 DOI: https://doi.org/10.36956/iser.v2i1.369

Analysis of Computer Network Security Technology

Chaofan Wu

Fujian Normal University, Fuqing, Fujian, 350300, China

Abstract

Based on the introduction of computer network security overview, the paper analyzes the reasons and methods of computer network security threats, and proposes preventive measures for computer network security.

Keywords

computer network; network security; prevention

计算机网络安全技术浅析

吴超凡

福建师范大学，中国 · 福建 福清 350300

摘　要

论文在介绍计算机网络安全概述的基础上，分析了计算机网络安全威胁产生的原因及方式，提出了计算机网络安全的防范措施。

关键词

计算机网络；网络安全；防范

1 计算机网络的潜在安全隐患

电子商务的网络环境包括 Intranet、Extranet、Internet 三种结构组成的网络环境，电子商务的网络安全涉及网络环境的各个方面。

企业内部的典型风险有：没有好的备份系统导致数据丢失；有外来磁盘携带的病毒攻击计算机系统；业务人员的误操作；删除了不该删除的数据，且无法恢复；系统硬件、通信网络或软件本身出故障。

如果企业的内部网连接上 Internet，则 Internet 本身的不安全性对企业内部信息系统带来的潜在风险主要有：外部非法用户潜入系统胡作非为，甚至破坏系统；数据丢失，机密信息泄漏；互联网本身固有的风险的影响；网络病毒的攻击。

Internet 的安全问题的主要原因之一在于 TCP/IP 和 UDP 的基本体系结构。

2 计算机网络安全体系

一个全方位的计算机网络安全体系包含网络的物理安全、访问控制安全、系统安全、用户安全、信息加密、安全传输和管理安全等。

在实施网络安全防范措施时应考虑以下几点：要加强主机本身的安全，做好安全配置，及时安装安全补丁程序，减少漏洞；要用各种系统漏洞检测软件定期对网络系统进行扫描分析，找出可能存在的安全隐患，及时修补；对敏感的设备和数据要建立必要的物理或逻辑隔离措施；安装防病毒软件，加强内部网的整体防病毒措施；建立详细的安全审计日志，以便检测并跟踪入侵攻击等。

3 常用的计算机网络安全技术

目前，常用的计算机网络安全技术主要有病毒防范技术、身份认证技术、防火墙技术和虚拟专用网 VPN 技术等。

3.1 病毒及黑客防范技术

计算机病毒是带有一段恶意指令的程序，一旦用户运行了被病毒感染的程序，它就会隐藏在系统中不断感染内存或硬盘上的程序。

黑客程序实际上是人们编写的程序，它能够控制和操纵远程计算机，一般由本地和远程两部分程序组成。考虑到黑

 DOI: https://doi.org/10.36956/iser.v2i1.369

客程序的危害性，把黑客程序也归于计算机病毒。

3.1.1 单机病毒

（1）单机病毒的种类

单机病毒就是以前的 DOS 病毒、Windows 病毒和能在多操作系统下运行的宏病毒。

DOS 病毒是在 MS-DOS 及其兼容操作系统上编写的病毒程序，例如以前著名的“黑色星期五”“DIR”等病毒。

Windows 病毒是在 Win3.x/Win9.x 上编写的纯 32 位病毒，例如 4 月 26 日危害全球的 CIH 病毒等。

宏病毒是利用 Office 特有的“宏”编写的病毒，它专门攻击微软 Office 系列 Word 和 Excel 文件。这种病毒不仅能运行在 Windows 环境，还能运行在 OS/2 或 MAC OS 上的微软 Office 软件中。例如“七月杀手”宏病毒，会在七月的任一天发作，发作时弹出“醒世恒言”对话框，要求用户选择“确定”或“取消”，如果按了“取消”，就会在 autoexec.bat 中增加一条删除 C 盘的命令，重新开机时，就会删除 C 盘上的全部数据。

