现代计算机技术与应用
2022 年 8 月第 4 卷第 3 期

浅析计算机网络安全

王　勇

辽宁农业职业技术学院，营口

摘　要 | 计算机的普及使用和网络应用的广泛深入，使得计算机网络安全问题变得日益复杂和突出。本文分析了当前计算机网络安全现状和安全威胁产生的原因及方式，随后对主要的网络安全技术进行了论述。

关键词 | 网络安全；影响网络安全的主要因素；网络安全技术

随着计算机的普及和网络应用的日趋广泛，计算机网络已经进入政治、经济、军事、文化、教育等各个社会领域，给整个人类社会的发展造成了深远影响。但是随之而来的网络安全问题变得日益复杂和突出。由于网络本身的开放性和网络系统内潜在的漏洞，使其受到威胁和攻击的可能性大大增加。因此，增强网络安全意识，防范不明身份的入侵者，保证网络信息安全，显得尤为重要。

1　什么是计算机网络安全

计算机网络安全包含两方面的内容——系统安全和信息安全，系统安全

作者简介：王勇，辽宁农业职业技术学院助教。
文章引用：王勇．浅析计算机网络安全［J］．现代计算机技术与应用，2022，4（3）：97–102.
https://doi.org/10.35534/mcta.0403014c

主要是指网络硬件设备、操作系统和应用软件的安全。信息安全主要指各种信息的存储、传输的俺去，具体体现在保密性、完整性及数据的可用性和可控性。

2　影响网络安全的主要因素

（1）TCP/IP 协议本身的缺陷

目前世界上所有的计算机网络都是基于 TCP/IP 协议的。由于 TCP/IP 协议在设计之初只是用于范围很小的几台计算机之间的通信，它的前提是相信每个计算机用户的安全性和合法性，因此，TCP/IP 协议在安全性方面存在先天缺陷。如今，接入 INTERNET 的计算机数以亿计，许多居心不良的计算机使用者就利用了 TCP/IP 协议在安全性方面的缺陷来进行网络攻击。

（2）黑客攻击

目前世界上所有的计算机网络都是基于 TCP/IP 协议的。由于 TCP/IP 协议在设计之初只是用于范围很小的几台计算机之间的通信，它的前提是相信每个计算机用户的安全性和合法性，因此，TCP/IP 协议在安全性方面存在先天缺陷。如今，接入 INTERNET 的计算机数以亿计，许多居心不良的计算机使用者就利用了 TCP/IP 协议在安全性方面的缺陷来进行网络攻击。

（3）病毒

计算机病毒是指为了某种目的而蓄意编制的计算机程序，它能在实际系统中生存，自我复制和传播。并且给计算机系统造成严重的损坏。病毒一直是计算机系统安全最主要的威胁之一，它可以通过各种移动存储设备、文件传输、电子邮件、网络下载等方式传播，网络硬件、软件的迅猛发展更是增加了病毒迅速传播的途径。一旦病毒发作，可能会造成文件丢失，系统运行缓慢甚至系统崩溃，硬件损坏等可怕的后果。

（4）系统漏洞

各种各样的操作系统和应用软件为我们管理和使用计算机带来了许多方便，但是任何一个操作系统或应用软件都不可能是百分之百的无缺陷、无漏洞的，这就给黑客入侵和病毒攻击留下了可乘之机，大多数的黑客和病毒都是利用了

系统的“漏洞”来进行攻击的。另外，有时候编程人员在开发软件时出于这样或那样的动机在软件中留下“后门”，这些“后门”就成了软件的“软肋”，很容易成为整个网络系统受攻击的首选目标和薄弱环节。

3 目前主要的网络安全技术

为了应对日新月异的网络安全挑战，网络安全技术也不断向前发展，目前主要的网络安全技术有：加密技术、认证技术、防火墙技术和入侵检测技术。

3.1 加密技术

数据加密技术是保障网络安全的最基本、最核心的技术措施，是信息安全的基础，是保证网络安全最直接、最有效的一种方法，其目的是保护网内的数据、文件、口令和各种控制信息，防止窃听。加密技术按照密钥的归属不同可以分为对称加密技术和非对称加密技术两种。对称加密技术指加密和解密均采用相同的或者类似的密钥。它的优点是加密和解密的算法都比较简洁，速度快，但缺点是安全性较弱。非对称加密技术指加密和解密所用的密钥不同。加密密钥又称为公钥，它是公开的，任何人都可以使用它加密数据；解密密钥又称为私钥，它是保密的，只有接收者才知道私钥，经过公钥加密的文件必须用相应的私钥才能解密。非对称加密算法的优点是可以很好地适应网络开放性的特点，避免了密钥在传递过程中泄露的危险，但缺点是加密速度慢，消耗系统的资源比较多。

