浅谈无线通信技术的安全性

◆康　丹

1　无线通信技术的安全威胁

无线通信是利用电磁波信号在自由空间中传播的特性进行信息交换的一种通信方式。近些年，在信息流转领域中，发展最快、应用最广的就是无线通信技术。然而无线环节也已经正成为信息安全最薄弱的一环。近日，Fortinet 联合市调机构 Lightspeed/GMI 发布了 2015 年最新的全球信息安全调查报告。报告显示，将近一半（49%）的受访者将无线网络列为最易受攻击的环节，92%的 CIO 担忧无线网络将受到攻击，而最大的担忧来自中国，71%的 CIO 表示对无线安全十分担心。无线通信系统主要面临以下几方面的安全威胁。

1.1　非法窃听

这种威胁包括攻击者窃取数据包中的机密数据或窃取机密的上下文信息，例如标识、路由信息和用户的通信行为。这种威胁源于无线链路的开放性。

1.2　未经授权访问数据

攻击者伪装成合法用户访问网络资源，以期达到破坏目的；或者攻击者违反安全策略，非法占有系统资源和访问本应受保护的信息，这将会大量耗费系统资源，使运营商无法为用户提供满意的服务质量，严重影响系统的运营，同时会引起运营商收入的大量流失。同互联网的访问控制策略相同，访问控制是保证卫星通信网络安全的最重要核心策略之一。在访问控制方面主要考虑的安全隐患是非授权用户对无线通信资源和数据信息的非法访问和操作使用。因为从无线通信安全隐患所占的比重上来看，人为破坏因素比系统自身存在问题所占因素比重大的多。

1.3　非法基站

非法接入设备也是无线网络中经常出现的情况，这对于用户而言是非常危险的，它可以轻易地对用户发起中间人攻击。侵入者以非法手段占用通信基站频率，强行与有效范围内的不特定手机用户建立连接，迫使用户与通信网络中断，并向搜索到的用户发送事先已编辑好的信息。

1.4　破坏通信终端

无线通信中的卫星通信是微波在自由空间当中传播以实现信息传递。卫星通信系统由卫星和地球站两部分组成。地球站属于地面通信设备，基本安置在地面附近，易于维护。人造卫星则是环绕地球在空间轨道上运行，当卫星发生故障且自身不能修复时，可能会造成通信质量下降甚至通信中断等。另外，战时若知晓对方卫星在太空中的具体位置，可以采取使卫星偏离轨道或者直接摧毁卫星的方法，造成整个卫星通信系统的瘫痪。

1.5　返回 PC 端的流量劫持

卫星通信主要应用在一些网络不稳定、网速过慢或者没有网络的偏远地区。其中最普遍、最便宜的卫星网络是通过所谓的仅下游（downstream-only）连接的。用户 PC 端的请求会通过常规线路（有线或者 GPRS 连接）进行通信，且所有流入的流量均来自卫星。如此一来，用户就可获得一个相对较快的下载速度。从安全角度来看，卫星通信的最大缺点就是返回 PC 端的流量是非加密的，导致任何用户均可劫持这些流量。近来，Turla 组织利用卫星通信中固有的安全缺陷隐藏 C&C 服务器的位置和控制中心引起了我们对这一问题的重视。我们都知道，一旦 C&C 服务器的位置暴露，幕后恶意操作的黑手就会很容易被发现，所以

（下转第 117 页）

（上接第 114 页）

（4）解密。删除明文，界面如图4所示：

密文不变动，点击“解密”，恢复明文，界面如图3所示，完成解密过程。

图4　删除明文界面

4　结束语

RSA 公开密钥加密算法发展至今，在电子安全领域的各方面已经形成了较为完备的国际规范。本文研究了公钥密码体制中的 RSA 算法，设计了 RSA 算法步骤，借于 Delphi7 具有非常优秀的设计窗体，强大的可视化编程环境，高效的编译器，设计了简单实用的加解密模块，实现了利用 Delphi 进行加解密的功能。经过实际的运行，验证了 RSA 算法快速和安全性，可以应用于工程实践。

引用：

[1]卿斯汉.密码学和计算机网络安全[M].北京：清华大学出版社，2000.

[2]肖攸安，李腊元.数字签名技术的研究[J].武汉理工大学学报：交通科学与工程版，2002.

