网络安全

安全技巧（二十一）

小未 主编

目　录

宽带网安全规范设计

一、宽带的概念

宽带是一种传输媒介，它通过不同的频道，在一根同轴电缆或光纤电缆上建立起多个独立的网络载体信号。一般意义上的宽带还指高速网络连接，例如，宽带 Internet 连接通常就是指使用电缆调制解调器（cablemodem）或 DSL（数字用户线路）的 Internet 连接。被称为宽带的连接，其速率一般都超过 1Mbps（每秒 1 兆比特）。

电缆调制解调器允许一个计算机或计算机网络通过有线电视网络连接到 Internet。电缆调制解调器通常有一个以太网接口连接到计算机，速率可达 5Mbps 以上。

DSL 使用的是电话的常规铜线。与电缆调制解调器相比，DSL 可为用户提供专用带宽，但其最大带宽一般要低于最大的电缆调制解调器。DSL 有很多种，下面分别做一简介：

·ADSL：即非对称数字用户线路，这是一种新技术，在标准电话铜线上允许非常高的带宽。当安装 DSL 时，本地电话公司会给你的电话线上增加一个网络电缆双绞线。DSL 线路可以同步传输声音和数字信息。根据线路的长度和环数以及线路质量状况，ADSL 可以提供高达 8Mbps 的下行速率和 1Mbps 的上行速率。

·SDSL：即对称数字用户线路，可在上行和下行两个方向上提供相同的速率。

·VDSL：通过光纤传输的 DSL，就是 ADSL 的快速版本，短距离内的最大下行速率可达 55Mbps，上行

速率可达 2.3Mbps。

·RADSL：即速率自适应 DSL，就是指线路速度可以根据线路质量状况的改变而改变。

·IDSL：即 ISDNDSL，就是基于 ISDN 技术的 DSL。

二、永久连接的安全弊端

宽带 Internet 正在蓬勃发展，蒸蒸日上。有报道说，近 5 年内，中国要成为世界上宽带接入最廉价的地方。因此，实现永久连接、随时在线不再是遥远的梦。同时，我们必须明白，永久连入 Internet 同样意味着永远连接上了侵入威胁。

总体上说，宽带引进了 2 个方面的安全挑战：

1、黑客攻击的程度大大增加

永久连接就意味着黑客可以在没人注意的时间尝试冲破安全保卫。另外，永久连接经常使用固定 IP 地址，这样黑客就可以不时回来继续他们的工作。

2、通过公网连接到其他网络要求更高的安全性

黑客有很好用的工具可对 Internet 进行扫描以寻找不安全的计算机。事实上，宽带用户的计算机每天被黑客扫描 2 至 3 次一点都不足为奇。宽带用户最常见的错误是打开了 Windows 文件和打印机共享：

这就使攻击者能够访问并进入计算机。一旦黑客控制了系统，他们就可以盗走敏感信息、蓄意破坏文件，甚至使用这个计算机对其它站点发动攻击，例如前段时间在对 Yahoo、eBay **等站点发动的** DoS、DDoS **攻击中，有一个最初未受怀疑的宽带用户被权威部门抓获，他的** PC **被指控是用来发动这次攻击的一个罪魁。多么可怕啊！如果你已经是宽带了，千万要未雨绸缪，事先做好安全工作啊，别冤枉成替罪羊。**

三、SOHO **的安全问题**

SOHO **即** SmallOfficeHomeOffice**。连接宽带** Internet **的** SOHO **应该设有防火墙，既允许用户访问** Internet**，又能防止外界对内部的未经授权的访问。如果要运行一**

个 Web 服务器，还需要增加更复杂的安全策略以允许外部只访问那个 Web 服务器，而不能访问网络的其它部分。其他的安全功能还有：阻止对网络发动 DoS、DDos 攻击，防止从网络内部发动 DoS 攻击(即防止 IP 欺骗)，设置 URL 过滤规则阻止雇员访问一些不适宜的 Web 站点。

其实，安全的问题根本在于人和宣传。以前，大多数企业都对其公司连接 Internet 所带来的安全问题满不在乎，但随着黑客对公司发动攻击或黑客控制公司 PC 的事件不断曝光，人们的安全意识显然大大增强。例如，我们单位的同事在重新安装系统后，第一个要安装的应用软件就会是反病毒软件。否则，他们的心里会没有底。

现在，企业已经改变了自己购买并管理安全产品的方式，更愿意接受让中间商安装并管理安全方案的工作方式，也就是所谓的服务外包。这会从很大程度上使用户集中于管理层面上，而不是琐碎的技术细节中。