（2）单机病毒的防范

考虑到每种杀毒产品都有其局限性，所以最好准备几套杀毒软件，用它们来交叉杀毒，杀毒软件还要及时升级；定期用杀毒软件检查硬盘，如果用的是 Win9.x（CIH 病毒对 WINNT 和 WIN2000 不起作用），每月的 26 号前一定要检查是否有 CIH 病毒，或者将系统日期跳过 26 号。C 盘最好是 FAT32 格式，容量大于 2G，这样设置的好处是，有利于提高系统运行速度，此外如果 C 盘被 CIH 病毒破坏了，只要它是 FAT32 格式，且容量大于 2G，用一般杀毒软件就可以将 C 盘上的数据恢复 98%。

CIH 病毒至少有 9 个变种，其中 V1.2 和 V1.3 在 4 月 26 号发作，V1.4 在每月的 26 号发作，还有的版本发作日期在 6 月 26 号。

3.1.2 网络病毒及其防范

网络病毒通常是指特洛伊木马和邮件病毒，因为是通过网络传播的，所以称为“网络病毒”。

（1）特洛伊木马病毒

特洛伊木马是一种黑客程序，与病毒有些区别，特洛伊木马本身一般并不破坏受害者硬盘上的数据，它只悄悄地潜伏在被感染的计算机里，一旦这台计算机上网，就可能大祸临头。木马、黑客病毒往往是成对出现的，即木马病毒负责侵入用户的电脑，而黑客病毒则会通过该木马病毒来进行控制。现在这两种类型都越来越趋向于整合了，一般的木马如 QQ 消息尾巴木马 Trojan.QQ3344，还有针对网络游戏的木马病毒如 Trojan.mir.PSW.60。值得注意的是，病毒名中有 PSW 或者什么 PWD 之类的一般都表示这个病毒有盗取密码的功能（这些字母一般都为“密码”的英文“password”的缩写）一些黑客程序有：网络枭雄（Hack.Nether.Client）等。

特洛伊木马病毒的防范方法是：不要轻易泄漏 IP 地址，下载来历不明的软件时要警惕其中是否隐藏了特洛伊木马，使用下载软件前一定要用特洛伊木马检测工具进行检查。

（2）邮件病毒

邮件病毒和普通病毒是一样的，只不过由于它们主要通过电子邮件传播，所以才称为“邮件病毒”，一般通过邮件中“附件”夹带的方法进行扩散，一旦你收到这类 E-mail，运行了附件中的病毒程序，就能使你的计算机染毒。这类病毒本身的代码并不复杂，比如 I love you 病毒，只要收到带有该病毒的 E-mail 并打开附件后，病毒就会按照脚本指令，将浏览器自动连接上一个网址，下载特洛伊木马程序，更改一些文件后缀为 .vbs，最后再把病毒自动发给 Outlook 通信薄中的每个人。

还有一个恶作剧，有人用 VBScript 编写了一个 HTML 文件，代码如下：

```
<script language="VBScript">
Dim WSHShell
Set WSHShell=CreateObject（wscript.Shell）
WSHShell.run（“c：\fbrmatd：”）
</script>
```

只要打开该网页，D 盘就被格式化了。预防办法是禁止 HTML 中脚本的运行（在浏览器的“工具 /Internet 选项 / 安全”中设置禁止 Java 或 Active X 的运行），当 IE 提示“该网页上的某个软件可能不安全，建议不要运行。

邮件病毒的防范方法是：不要打开陌生人来信中的附件，特别是“.exe”等可执行文件；养成用最新杀毒软件及时查毒的好习惯，不要急于打开附件中的文件，先将其保存在特定目录中，然后用杀毒软件进行检查；收到自认为有趣的邮件时，不要盲目转发，因为这样会帮助病毒的传播；对于通过脚本“工作”的病毒，可采用在浏览器中禁止 Java 或 Active X 运行的方法来阻止病毒的发作。