[3]唐正军.信息安全的核心——密码技术[J].网络世界，2001.

[4]陈彦学.信息安全理论与实务[M].北京：中国铁道出版社，2000.

[5]吴昊.基于 DES 算法和 RSA 算法的数据加密方案[J].焦作工学院学报：自然科学版，2002.

[6]肖振久，胡驰，姜正涛，陈虹.AES 与 RSA 算法优化及其混合加密体制[J].计算机应用研究，2014.

[7]向进.RSA 加密算法的安全性分析[J].吉普大学学报（自然科学版），2011.

[8]段晓萍，李燕华.非对称密码体制 RSA 的原理与实现[J].内蒙古农业大学学报，2009.

[9]朱作付，徐超，葛红美.基于 DSE 和 RSA 算法的数据加密传输系统设计[J].通信技术，2010.

[10]李云飞，柳青，郝林，周保林.一种有效的 RSA 算法改进方案[J].计算机应用，2010.

[11]张增强.Delphi7 实用教程[M].北京：中国铁道出版社，2003.

（江苏省常州市金坛开放大学　江苏　213200）

3 结束语

随着无线传感器的广泛应用，研究和开发网络数据隐私保护技术对其以后的发展有重大的积极影响，同时怎样做好隐私保护技术也成为研究领域的一大挑战。当前无线传感器网络数据隐私保护技术成为一个新的谈论话题，主要包括数据聚合、查询信息以及控制使用数据等。本文对无线传感器对网络数据隐私保护的现有成果进行阐述，其安全保护系数还是很高的，但我们也要看到还有很多方面发展的不完善，所以需要进一步调查和探究，很多战略性问题值得深思和考察。

引用：

[1]唐秀奎，刘国军. 解析无线传感器网络数据隐私保护技术. 中国新通信，2015.

[2]范永健，陈红，张晓莹. 无线传感器网络数据隐私保护技术. 计算机学报，2012.

[3]杨庚，王安琪，陈正宇. 一种低耗能的数据融合隐私保护算法. 计算机学报，2011.

[4]钟治初，郭江鸿，张海峰. 高效安全的无线传感器网络数据聚合方案. 计算机应用，2013.

[5]郭江鸿，马建峰. 安全透明的无线传感器网络数据汇聚方案. 通信学报，2012.

（新乡学院　河南　453007）

（上接第 115 页）

Turla 组织才会努力地去隐藏 C&C 服务器位置。

在劫持卫星 DVB-S 链接之前，需要具备以下设备：（1）卫星天线（大小取决于地理位置和卫星）；（2）低噪声块下变频器（LNB）；（3）专用的 DVB-S 调制器（PCIe 卡，建议使用 TBS Technologies 公司的 TBS-6922SE）；（4）电脑（最好是 Linux 系统的）。

为了攻击卫星网络链接，无论是卫星链接的合法用户还是攻击者自身的卫星天线都要指向特定的用于广播流量的卫星。攻击者会滥用卫星网络流量明文传输这一缺陷，具体的方式如下：（1）通过监听卫星中的 downstream 来识别卫星网络用户的 IP 地址；（2）然后在用户不知情的情况下选择一个 IP 地址来掩盖其 C&C 服务器真实 IP 地址；（3）被 Turla 感染的设备会收到一个指令：发送所有数据到被选中的 IP 地址上。数据先通过常规路径发送到卫星系统，然后再由卫星系统发送给选中 IP 地址的用户；（4）合法用户会以垃圾的方式将这些数据丢掉，但威胁操作者会从下游卫星链接处重新收集起这些数据。因为卫星通信的覆盖范围非常广，所以很难追踪到威胁操作者的具体位置。被 Turla 组织利用的卫星网络大多是位于中东和非洲的国家，如刚果、黎巴嫩、利比亚、尼泊尔、索马里和阿拉伯联合酋长国。

2 无线通信系统的安全技术分析

针对无线通信系统存在的主要安全威胁，无线通信中可采取的应对措施包括，一方面可以把传统的安全策略应用到无线通信技术上；另一方面加强系统自身的物理安全措施和链路安全措施。