四、将企业安全界限扩展到分支机构和网上独立工作者

宽带连接最引人注目的用途就是允许分支机构和网上独立工作者（Telecommuters）用高速远程访问连接到公司的网络中。宽带连接与低速拨号线路相比可以显著降低访问的收费，因为后者要想连接到中心站点经常需要打长途电话。

使用 IPSec 加密技术的 VPN（虚拟专用网络）是企业将其网络扩展到分支机构和网上独立工作者的重要方式。VPN 使用公网如 Internet 作为网络传输途径，将公司站点、变动的工作人员和网上独立工作者安全地互相连接在一起。根据专家分析，VPN 的费用大约相当于专

用网络的一半，比帧中继便宜四分之一，将 VPN 用于远程访问连接可以节约企业开支 30%到 70%。

网上独立工作者在他们的 PC 上安装 VPN 客户软件，由它创建一个从 PC 到中心站点 VPN 网关的加密通道，从而实现连回公司网络的目的。但是，VPN 客户软件现在也存在许多问题，这些问题包括：

·难于实现在大量远程 PC 上安装和更新网络软件。

·除了 Windows 以外，许多操作系统都缺乏 VPN 客户软件，例如 Linux、Mac、Solaris、BSDI

·被用来做保密工作的远程 PC 缺乏安全性

·带来了新的安全突破口，黑客可通过对远程 PC 进行 U-turn 攻击从而破坏公司网络的安全。在一个 U-turn 攻击中，黑客获取了网上独立工作者的不安全 PC 的访问权，利用那个 PC 通过 VPN 通道连接到公司网络内部，从而使黑客能够充分利用公司网络并威胁企业的安全基础架构。

五、宽带网络安全方案设计技巧

如果你或你的单位已经实现了宽带 Internet，强烈建议考虑并采用以下安全方案：

·防火墙：防火墙在两个网络之间执行一个访问控制策略。防火墙可以是软件，如 Checkpoint、Symantec、CA，也可以是硬件设备，如 NetScreen、Watchguard、Sonicwall、Nokia 等。家庭用户可以使用个人防火墙，如 NetworkICE、Symantec 等。

·反病毒软件：现在，一天没有反病毒软件，一天就不会踏实。强烈建议在宽带连接上使用反病毒软件，如 Norton、McAfee、TrendMicro、CA、瑞星、金山毒霸、北信源 VRV 等。

·加密：对于特别敏感的通信，要考虑对 PC 上的通信进行加密。带有 VPN 保护的防火墙可以保护远程站点的敏感数据，并防止来自这些计算机的拒绝服务攻击。VPN、SSL 提供了电子商务交易的安全方法。根据业务需要，可以采用 PGP、PKI 这样的产品。

·调制解调器安全：有时候，调制解调器的配置和验证信息会存储在它上面，有些会存储在计算机上。因此，最好咨询厂商以确定并保护这些信息。

·共享的电缆调制解调器连接：电缆网络经常由多个用户共享使用，这使得黑客可以使用嗅探器对信息传输进行监控。因此，要确定服务供应商是否将网络和设备升级到了 DOCSIS(基于线缆数据传输服务接口标准)。

·内容检查：Java、JavaScript、ActiveX 等互动技术是宽带内容站点和 Email 的重要组成部分，同时也是黑客攻击的潜在媒体。建议在浏览器中和 Email 客户软件中禁止这些功能。

·系统安全：这方面的因素有许多，在此列举一些。

1、在不使用连接时应该退出网络并关掉 PC 电源。

2、许多聊天室客户软件都允许交换可执行文件，它们所带来的风险与 Email 客户软件是相同的，因此要尽量避免使用聊天室。

3、做好常规的系统备份，并保存一份启动盘。

4、为所有应用程序和 OS 及时安装补丁程序。

5、不要运行来历不明的程序，不要打开未知 Email 的附件。

6、除非完全必要，请关闭文件和打印共享。

7、登录 id 和口令要８个字符以上，最好是文字和数字的组合。

六、结论

总而言之，一旦你宽带了，就必须清醒地意识到你是 7 天 24 小时地连接在网上了。只有将宽带访问技术与整体安全方案综合考虑，我们才可能安全地、放心地在高速网络上畅通行驶。

网络安全思想

网络安全，这是个百说不厌的话题。因为在互联网上，每台计算机都存在或多或少的安全问题。安全问题不被重视，必然会导致严重后果。诸如系统被破坏、数据丢失、机密被盗和直接、间接的经济损失等。这都是不容忽视的问题。既然说到网络安全，我们经常提到要使用防火墙、杀毒软件等等。这些的确很重要，但是人们往往忽视了最重要的，那就是思想意识。