 DOI: https://doi.org/10.36956/iser.v2i1.369

（3）脚本病毒

脚本病毒的前缀是：Script。脚本病毒的共有特性是使用脚本语言编写，通过网页进行传播的病毒，如红色代码（Script.Redlof）o 脚本病毒还会有如下前缀：VBS、JS（表明是何种脚本编写的），如欢乐时光（VBS.Happytime）、十四日（Js.Fortnight.c.s）等。

（4）蠕虫病毒

蠕虫病毒的前缀是：worm 这种病毒的共有特性是通过网络或者系统漏洞进行传播，很大部分的蠕虫病毒都有向外发送带毒邮件，阻塞网络的特性。比如冲击波（阻塞网络）、小邮差（发带毒邮件）等 [1]。

3.1.3 网上炸弹及其防范

（1）IP 炸弹

IP 炸弹一般是指用专用的攻击软件（如 WinNuke、IGMPNuke 等）发送大量的特殊数据，对远程计算机中的 Windows 系统的漏洞进行攻击，造成对方的 Windows 蓝屏死机。当用户在聊天室聊天时，其 1P 地址很容易被别人查到，如果对方要发起攻击，只要用专用软件攻击用户的 IP 就可以了。

对付 IP 炸弹最好的办法是安装个人防火墙。个人防火墙实际上是一套程序，即对进出计算机的所有数据进行分析，切断非法连接。使用个人防火墙前一般要进行系统设置，进行“安全规则设置”。

（2）邮件炸弹

邮件炸弹的原理是向有限容量的信箱投入足够多或者足够大的邮件，使邮箱崩溃。这类炸弹很多，如 Nimingxin，Quickfyre mair Emailbomb、Upyours 系列、雪崩等。

防范邮件炸弹的方法有以下几种：①在邮件软件中设置好防范项目；②在邮件服务器上设置过滤器，防范邮件炸弹；③使用删除 E-mail 炸弹的工具；④谨慎使用自动回信。

3.2 身份识别技术

身份识别技术的基本思想是通过验证被认证对象的属性来达到确认被认证对象是否真实有效的目的。被认证对象的属性可以是口令、问题解答或者指纹、声音等生理特征，常用的认证技术有口令、标记法和生物特征法。

3.2.1 口令

传统的认证技术主要采用基于口令的认证方法。当被认证对象要求访问提供服务的系统时，提供服务的认证方要求被认证对象提交该对象的口令，认证方收到口令后，将其与系统中存储的用户口令进行比较，以确认被认证对象是否为合法访问者。

一般的系统都提供了对口令认证的支持，对于封闭的小型系统来说不失为一种简单可行的方法。

但是，传统的认证技术也有一些不足之处。用户每次访问系统时都要以明文方式输入口令，很容易泄漏；口令在传输过程中可能被截获；系统中所有用户的口令以文件形式存储在认证方，攻击者可以利用系统中存在的漏洞获取系统的口令文件；用户在访问多个不同安全级别的系统时，都要求用户提供口令，用户为了记忆的方便，往往采用相同的口令；只能进行单向认证，即系统可以认证用户，而用户无法对系统进行认证。

3.2.2 标记方法

标记是个人持有物，作用类似于钥匙，标记上记录着用于机器识别的个人信息。常用的标记有磁介质、智能卡。

3.2.3 生物特征法

每个人都有唯一且稳定的特征，如指纹、眼睛以及说话和书写等做事的标准方法。生物特征法是基于物理特征或行为特征自动识别人员的一种方法，其优点是严格依据人的物理特征并且不依赖任何迸被拷贝的文件或可被破解的口令，所以它是数字证书或智能卡的选择 [2]。

3.3 防火墙技术

3.3.1 防火墙概述

（1）防火墙的概念

防火墙是指一个由软件和硬件设备组合而成，处于企业或网络群体计算机与外界通道（Internet）之间，在内部网与外部网之间实施安全防范的系统，可被认为是一种访问控制机制，用于限制外界用户对内部网络访问及管理内部用户访问外界网络的权限，即确定哪些内部服务允许外部访问，以及允许哪些外部访问访问内部服务。

