SECURITY ASSURED COMMNUNICATIONS

移动通信安全技术与产品

---------安全的 PDA 通信

摘要：随着*现代通信*与*计算机科学技术*的突飞猛进，针对现代通信的监听手段已经发展到了前所未有的成熟阶段。不但监听成功率大幅提高，效果突出，而且成本日趋低廉！！北京微点科技有限公司现提供一款移动通信安全技术产品**安全的 PDA 产品**，它基于*可配路单片系统硬件平台*与*安全操作系统*，支持 *GSM/GPRS 三频（900MHz，1800MHz，1900MHz）无线移动网络接入*以及 *2.4GHz 宽带无线局域网络（WiFi802.11b/g）接入*，实现端到端的、高强度、全数字化加密的**移动语音、短信息**与**数据通讯**，完备保护个人隐私、商业秘密的移动通信安全。

关键词：安全、PDA、移动通信、保护隐私、

信息安全的现实困扰 ！！

在信息社会的今天，无论是*个人消费者、商业企业、*还是*政府单位*等其他特殊实体，都越来越依赖各种现代通讯手段。然而，*电信网络基础结构*本质所决定的不安全性使得针对*无线及有线通讯*的侦听仅仅是个关于时间和经费的简单问题。

事实上，对于标准公共固定电话网络系统（PSTN），搭线窃听（Wiretapping）仅仅是*如何在通讯双方之间的物理或电气传输通道中获得某种形式接入的问题*，比如在*通讯双方的任意一端*、在*私有电话交换机设备（PBX）*、在*端局（Central Office）交换设备*，或者是在*端局间的长途传输设备*上等取得授权的或未经授权的接入。搭线窃听的相应费用虽然随着*接入点*的不同而有所变化，然而就总体而言是非常低廉的：如果接入点在有线接入最后一公里（Last Mile）中的某一点，一个十余美元的录音机即可完成任务；即使要在*端局间*的*微波线路*中获得*监听点*，现成的设备在市场上也不难得到。针对无线蜂窝电话（GSM、CDMA）空中接口（Wireless Air Interface）的监听设备从几百、几千至数万美元不等在国际市场上更是随处可见。而且，主流无线移动网络（GSM、CDMA）的空中接口部分也缺乏足够的安全保障。众所周知，GSM的空中接口加密技术已被证明有严重缺陷，监听及破解设备早已市场有售。所谓安全的*CDMA空中接口加密技术*也被证明是不安全的（Qualcomm 主席Irwin Jacobs 2003年在接受Yonhap 新闻机构采访中承认CDMA加密及授权认证机制存在缺陷）。以色列的安全分析人员亦曾在互联网络上公布了相应监听设备。其实，针对无线移动通信的监听往往在*有线传输系统*中更易于实现。事实上，无线信号在基站（Base Station）完成接入后皆以明文形式在*有线、微波或卫星网络*中传输。任何廉价的用于监听有线固定网络的设备皆可用于此目的。