人类的主观能动性是很厉害的，可以认识世界、改造世界，正确发挥人的主观能动性可以提高认知能力。但是人类本身固有的惰性也是十分严重的，喜欢墨守成规、图省事。就是这点惰性给我的网络带来了安全隐患。据不完全统计，每年因网络安全问题而造成的损失超过 300 亿美元，其中绝大多数是因为内部人员的疏忽所至。所以，思想意识问题应放在网络安全的首要位置。

一、密码

看到这里也许会有读者以为我大放阙词，那就先以我自己的一个例子来说起吧。

本人也很懒，但是也比较注意安全性，所以能设置密码的地方都设置了密码，但是密码全是一样的。从 E-

mail 信箱到用户 Administrator，统一都使用了一个 8 位密码。我当初想：8 位密码，怎么可能说破就破，固若金汤。所以从来不改。用了几年，没有任何问题，洋洋自得，自以为安全性一流。恰恰在你最得意的时候，该抽你嘴巴的人就出现了。我的一个同事竟然用最低级也是最有效的穷举法吧我的 8 位密码给破了。还好都比较熟，否则公司数据丢失，我就要卷着被子回家了。事后我问他，怎么破解的我的密码，答曰：只因为每次看我敲密码时手的动作完全相同，于是便知道我的密码都是一样的，而且从不改变。这件事情被我引以为戒，以后密码分开设置，采用 10 位密码，并且半年一更换。现在还心存余悸呢。

我从中得出的教训是，密码安全要放在网络安全的第一位。因为密码就是钥匙，如果别人有了你家的钥匙，就可以堂而皇之的进你家偷东西，并且左邻右舍不会怀疑什么。我的建议，对于重要用户，诸如：Root，Administrator 的密码要求最少要 8 位，并且应该有英文字母大小写以及数字和其他符号。千万不要嫌麻烦，密码被破后更麻烦。

为什么要使用 8 位密码呢？Unix 一共是 0x00 至 0xff 共 128 个字符。小于 0x20 的都算是控制符，不能输入为口令，0x7f 为转义符，不能输入。那么总共有 128-32-1=95 个字符可作为口令的字符。也就是 10（数字）+33（标点符号）+26*2（大小写字母）=95 个。如果口令取任意 5 个字母+1 位数字或符号（按顺序），可能性是：52*52*52*52*52*43=16，348，773，000（即 163 亿种可能性）。但如果 5 个字母是一个常用词，估算一个，设常用词 500 条，从 5000 个常用词中取一个词与任意一个

字符组合成口令，因每一个字母都分为大小写，所以其可能性为：5000*282828282843=6，880，000（即 688 万种可能性）。但实际上绝大多数人都只用小写字母，所以可能性还要小。这已经可以用微机进行穷举了，在 Pentium200 上每秒可算 3.4 万次，像这样简单的口令要不了 3 分钟。如果用 P4 算上一周，可进行 3000 亿次演算。所以 6 位口令很不可靠，应用 8 位。

密码设的越难以穷举，并不是带来更加良好的安全性。相反带来的是更加难以记忆，甚至在最初更改的几天因为输入缓慢而被别人记住，或者自己忘记。这都是非常糟糕的，但是密码难于穷举是保证安全性的前提。矛盾着的双方时可以互相转化的，所以如何使系统密码既难以穷举又容易记忆呢，这就是门科学了。目前这方面的书籍几乎没有，所以我只能凭借自我经验来向大家介绍了。

1、采用 10 位以上密码。

对于一般情况下，8 位密码是足够了，如一般的网络社区的密码、E-mail 的密码。但是对于系统管理的密码，尤其是超级用户的密码最好要在 10 位以上，12 位最佳。首先，8 位密码居多，一般穷举工作的起始字典都使用 6 位字典或 8 位字典，10 位或 12 位的字典不予考虑。其次，一个全码 8 位字典需要占去 4G 左右空间，10 位或 12 位的全码字典更是天文数字，要是用一般台式机破解可能要到下个千年了，运用中型机破解还有有点希望的。再次，哪怕是一个 12 个字母的英文单词，也足以让黑客望而却步。

2、使用不规则密码。

对于有规律的密码，如：a1b2c3d4e5f6，尽管是 12

位的，但是也是非常好破解的。因为现在这种密码很流行，字典更是多的满天飞，使用这种密码等于自杀。

3、使用键盘外围的按键作为密码的组成部分。

现在的许多破解软件都支持 Incremental（渐进）方式的密码组合进行穷举，其核心内容就是引入频率统计信息，即“高频先试”的原则。所以，对于键盘外围的按键都属于“低频使用”的按键。运用这些按键组成密码可以防止支持渐进式组合穷举的破解软件。