（2）防火墙的设计原则

防火墙的设计有以下两个原则：

第一，一切未被允许的就是禁止的。基于该准则，防火墙应封锁所有信息流，然后对希望提供的服务逐项开放，只有经过精挑细选的服务才被允许使用。其弊端是安全性高于

 DOI: https://doi.org/10.36956/iser.v2i1.369

用户使用的方便性，用户所能使用的服务范围受到很大限制。

第二，一切未被禁止的就是允许的。基于该准则，防火墙应转发所有信息流，然后逐项屏蔽可能有害的服务，从而可为用户提供更多的服务。其弊端是在日益增多的网络服务面前，网管人员疲于奔命，特别是受保护的网络范围增大时，很难提供可靠的安全防护。

（3）防火墙的实现技术

按照建立防火墙的主要途径，防火墙的实现技术可分为分组过滤、代理服务和应用网关。分组过滤技术是一种简单、有效的安全控制技术，它通过在网络间相互连接的设备上加载允许、禁止来自某些特定的源地址、目的地址、TCP 端口号等规则，对通过设备的数据包进行检查，限制数据包进出内部网络。分组过滤技术的最大优点是对用户透明，传输性能高。但由于安全控制层次在网络层和传输层，其安全控制的力度只限于源地址、目的地址和端口号，因而只能进行较为初步的安全控制，对于恶意的拥塞攻击、内存覆盖攻击或病毒等高层次的攻击手段则无能为力。

代理服务是运行于内部网络与外部网络之间的主机之上的一种应用。当用户需要访问代理服务器另一侧主机时，对符合安全规则的连接，代理服务器会代替主机响应，并重新向主机发出一个相同的请求。当此连接请求得到回应并建立起连接后，内部主机同外部主机之间的通信将通过代理程序将相应连接映射来实现。对于用户而言，似乎是直接与外部网络相连的，代理服务器对用户透明。由于给予代理服务的防火墙是在应用层实现的，所有它提供了较高的安全性和较强的身份验证功能。但是其透明性差，也离不开用户的合作。同时，它对网络性能的影响也较大。

应用网关技术是建立在网络应用层上的协议过滤，它针对特别的网络应用服务协议，即数据包分析并形成相关的报告。

3.1.2 防火墙的原理

防火墙是在专用网（Intranet）和 Internet 之间设置的安全系统，可以提供接入控制，可以干预这两个网络之间的任何消息传送。

（1）防火墙设计的基本原则

防火墙设计需要满足的基本原则如下：

①由内到外，或由外到内的业务流均经过防火墙；②只允许本地安全策略认可的业务流程通过防火墙；③尽可能控制外部用户访问专用网，应当严格限制外部人员进入专用网中；④具有足够的透明性，保证正常业务流通；⑤具有抗穿透攻击能力，强化记录、审计和报警功能。

（2）防火墙的组成

防火墙主要由 5 部分组成：即安全操作系统、过滤器、网关、域名服务和 E−mail 处理。有的防火墙可能在网关两侧设置内外过滤器。外过滤器保护网关不受攻击，而内过滤器在网关被攻破后提供对内部网络的保护。

安全操作系统可以保护防火墙的代码和文件免遭入侵者攻击；过滤器则执行由防火墙管理机构制定的一组规则，检验各数据组决定是否允许运行；应用网关可以在 TCP/IP 应用级上控制信息流和认证用户；域名访问使专用网的域名与 Internet 相隔离，专用网中主机的内部 IP 地址不至于暴露给 Internet 中的用户；函件处理能力保证专用网中用户和 Internet 用户之间的任何函件交换都必须经过防火墙处理。

（3）防火墙不能对付的安全威胁

首先，防火墙不能防止专用网内部用户对资源的攻击，它只是设在专用网和 Internet 之间，对其间的信息流进行干预的安全设施。

其次，如果专用网中有些资源绕过防火墙直接与 Internet 连通，则得不到防火墙的保护。

另外，从病毒防护来看，一般防火墙不对专用网提供防护外部病毒的侵犯。

（4）防火墙的分类

①分组过滤网关，按源地址和目的地址或业务（即端口号）卸包（组），并根据当前组的内容做出决定。管理者拟定一个提供接收和服务对象的清单，一个不接受访问或服务对象的清单，按所定安全政策实施允许或拒绝访问。