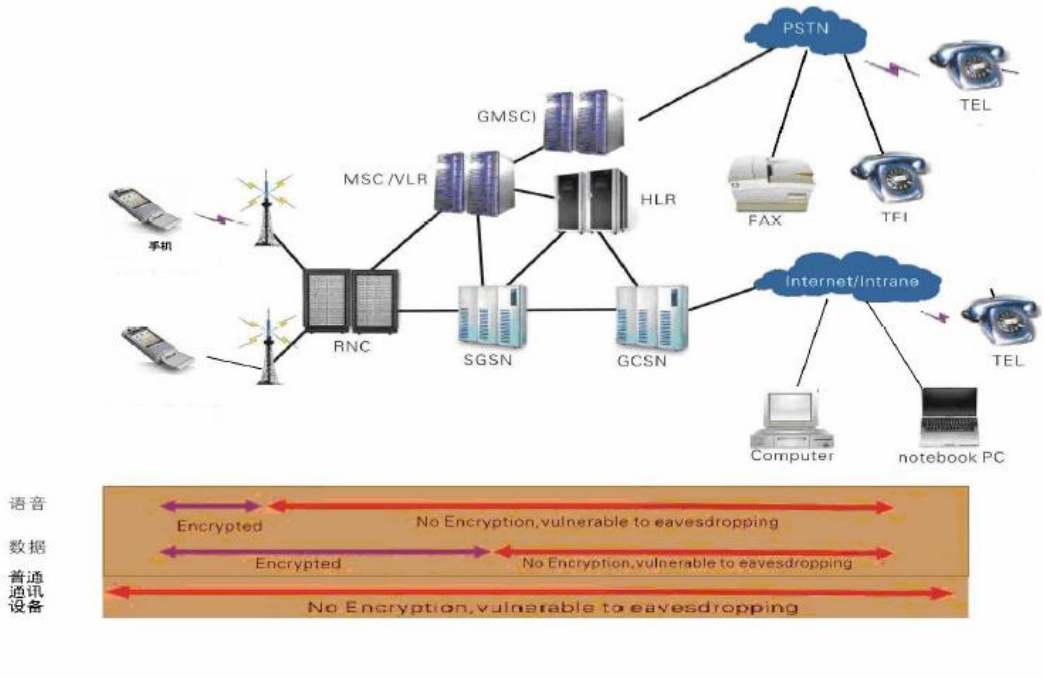


图 1：移动通信网络基础结构示意图

在中国的电信市场，由于*核心*及*端局*交换设备多数来自国外的公司，*公共电信网络*甚至是*政府用电信网络*更容易受到攻击，尤其是在*二代（2G）*，*二代半（2.5G）*和*三代（3G）*移动通讯网络中，安全问题已经，而且将更为严重。另外必需注意的是，即使在电信基础结构的物理安全有所保证的特殊环境中，如*政府专用网络*，*私有专用网络*等，当通信的一方处于*外网漫游状态*时，如*国际旅行*等，通讯的安全仍就难以保证。

危害信息安全的常用监听手段 ！！

随着*现代通信*与*计算机科学技术*的突飞猛进，针对现代通信的监听手段已经发展到了前所未有的成熟阶段。不但监听成功率大幅提高，效果突出，而且成本日趋低廉！！

常见的针对通信信息的监听手段包括：

搭线窃听：*最直接*的、同时也是*适用面积最广*、*设备*及*实施成本最低*、*技术发展最成熟*、*种类最丰富*的窃听手段。这种手段使用的设备，从*普通电话（串机使用）*到*磁带式、电子式被动录音设备*，到*铜缆搭线监听设备*、到*泄漏电磁信号恢复设备*、到光缆监听器、*深水水下光缆监听*、*长途微波传输信道*以及*卫星信道*的监听等等，都可可靠实现针对个人、团体乃至国家的非法监听。

针对空间链路的被动侦听：针对**2G/2.5G**乃至***3G****无线移动通信*的*空间链路拦截*与*实时解密监听*可直接扫描并在线监听手机通话（**1999**年**12**月第一台以低配置个人**PC**机为主体的可实时监听**GSM**手机空间链路的设备面市，彻底宣告了**GSM A5**加密算法的崩溃）。

针对空间链路的主动攻击：区别于上述被动侦听技术，侦听设备可*模拟无线移动通信的基站设备*，使用户手机终端设备“注册”到这些伪装的基站上，用户的通信信息则首先进入该监听设备，在由该设备“转发”到真正的基站，进入公共网络。用户的信息不但被监听，而且可被任意**篡改！！**

SIM/UIM卡复制与盗用：**SIM/UIM**卡，是现代移动通讯技术中普遍使用的用于*终端身份识别*、*用户特征识别*、*访问权限描述*、用户*数据存储*等功能的设备。早在**1998**年已有第一个关于**SIM**卡被复制并盗用合法用户手机使用的报道。目前，以很低廉的价格即可在市场上买到相关设备。一旦**SIM/UIM**卡被非法复制，合法用户不但将承担账号被盗用的相关经济损失，由于个人隐私、商业秘密甚至其他敏感信息的