4、使用左右上下按键结合输入的密码。

把键盘从“T、G、B”三个键和“Y、H、N”三个键中间划分成左右部分，从“Q~P”和“A~””这两行中间划分为上下部分，这样键盘就被围成了 4 部分。选取组成密码的按键最好从这 4 部分中分别选取交叉组合,这样做的目的是防止别人轻易看出并且记住你密码。最好是熟练使用“CapsLock”键，可以达到密码安全的最高境界。

5、不要选取显而易见的信息作为口令。

单词、生日、纪念日、名字都不要作为密码的内容。

以上就是密码设置的基本注意事项。密码设置好了，并不代表万事大吉，密码的正确使用和保存才是关键。

1、要熟练输入密码，保证密码输入的速度要快。输入的很慢等于给别人看，还是熟练点好。

2、不要将密码写下来。密码应当记在脑子里，千万别写出来。

3、不要将密码存入计算机的文件中。

4、不要让别人知道。

5、不要在不同系统上使用同一密码。

6、在输入密码时最好保证没有任何人和监视系统的

窥视。

7、定期改变密码，最少半年一次。这点尤为重要，是密码安全问题的关键。永远不要对自己的密码过于自信，也许无意中就泄漏了密码。定期改变密码，会使密码被破解的可能性降到很低的程度。

8、对于大型网络的系统管理员，应该定期使用密码破解软件来检测全体用户密码的安全性。但要注意这些软件是否留有后门。

对于有些用户来说，这样做的确有点太那个了；但是对于管理员来说，就显得尤为重要。有些用户采用诸如 PGP（PrettyGoodPrivacy，良好隐私）这类的软件来生成密码。这是个很好的方法，但是 PGP 的真正用途是用于对机密性文件的加密。一般密匙都在 1024 位，如著名的 RSA 公匙。对于一般密码生成，PGP 不是最好的，它并不适合你自己。

管理员应该保证 Root 用户、Administrators 用户组、PowerUsers 用户组、SuperUsers 用户组以及 Replicator 用户组密码的安全性要高，防止低权限的用户的密码被窃取影响到高权限用户的安全性及整个系统的安全性。不要用 Root 及其他高权限用户去察看其他用户的文件，以免造成安全隐患。管理员要定期给员工进行安全知识培训，增强员工的安全意识。一旦发现高权限用户无法登陆，察看系统日志，必要时刻将主机断开所有网络以保证主机系统及重要文件的安全性。

二、漏洞

网络安全性之所以这么低的一个主要原因就是系统漏洞。譬如管理漏洞、软件漏洞、结构漏洞、信任漏洞。如果管理员解决不好结构漏洞和信任漏洞，我想这位管

理员应该可以卷着被子回家了。在此主要谈论一下管理漏洞和软件漏洞。这两种漏洞产生的原因也是人为的。

1、微软系统

这个涉及面就比较广了，但主要是 Windows9x 系统、WindowsNT 系统、SQLServer。

不可否认，尽管这些系统的内核和组成有所不同，但通病还是有的，比如容易受到 DoS（DenialOfService，分布式拒绝服务）和 OOB（OutOfBand）方式的攻击。这是比较致命的漏洞，但是通过修改注册表、打补丁的方法都可以避免。但是有一点漏洞是不能避免的，就是在 Windows 系统下运行 IIS（InternetInformationServer，Internet 信息服务），这样约等于自杀。

首先，Windows 下的密码文件存储时都不能经过 shadow，所以只要拿到了这个文件用相应的软件打开，所有的用户名和密码都暴露无遗。其次，现在许多用户喜欢用 Windows2000，原因是不易崩溃。但是很多人都在 Windows2000 下安装了 IIS，但是他们却不会配置 IIS。最可悲的是只要你登陆到 Internet，IIS 就自动运行，而且端口都是固定的：默认 FTPPort21，默认 WebPort80，默认 SMTPPort25。等于给人家大开后门。

对于用 SQLServer 或 Windows2000+IIS 架站的服务器，安全系数并不如用 Unix 系统。因为 Windows 固有的易崩溃的特性依然保留，对 DoS 的抵抗力还是太低，直到 Beta2 版的 WindowsXP 依然保留了这个特性。而且通过 Ftp 登陆，首先告诉你机器的 IIS 是什么版本，这就为攻击服务器提供了方便，而且如果权限设置不好，anonymous 都可以使用 debug。安全性实在不好。

