要求, 如果是采用天线耦合,考虑到天线耦合的信号衰减比较大,需要在射频设置中给所采用的射频端口补偿 10 个 DB 的衰减值;如果采用插入式天线,则只需要在射频设置中给所采用的射频端口补偿 1～2 个 DB 的衰减值。在这里,本文采用了天线耦合,给出了 10 个 DB 的衰减值。

对于频带要求,目前所有的 9 个频段,CMU200 都可以支持。本文选用了 WCDMA BAND Ⅰ2100 频段,同时,3G 终端也必须保持频段一致。

环境搭建成功后,测试条件准备就绪,将手机终端置于耦合天线信号覆盖范围之内。可在手机 UI 上观察到,起机完成后将会注册到 CMU200 的模拟 3G 网络。这种方法是目前各大手机制造商普遍采用的方法,简单直接,可操作性强。

然而,这种方法虽然直接简单,但是,却是有很大的局限性的。对于手机终端来说,卡的兼容性也在手机质量的测试要求之内。根据卡的不同分类规则,手机卡的种类繁多。所以,如果有一种方法能够将卡的密钥修改,就可以解决手机对不同卡的兼容性测试问题。

方案二

修改 USIM 卡的密钥,与 CMU200 的网络 Security Code 保持一致。

如果能够获取 USIM 卡的密钥,就可以在 CMU200 的网络设置中将 Security Code 设置成已获得的 USIM 卡密钥。但是,卡制造商出于安全性的考虑,USIM 卡的密钥都是不可获取的,因为一旦卡的密钥被获知,这张卡就可以被完全复制。然而,我们可以通过获得 USIM 卡密钥的修改权,把需要注册到 3G 网络的 USIM 卡的密钥修改为我们需要的密钥,同时,设置 CMU200 网络端 Security Code,使两者保持一致。

如何修改 USIM 的密钥呢? Gemplus 公司提供的 GemXplore Admin 和 USIM CardReader 可以解决这个问题。当然,即使拥有 USIM Card Reader 的硬件和 GemXplore Admin 的应用软件,一般情况下,密钥也是不可修改的。唯一的途径是,可以通过修改相应的 Arr 文件,获得修改权限,从而把 USIM 卡的密钥修改成 CMU200 的密钥,获得鉴权的成功,从而接入 3G 模拟网络。

所以,首先要把密钥的访问和修改权限重新定义。根据 3gpp 规范,密钥是由 3F00 的 MF 目录下的 0001 文件定义的。读取 0001 文件的 EF information,可获知对应 Arr ID 的 Recorder Number SE # 01 的第 2 个配置文件定义了密钥的访问和修改权限。鉴于卡的安全性考虑,最好将密钥访问修改权限修改成 ADM1 或者 ADM4 定义,这是因为这两个保密参数拥有比 PIN 更高的保密度。当 ADM1 或者 ADM4 验证通过后,就获得了密钥修改权限。值得注意的是,算法 Algorithm 也要保持一致。这里是 DUMMY XOR 算法 Key Value 参照 CMU200 网络设置中的 Security Code 修改为:00 01 02 03 04 05 06 07 08 09 0A 0B 0C 0D 0E 0F(这个 Code 是一个任意的 32 位 Code),与 CMU200 网络端保持了密钥一致。

与方案一中一样,IMSI 也需要保持号段一致。在这里,本文将 MCC 定义为 001,MNC 定义为 01,MSIN 定义为 0123456789(这个 15 位号段也是任意制定的),与 CMU200 网络端保持一致。

同样,对于射频要求,如果是采用天线耦合,考虑到天线耦合的信号衰减比较大,需要在射频设置中给所采用的射频端口补偿 10 个 DB 的衰减值;如果采用插入式天线,则只需要在射频设置中给所采用的射频端口补偿 1～2 个 DB 的衰减值。在这里,本文采用了插入式天线,给出了 1 个 DB 的衰减值。

对于频带要求,目前所有的 9 个频段,CMU200 都可以支持。本文选用了 WCDMA BAND Ⅰ2100 频段,同时,3G 终端也必须保持频段一致。

值得注意的一点是 WCDMA 的上行和下行是分开的,所以对于插入式天线,必须同时分别接入上行和下行天线。

环境搭建成功后,测试条件准备就绪。将上行天线和下行天线分别插入测试终端的 2 个射频端

口。同样可以在手机 UI 上观察到,起机完成后将会注册到 CMU200 的模拟 3G 网络。

上面 2 种测试方案,都是借助仪器提出的黑盒测试方法。此外,还有一种是白盒测试方法,也可以在一定程度上对终端接入网络进行测试。那就是模拟底层消息,发出一个已经搜索到可注册网络的消息,应用层对这个消息进行处理,发起注册,可以在程序中检测注册结果。

3 结束语

3G模拟网络接入的关键,在于成功鉴权。鉴权的关键,就是取得模拟网络端和 3G 终端的密钥一致。有 2 种方案可以实现这个条件。第一种方案是直接通过卡商获取 USIM 卡的密钥,在 CMU200 网络设置中取得密钥一致;第二种方案是在 USIM 上修改卡的密钥,与 CMU200 模拟网络端取得一致。

参考文献:

[1] 2G与3G移动网络接入的安全性分析[OL]. http://www.chinaunicom.com. 2007-04.

[2] ETSI TS 102 223V6.8.0:Technical Specification Smart cards; Card Application Toolkit (CAT) (Release 6) [CP]. 2005-05.

[3] ETSI TS 100 977 V8.3.0: Technical Specification Digital cellular telecommunications system (Phase 2+); Specification of the Subscriber Identity Module-Mobile Equipment (SIM-ME) interface (GSM 11.11 version 8.3.0 Release 1999) [CP]. 2005-08.

[4] ETSI TS 101 267 V8.3.0:Technical Specification Digital cellular telecommunications system (Phase 2+); Specification of the SIM Application Toolkit for the Subscriber Identity Module-Mobile Equipment (SIM-ME) interface (GSM 11.14 version 8.3.0 Release 1999) [CP]. 2006-06.

[5] ETSI TS 131 124 V6.5.0:Technical Specification Universal Mobile Telecommunications System (UMTS); Mobile Equipment (ME) conformance test specification; Universal Subscriber Interface Module Application Toolkit (USAT) conformance test specification (3GPP TS 31.124 version 6.5.0 Release 6) [CP]. 2006-06.

[6] ETSI TS 131 124 V6.6.0:Technical Specification Universal Mobile Telecommunications System (UMTS); Mobile Equipment (ME) conformance test specification; Universal Subscriber Interface Module Application Toolkit (USAT) conformance test specification (3GPP TS 31.124 version 6.6.0 Release 6) [CP]. 2006-09.

[7] How do UMTS, UICC, USIM and USAT-(I) fit together? [OL] http://www.imcorporation.com/pdf/whitepaper_UMTS_USIM_UICC.pdf[CP]. 2007.

Study of 3G phone register based on simulated network test

LI ChunMei[1], GONG YunZhan[2]

(1. College of Information Engineering; 2. College of Computer Science and Technology, Beijing University of Posts and Telecommunications, Beijing 100876, China)

Abstract: This paper recur to CMU200 simulated 3G network, Motorola 3G phone, Gemplus, USIM card and GemXplore Admin application software, Analyze 3G's core technique-Authentication and study for phone registering on 3G simulated network. Finally, the phone registered on the network.

Key words: 3G; USIM card; key file; IMSI; register