SIM卡复制盗用新变种的剖析与防范

余岳群　管纯辉
中国联通湖南分公司　长沙　410001

1 前言

GSM系统有加密鉴权功能，近些年GSM部分加密算法遭到破解，导致SIM卡很容易被复制，给GSM网络用户和运营商带来了很大的危害，不但造成了经济损失，也给个人隐私、商业机密增加很多不确定因素。虽然GSM协会和运营商采取了一系列措施，但巨大的利益驱动仍使SIM卡复制方法不断改进。

2 SIM卡复制新变种

通过用户投诉并结合话单，近期笔者发现多起同一个用户号码在同一时间内短信嵌套的话单，凭以往经验，基本认定这是一种新的SIM卡复制盗用技术。

以前SIM卡复制后，在同一时间内只有一张SIM卡能正常使用，不能多张同时使用。这种新的SIM卡复制盗用技术是某些人利用非法的手段复制SIM卡后，造成多张卡有同一个IMSI，然后将多张卡分布到不同省份的不同交换机下，再利用某种多频率设备进行位置更新请求（每秒进行好几次，正常情况下是几秒进行一次）。正因为多张卡在不同的地方多次进行这样的位置更新，最终导致同一用户在多个MSC/VLR下登录，由于HLR中记录了其中一个VLR地址，而HLR中仅能记录一个VLR地址信息，这样会导致HLR仅能控制数据库中登录的VLR的SIM卡，而有该用户数据的其他VLR并没有在HLR中登记，所以这些卡不受HLR控制，只要被复制的SIM卡用户不进行跨MSC位置更新，就不会受HLR控制，除被叫外这些SIM卡还可以进行主叫和短信发送。最后造成用户恶意欠费后，不能被正常停机，运营商流失大量话费，且这些盗用的SIM卡往往是从事非法活动，引起社会安全隐患等系列问题。

这种新的SIM卡复制盗用技术非常难以被主动发现并采取有效的预防措施。因为在发现用户欠费以后只能对HLR中登记的SIM卡进行停机处理，而其他的卡照样可以进行主叫与短信发送，却不知用户到底在哪登录，只能分析停机以后产生的短信或主叫话单才能够知道用户还在哪些MSC上使用。再采取手段时高额的话费已经产生，恶劣影响也已造成，而这时不法分子又会复制另外一批SIM卡登录在其他城市的MSC上。

3 问题剖析

这种新的SIM卡复制盗用技术到底有何不同呢？我们可以通过移动用户的位置更新流程解密这种新的SIM卡复制盗用技术。在一次正常的位置更新过程中，当新VLR向HLR发出Update Location请求消息后，HLR会给原VLR发MAP Cancel Location消息，删除原VLR中的用户信息；得到原VLR的MAP Cancel Location ACK删除确定消息后，再向新VLR插入用户数据，完成位置更新过程。当一段时间内有多个新MSC/VLR频繁向该HLR发起同一IMSI的位置更新请求时，情况就变得非常复杂。

以两个MSC/VLR同时发起位置更新为例。当复制卡在两个VLR下进行位置更新，且两次位置更新时间接近时，使得HLR在VLR1刚发起位置更新请求时就发送了对同一用户的Cancel Location，而此时MSC/VLR在还没有开始Insert Subscriber Data流程（也就是VLR中还没有用户数据）的情况下，就收到Cancel Location。按照GSM规范，这种情况下应直接回送Cancel Location ACK。HLR发送Cancel Location给VLR1并记录VLR2的地址后（此时VLR1中用户信息已经被删除），继续进行VLR1和VLR2的位置更新流程，导致用户数据在两个VLR下同时登录（VLR1和VLR2中用户信息同时存在）。HLR中只能记录VLR2的登录消息，也就只能控制VLR2中的SIM卡，登录在VLR1的SIM卡则可以不受控制地进行恶意呼叫等行为。

位置更新分为首次开机时的位置更新、周期性位置更新、用户更变VLR时的位置更新3种。用户在同一位置不停发送短信或作为主叫时不满足上述3种位置更新中的任何一种，因此该SIM卡在该MSC/VLR下不会触发位置更新的操作，可以一直继续恶意呼叫行为，而HLR则一直不能控制该SIM卡，只有被发现后人为从VLR中清除该用户才可以中断恶意呼叫行为。

4 防范措施

从技术角度上分析，不法分子钻了GSM规范的空子，该问题并非HLR或MSC/VLR任何一方的软件缺陷导致，因此无论是在HLR侧改进还是在VLR侧改进，或者两侧同时改进，均可以解决问题，但解决复制卡频繁位置更新引发的多卡同时登录问题的关键是HLR具备串行处理功能，保证同一个用户在HLR中的位置更新处理流程串行化，使HLR或VLR增加“在位置更新期间发生Cancel Location，终止后续位置更新流程”这样一个处理机制。如果仅在MSC/VLR侧解决将无法杜绝此类问题的发生，因此在HLR侧完善位置更新机制是首选解决方案。

如对本文内容有任何观点或评论，请发E-mail至editor@ttm.com.cn。

红帽推出企业虚拟化2.2版本产品

作为集成企业级服务器和桌面虚拟化的进一步举措，红帽公司正式推出企业虚拟化2.2版本产品。除了包含第一版的红帽企业虚拟化桌面版，2.2版还包括新的可扩展性功能和迁移工具，以扩展解决方案的性能和安全性。

红帽企业虚拟化2.1版本是在2009年11月发布的，主要是红帽企业虚拟化服务器版。红帽企业虚拟化是红帽企业Linux和微软Windows（通过了微软SVVP认证）虚拟化以及云计算环境的理想基础，得到许多客户的认可。红帽企业虚拟化2.2能够托管和管理微软Windows和Linux虚拟机，为客户提供可以管理服务器和桌面虚拟化部署的统一基础架构。在2.2版升级中推出的红帽企业虚拟化桌面版使客户可以部署托管虚拟桌面配置。

红帽企业虚拟化2.2版本具有先进的可扩展性，每虚拟机可支持多达16个虚拟CPU和256 GB内存。此外，新版本通过一个V2V工具提供虚拟机转换能力，这个工具可以完成在红帽企业虚拟化中使用的VMware或Xen虚拟机的自动转换。为了进一步简化虚拟机映像在环境之间的迁移，红帽企业虚拟化2.2还包含利用开放虚拟化格式导入导出虚拟机映像和模板的能力。

HUBER+SUHNER推出最优等的浮动式同轴连接器

HUBER+SUHNE（灏讯中国）针对目前无线通信设备变得越来越小巧紧凑，板对板、板对模块和模块对模块之间的连接需求，推出一款新型的板对板连接器MBX，让众多的厂商找到了应对小型化和集成化的方法。

MBX具有可靠的电性能和机械性能，在小型板对板同轴连接器中拥有250 W的功率容量（在2.4 GHz室温环境下），板与板之间轴向容差补偿能力为±1.2 mm。板与板连接或板与模块连接的独特设计不会对连接器中零件产生压力，不会给焊点带来压力，最小的板与板的距离是13 mm，轴向的浮动能力是±1.2 mm，同时可以对轴向和径向的机械公差做弥补，盲插连接、优异的射频性能和出色的功率容量是该产品的显著特点。MBX作为灏讯板对板同轴连接器系列中的一个新成员，低成本、小型化、可靠连接、高功率容量等特点满足了更多用户的需求，该产品突破了多项技术瓶颈，完善并延续了MMBX在过去几年中成功的市场表现并直接受益于最终用户。