②应用级网关，在专用网和外部网之间建立一个单独的子网，它将内部网屏蔽起来。此子网有一个代理主机、一个路由器和一个较复杂的网关与内部网相连，另一个路由器和网关与外部相连。进出用户通过网关时必须在应用级上（要求特定的用户程序或用户接口）与代理主机连接 [3]。

③线路级网关，它使内部与外部网之间实现中继 TCP 连接。

3.1.3 防火墙产品

防火墙产品的用户主要分为个人用户、企业用户和政府部门用户。个人用户的安全需求基本上局限于防止网络病毒

 DOI: https://doi.org/10.36956/iser.v2i1.369

和“邮件炸弹”，一般的单机防火墙软件就能满足需求，而企业级用户和政府部门用户是安全产品最重要的应用对象。

（1）Checkpoint Firewall−1

Checkpoint 公司是一家专门措施网络安全产品开发的公司，是软件防火墙领域中的佼佼者，其旗舰产品 Checkpoint Firewall−1 在全球软件防火墙产品中位居第一。Checkpoint Firewall−1 是一个综合的、模块化的安全套件，它是一个基于策略的解决方案，提供集中管理、访问控制、授权、加密、网络地址传输、内容显示负载平衡等功能。其主要用在保护内部网络资源、保护内部进程资源和内部网络访问者验证等领域。

（2）Sonicwall 系列防火墙

Sonicwall 系列防火墙是 Sonic System 公司针对中小型企业需求开发的产品，并以其高性能和极具竞争力的价格受到中小企业和 ISP 公司的青睐 [4]。

（3）NetScreen 防火墙

NetScreen 公司推出的 NetScreen 防火墙是一种新型的网络安全硬件产品，把多种功能诸如流量控制、负载均衡、VPN 等集成到一起，优势在于采用了新的体系结构，可以有效地消除传统防火墙实现数据加盟时的性能瓶颈，能实现最高级别的 IP 安全保护。

（4）Alkatel intent Deices 系列防火墙

1999 年 6 月，阿尔卡特公司与 intent Deices 经过谈判达成协议，以 1.8 亿美元巨资收购 intent Deices 公司——一个业界具有重要地位的防火墙和 VPN 解决方案供应商。intent Deices 公司专门从事高性能计算机网络安全系统的设计、开发、销售和服务，其产品系列 intent Deices 1000/3000/5000 和 intent Deices 10K 分别适用于小型、中型、大型网络环境。其 中 intent Deices 3000>intent Deices 5000 及 intent Deices 10K 带有 VPN 功能，支持 VPN 用户。

（5）NAIGauntlet 防火墙

NAI 公司是全球著名的网络安全产品提供商，其产品包括网络检测、防火墙以及防病毒产品等。

3.4 虚拟专用网技术

虚拟专用网是用于 Internet 电子交易的一种专用网络，它可以在两个系统之间建立安全的通道，非常适合电子数据交换。在虚拟专用网中交易双方比较熟悉，而且彼此之间的数据通信量很大。只要交易双方取得一致，在虚拟专用网中就可以使用比较复杂的专用加密和认证技术，这样可以大大提高电子商务的安全性。

参考文献

[1] 庄建忠 . 计算机网络安全技术及策略浅析 [J]. 农业网络信息 ,2007 (08):91−93.

[2] 王宇光 . 计算机网络安全技术浅谈 [J]. 科技传播 ,2015,007 (021):114−115.

[3] 仉琦 , 缪超 , 张辉 . 计算机网络安全技术的影响因素与防范措施 [J]. 电脑迷 ,2017 (012):17.

[4] 罗小珠 . 浅析计算机网络安全的管理技术 [C]// 网络安全技术的开发应用学术会议论文集 .2002.