2.1 传统的网络安全策略

传统的网络安全策略对卫星网络安全依然有效可行。传统网络安全策略包括访问控制，信息加密，鉴别交换和安全审计等。根据无线通信技术所面临的主要威胁的分析，可以看出，无线通信网与互联网对网络安全的目标要求一致，不同之处体现在物理链路和通信基础设施以及空间位置的局限上，若排除这些因素，其通信协议都是以 TCP/IP 协议为基础，因此传统的网络安全策略应用于无线通信网仍然可行。

2.2 数据加密

对无线通信进行加密能够减少甚至避免数据的泄露。无线通信终端设备的能源和存储容量是存在一定限制的，因此，想要用复杂的算法对无线通信进行加密是难以实现的。加之无线通信技术中的卫星通信具有一定的时延性，和较高的数据获取实时性要求。开展复杂的加密运算，会影响数据获取的实时性。DES 算法是对称密钥加密体制中的一种重要的算法，该算法选择的密钥决定了它的安全性。在 DES 算法中，数据通过 64 位分组开展加密工作，密钥长度为 56 位。通过一定的方式将位的输入转化为位的输出，解密时通过同样的步骤与密钥完成。美国卫星公司最早把这种算法应用到卫星通信系统中，从而实现对数据的加密，保护重要数据的安全，除此之外，还可以保障卫星指令链路的安全。

2.3 访问机制

非法用户如果能够顺利对无线网络进行访问，就会对通信进行恶意的破坏，使通信网络无法正常运行，甚至篡改和窃取重要数据。所以，必须通过访问控制对无线通信的安全加以落实。访问控制的内容应当囊括入网访问控制、网络权限控制、目录安全控制甚至属性安全控制等众多方面。通过这些方面的控制，对登录的用户进行筛选，保证登录用户为合法用户，用户只能开展授权操作，不得进行非授权操作。

2.4 运用 VPN 技术

应用 VPN 能够提高无线通信的安全性，VPN 技术安全保障的实现需要三个方面：用户认证、加密和数据认证。用户认证就是使得没有被授权的用户无法进行无线通信连接、无法进行铜线数据的发送和接收。加密就是对网线通信数据进行加密，使得非法入侵者即使成功获取了传输信号，也无法对传输的正确信息进行解读。数据认证则是对无线通信数据完整性的保护，必须保证全部的业务流都源于自身已经取得认证的设备。

2.5 加强网络外部环境管理

完善无线通信的相关法律规定，对非法入侵人员造成一定的震慑，提高其犯罪成本，减少犯罪冲动；加强对无线通信系统的使用管理与维护，减少由于使用与维护不当造成的系统故障；加强对无线通信安全管理人员的培训，不断提高其管理素质与应变能力，使其能够及时发现隐患，并在发现问题后可以迅速恢复无线通信系统的安全运行环境。

2.6 减少干扰

由于现阶段我们所使用的卫星都是采用透明转发器，对地面传来的信号只是变频转发而不加以任何处理，其主要部件之一是高功放器件，一般为行波管放大器（TWTA）或固态功放（SSPA），这两种器件最主要的特点是当输入功率小于饱和点时，可以近似地认为工作在线性区，而当输入功率进一步增大超过该电频时，功率放大器就进入饱和区或过饱和区。在过饱和区，不仅输出功率大大降低，而且出现大信号压缩小信号，即所谓的"功率掠夺"现象或"功率占用"，同时由于非线性的因素，还会出现大量寄生互调分量。为避免将卫星上功放推入饱和区或过饱和区，在使用中一般要实行严格的上行功率控制，或在高功放前加限幅器，尽可能使透明转发器可以避免功放工作在过饱和区。但是假如存在恶意的大功率上行干扰，转发器仍然有可能工作在非线性区，依然存在"功率掠夺"现象，致使正常通信业务信号或广播电视信号被压缩。对卫星上转发器实施干扰目前主要有堵塞式干扰和插播干扰两种形式。堵塞式干扰是指强占转发器的功率，将转发器全部阻塞，使通过该转发器的电视广播或通信业务全部瘫痪。其干扰源的频谱可以与正常信号重叠，也可以不重叠。插播干扰，即利用前面提到的"功率掠夺"插播非法信号，使正常工作的接收台站收到干扰方的非法信号。

引用：

[1]贺政明.谈无线通信技术的安全性[J].城市建设理论研究（电子版），2013.

[2]刘晓林.浅谈卫星通信的网络安全机制的构建[J].中国信息化，2013.

（石家庄士官学校指挥信息系统运用教研室　河北　050000）