网络安全威胁与安全技术

空军第一航空学院

刘成林　杨文杰　王文良 冉 涛

河南省信阳市航空路２３号７０３＃

邮政编码：４６４０００

电话：（０３７６）６５７１１７１－５５９４１

网络安全威胁与安全技术

空军第一航空学院　　刘成林　杨文杰　王文良 冉 涛

摘要

本文主要介绍了网络安全的两个方面的内容，即安全威胁（进攻）与安全技术（防御）。

关键词：网络、安全、威胁、防御

网络已经成为人们日常工作和生活的一部分，给人们提供了前所未有便利和机遇。然而互联网是一个面向大众的、开放的网络，对于信息的保密和系统的安全考虑得并不完备，非法侵入、黑客攻击、保密性信息泄露等安全问题已经造成了巨大的损失。这给互连网的发展提出了一个严峻的挑战，应该充分重视并设法解决。网络的安全问题实际上包括两方面的内容，即安全威胁（进攻）与安全技术（防御）。

一、网络安全威胁

由于计算机系统本身就存在着种种安全性问题，互联网的安全问题就更为复杂，因为互联的设计使得攻击者可以在连接处进行破坏。网络的安全性主要包括三个方面：网络服务的可用性（Availability）、网络信息的保密性（Confidentiality）和网络信息的完整性（Integrity）。

目前，互联网络面临的安全威胁主要有以下几个方面：

1. 非法访问和破坏（“黑客”攻击）

操作系统总不免存在这样那样的漏洞，一些人就利用系统的漏洞，进行网络攻击，其主要目标就是对系统数据的非法访问和破坏。“黑客”攻击已有十几年的历史，黑客活动几乎覆盖了所有的操作系统，包括UNIX、Windows NT 、VM、VMS以及MVS。

2. 计算机病毒

计算机病毒程序很容易做出，有着巨大的破坏性，其危害已被人们所认识。单机病毒就已经让人们谈毒色变了，通过网络传播的病毒无论是在传播速度、破坏性和传播范围等方面都是单机病毒所不能比拟的。

3. 特洛伊木马（Trojan Horse）

特洛伊木马的名称来源于古希腊的历史故事。特洛伊程序一般是由编程人员编制，它提供了用户所不希望的功能，这些额外的功能往往是有害的。把预谋的功能隐藏在公开的功能中，可掩盖其真实企图。

4. 蠕虫（Worms）

蠕虫是一种子含的一个或一组程序，它可以从一台机器向另一台机器传播。它同病毒不一样，它不需要修改宿主程序就能传播。

5. 活板门（Trap Doors）

为攻击者提供“后门”的一段非法的操作系统程序。这一般是指一些内部程序人员为了特殊的目的，在所编制的程序中潜伏代码或保留漏洞。

6. 隐蔽通道

是一种允许违背合法的安全策略的方式进行操作系统进程间通信（IPC）的通道，又分隐蔽存储通道和隐蔽时间通道。隐蔽通道的重要参数是带宽。

7. 拒绝服务攻击（Denial Of Service Attack）

一种破坏性攻击，最早的拒绝服务攻击是“电子邮件炸弹”，它能使用户在很短的时间内收到大量电子邮件，使用户系统不能处理正常业务，严重时会使系统崩溃、网络瘫痪。

8. 泄露机密信息

包括两种情况：系统内部人员的泄露机密和外部人员通过非法手段截获机密信息。

而在所有的操作系统中，由于 UNIX系统的核心代码是公开的，这使其成为最易受攻击的目标。攻击者可能先设法登录到一台UNIX的主机上，通过操作系统的漏洞来取得特权，然后再以此为据点访问其余主机，这被称为“跳跃”（Island-hopping）。攻击者在到达目的主机之前往往会先经过几次

这种跳跃。这样，即使被攻击网络发现了攻击者从何处发起攻击，管理人员也很难顺次找到他们的最初据点，何况他们能在窃取某台主机的系统特权后，在退出时删掉系统日志。用户只要能登录到UNIX系统上，就能相对容易地成为超级用户。所以，如何检测系统自身的漏洞，保障网络的安全，已成为一个日益紧迫的问题。

二、网络安全技术

1. 身份验证

身份验证是一致性验证的一种，验证是建立一致性证明的一种手段。身份验证主要包括验证依据、验证系统和安全要求。身份验证技术是在计算机中最早应用的安全技术，现在也仍在广泛应用，它是互联网上信息安全的第一道屏障。