2、Unix 系统

我这里说的Unix系统指的是和Unix有类似的系统，比如：SCOUnix、以前的SUNOS和现在的Solaris、FreeBSD、xBSD、HP和IBM的Unix。这些Unix的结构基本相同，长的差不多，区别不大，但是都有各自的漏洞。比如SUNOS的snoop命令，可以监听到同一共享网段内的其他用户口令，包括超级用户。这一点也被Solaris继承了。而且这些Unix系统有个通病，就是在能访问对方机器的情况下，把shell命令用ksh运行，在自己能用的目录里放上叫“ls”之类的程序，希望超级用户可以不小心的运行他们，一旦运行，就可以获得其权限。对于这一点，超级用户的Path中不应当有“.”（既当前目录）。

所以这就要求管理员的素质相对的要高，可以把软件漏洞都补上，同时不出现管理漏洞。还得防止被窃听。

现在最多的漏洞出现在CGI上。使用这些服务最容易受到DoS方式的攻击。CGI是Web的安全漏洞的主要来源。尽管CGI协议并不是固有的不安全，然而不幸的是，有的Script缺少这样的标准，而对之信任的管理员把它安装在节点上，造成每个CGI都存在被攻击bug的可能性。CGI的安全隐患主要在于两个方面：①他们会有意无意的泄漏主机的系统信息；②处理远程用户输入的如表格的内容或“搜索内容”命令的Script，可能容易被远程用户攻击而执行命令。

对于Java，PHP，ASP也存在相应的错误。这些都是管理员应该予以注意。

三、总结

由于思想涣散造成的漏洞要远高于系统自身的漏洞，而系统自身的漏洞也是由于管理员的大意造成的。

所以，加强思想意识上的安全教育，势在必行。

黑客的七大类型

恶作剧型

喜欢进入他人网站，以删除某些文字或图像、篡改网址、主页信息来显示自己的厉害，此做法多为增添笑话自娱或娱人，或者进入他人网站内，将其主页内商品资料内容、价格作降价等大幅度修改，使消费者误以为该公司的商品便宜廉价而大量订购，从而产生 Internet 订货纠纷。

隐蔽攻击型

躲在暗处以匿名身份对网络发动攻击，往往不易被人识破，或者干脆冒充网络合法用户，侵入网络“行黑”，这种行为由于是在暗处实施的主动攻击行为，因此对社会危害极大。

定时炸弹型

在实施时故意在网络上布下陷阱，或故意在网络维护软件内安插逻辑炸弹或后门程序，在特定的时间或特定条件下，引发一系列具有连锁反应性质的破坏行动，或干扰网络正常运行或致使网络完全瘫痪。此种黑客在原公司离职后，通过连线，在得知原公司 Internet 地址密码的情形下，可从网上再次了解到原公司网络密址及电子邮件中各项文件资料，进而大量截取原公司最新资料，作为不正当竞争之用。这类黑客是企业内部蛀虫，其危害和影响巨大，有时几乎导致企业的破产倒闭，而混在政府内的这类黑客，破坏性更大。

矛盾制造型

非法进入他人网络，修改其电子邮件的内容或厂商签约日期，进而破坏甲乙双方交易，并借此方式了解双方商谈的报价价格，乘机介入其商品竞争。有些黑客还利用政府上网的机会，修改公众信息，挑起社会矛盾和动乱。

职业杀手型

此种黑客以职业杀手著称，经常以监控方式将他人网站内由国外传来的资料迅速清除，使得原网站使用公司无法得知国外最新资料或订单，或者将电脑病毒植入他人网络内，使其网络无法正常运行。更有甚者，进入军事情报机关的内部网络，干扰军事指挥系统的正常工作，任意修改军方首脑的指示和下级通过网络传递到首脑机关的情报，篡改军事战略部署，导致部队调防和军事运输上的障碍,达到干扰和摧毁国防军事系统的目的，严重者可以导致局部战争的失败。

窃密高手型

出于某些集团利益的需要或者个人的私利，利用高技术手段窃取网络上的加密信息,使高度敏感信息泄密。或者窃取情报用于威胁利诱政府公职人员，导致内外勾结进一步干扰破坏内部网的运行。有关商业秘密的情报，一旦被黑客截获，还可能引发局部地区或全球的经济危机或政治动荡。

业余爱好型

计算机爱好者受到好奇心驱使，往往在技术上追求精益求精，丝毫未感到自己的行为对他人造成的影响，属于无意识攻击行为。这种人可以帮助某些内部网堵塞漏洞和防止损失扩大。有些爱好者还能够帮助政府部门