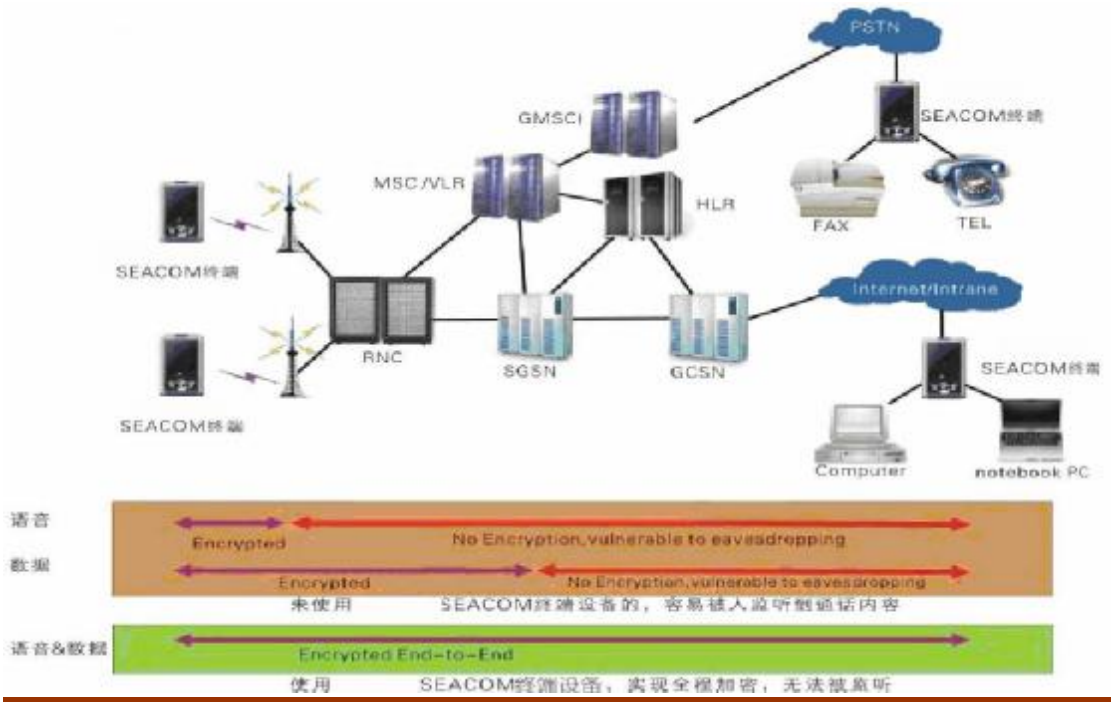
泄漏所造成的损失将无法用金钱衡量。

手机病毒：随着*手机功能的不断丰富*以及***3G****时代数据服务能力*与*容量*的提升，*智能手机等现代移动通信设备*的软件越来越复杂，饱受各种计算机病毒困扰的计算操作系统软件已运行于智能手机平台之上，*“手机病毒”*已经并将造成越来越大的危害，首当其冲就是因此引发的信息安全问题。

端到端的信息安全解决方案！！

北京微点科技有限公司现提供一款**移动通信安全技术产品**

安全的 PDA 产品，



它基于*可配路单片系统硬件平台*与*安全操作系统*， 支持 *GSM/GPRS 三频（900MHz, 1800MHz, 1900MHz）无线移动网络接入*以及 *2.4GHz 宽带无线局域网络（WiFi802.11b/g）接入*，实现端到端的、高强度、

全数字化加密的**移动语音、短信息**与**数据通讯**，完备保护个人隐私、商业秘密的移动通信安全。

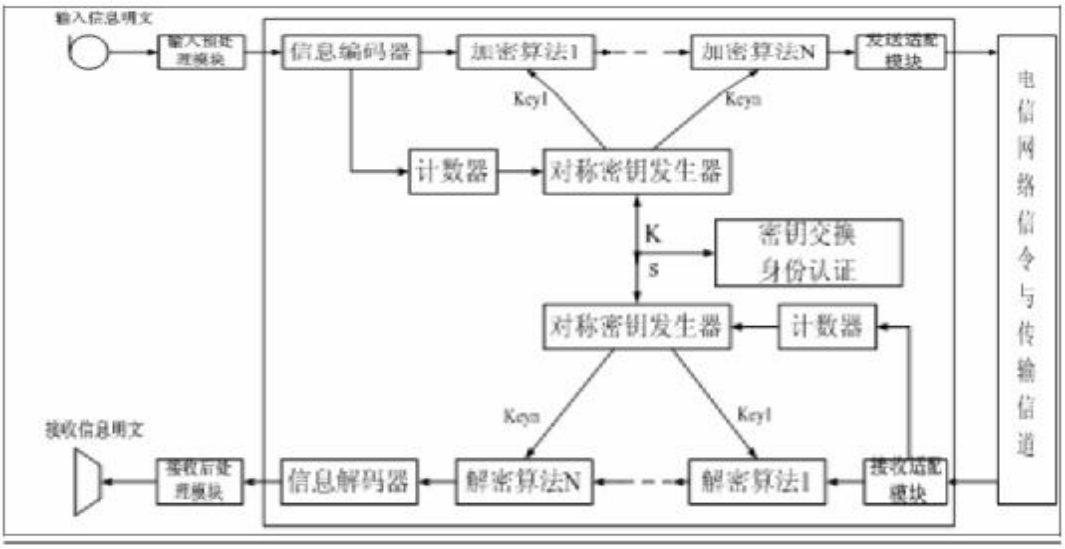


图 3：SEACOM 信息安全机制总体工作原理图

如有需要或咨询详情请与我公司联系。

公司：北京微点科技有限公司
地址：北京市海淀区中关村南大街 31 号中国空间技术研究院天辰写字楼 116
电话：010-68118075 刘飞
邮箱：leo@micronode.cn