2. 存取控制

存取控制规定何种主体对何种客体具有何种操作权力。存取控制是网络安全理论的重要方面，主要包括人员限制、数据标识、权限控制、类型控制和风险分析。存取控制也是最早采用的安全技术之一，它一般与身份验证技术一起使用，赋予不同身份的用户以不同的操作权限，以实现不同安全级别的信息分级管理。

3. 数据完整性

完整性证明是在数据传输过程中，验证收到的数据和原来数据之间保持完全一致的证明手段。检查和是最早采用的数据完整性验证的方法，它虽不能保证数据的完整性，只起到基本的验证作用，但由于它的实现非常简单（一般都由硬件实现），现在仍广泛应用于网络数据的传输和保护中。近几年来研究比较多的是数据摘压算法和数字签名算法，它们虽可以保证数据的完整性，但由于实现起来比较复杂，系统开销比较大，一般只用于完整性要求较高的领域，特别是商业、金融业等领域。

4. 数据机密性

机密性由加密算法保证。现在金融系统和商界普遍使用的算法是美国数据加密标准DES。Internet免费提供PGP系统。近几年来我国对加密算法的研究主要集中在密码强度分析和实用化研究上。

5. 防火墙技术

防火墙是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，用于确定哪些内部服务允许外部访问，以及允许访问哪些外部服务。

（1）防火墙技术的发展

早期的防火墙主要起屏蔽主机和加强访问控制的作用，现在的防火墙则逐渐集成了信息安全技术中的最新研究成果，一般都具有加密解密和压缩解压等功能，这些技术增加了信息在互联网上的安全性。现在，防火墙技术的研究已经成为网络信息安全技术的主导研究方向。

（2）现有防火墙的局限性

防火墙不能防范人为因素的攻击。防火墙不能防止由内奸或用户误操作造成的威胁,以及由于口令泄露而受到的攻击。

防火墙不能防止受病毒感染的软件或文件的传输。由于操作系统、病毒、二进制文件类型(加

密、压缩)的种类太多且更新很快,所以防火墙无法逐个检查每个文件以查找病毒。

防火墙不能防止数据驱动式的攻击。当有些表面看来无害的数据邮寄或拷贝到内部网的主机上并被执行时,可能会发生数据驱动式的攻击。例如,一种数据驱动式的攻击可以使主机修改与系统安全有关的配置文件,从而使入侵者下一次更容易攻击该系统。

防火墙不能防范不经由防火墙的攻击。例如，如果允许从受保护网内部不受限制的向外拨号，一些用户可以形成与Internet的直接的SLIP或PPP连接。从而绕过防火墙，造成一个潜在的后门攻击渠道。

现在防火墙技术的研究主要集中在已有系统的完善和突破现有技术的局限性上。

总的来说，防火墙只是一种整体安全防范政策的一部分。这种安全政策必须包括公开的，以便用户知道自身责任的安全准则、职员培训计划以及与网络访问、当地和远程用户认证、拨出拨入呼叫、磁盘和数据加密以及病毒防护的有关政策。网络易受攻击的各个点必须以相同程度的安全防护措施加以保护。在无全面的安全政策的情况下设置Internet防火墙，就形同在一顶帐篷上装置一个防盗门。

6. 安全协议

安全协议的建立和完善是安全保密系统走上规范化、标准化道路的基本因素。一个较为完善的内部网和安全保密系统，至少要实现加密机制、验证机制和保护机制。

网络安全技术成为当今热门技术之一。Internet 安全性领域不是一成不变的，它的发展变化非常迅速，同时各种反攻击系统也在不断完善，已成为提高网络系统安全性的利器。

作者简介：刘成林，男，１９６６年生，本科，空军第一航空学院讲师，研究方向为计算机与网络技术、新型飞机电气技术等，制作了多套多媒体软件、课件和模拟器，曾获军队科技进步二、三等奖等奖励。

杨文杰，男，１９６３年生，本科，空军第一航空学院副教授，研究方向为计算机控制技术、新型飞机电气技术等，承担了多项重大科研项目，曾获军队科技进步二、三等奖等奖励多项。

王文良，男，１９６２年生，本科，空军第一航空学院副教授，研究方向为计算机控制技术、新型飞机电气技术等，承担了多项重大科研项目，曾获军队科技进步二、三等奖等奖励多项。

冉 涛，男，1969年生，本科，空军第一航空学院助教，现代教育技术应用，制作多部电教片和多媒体软件曾获全军电教教才评比一、二等奖。