3.2 认证技术

认证技术是信息安全理论与技术的一个重要方面，使用认证技术可以防止数据被非法访问及被篡改。它主要包括信息认证与身份认证两个方面的内容，其中身份认证用于鉴别用户身份，限制非法用户访问网络资源；信息认证又称为报文鉴别，是指对信息实施加密传输与验证。它的主要目的是用来检验数据的真实性和完整性，信息认证是建立在身份认证的基础上的。要实现认证功能，需要多种认证技术相互配合才能完成，主要的认证技术有消息摘要、数字签名、

https://doi.org/10.35534/mcta.0403014c

数字信封等。

3.3 防火墙技术

防火墙是位于两个（或多个）网络之间执行安全策略的一组组件的集合。它包括硬件和软件，设置防火墙的目的是保护内部网络资源不被外部非授权用户使用，防止内部网络受到外部非法用户的攻击。

防火墙技术是一种网络访问控制技术，它对两个或多个网络之间传输的数据包的信息如链接方式按照一定的安全策略来实施检查，以决定网络之间的通信是否被允许，并监视网络运行状态。常用的防火墙技术主要有：分组过滤技术、代理服务技术和网络地址转换（NAT）技术。

3.4 入侵检测系统

入侵检测即是对入侵行为的发觉。它通过收集和分析计算机网络或计算机系统中若干关键点的信息，检查网络或系统中是否存在违反安全策略的行为和被攻击的迹象。作为一种重要的安全技术，作为对防火墙的一种合理补充，入侵检测不仅能够揪出系统入侵者的非授权使用，同时也能够识别系统合法用户的滥用行为。进行入侵检测的软件与硬件的组合便是入侵检测系统，它的主要功能有以下几个方面：监控、分析用户和系统的一切活动；检查系统配置及薄弱环节；分析异常活动；对操作系统进行审计；对关键系统及数据文件进行完整性评估。

一般的，入侵检测系统由数据提取、数据分析和结果处理三个功能模块组成，它的工作原理如下：首先，数据收集模块从主机上的日志信息、变动信息，网络上的数据信息，甚至是流量变化等系统的不同环节收集数据，并对这些数据进行简单的处理，如简单的过滤、数据格式的标准化等，而后，将经过处理的数据提交给数据分析模块。数据分析模块是整个入侵检测系统的核心，它通过分析数据特征来判断此活动是否为入侵，并根据分析的结果产生事件，传递给结果处理模块。结果处理模块根据预定的策略对检测到的行为及时地做出响应，包括切断网络连接、纪录并报告检测过程结果等。

4 网络安全新技术——主动防御技术

在以上四种网络安全技术中，密码技术和认证技术都是保证网络安全最基础，最重要的技术，无论网络安全技术如何发展，这两者的地位无可取代。在这基础之上的防火墙技术和入侵检测技术虽然各有所长，能够在一定程度上抵御黑客和病毒攻击，但各自都存在缺陷。比如，防火墙对于网络内部或者系统内部的攻击无能为力，而入侵检测技术对于目前日新月异、层出不穷的各种攻击无法在第一时间识别并及时、正确的处理。这些，都对网络安全技术提出了更高的要求。在传统安全技术的基础上，以主动防御技术为核心的入侵防御系统（IPS）随之诞生。

入侵防御系统（IPS）是一种主动的、积极的入侵防范、阻止系统。不仅能实现检测攻击，还能有效阻断攻击，提供深层防护，注重主动防御。IPS 部署在网络的进出口处，当检测到攻击企图后，它会自动地将攻击包丢掉或采取措施将攻击源阻断，其设计宗旨是预先对入侵活动和攻击性网络流量进行拦截，避免其造成损失，而不是简单地在恶意流量传送时或传送后才发出警报。IPS 通过一个网络端口接收来自外部系统的流量，经过检查确认其中不包含异常活动或可疑内容后，再通过另外一个端口将它传送到内部系统中，这样，有问题的数据包以及所有来自同一数据流的后续数据包，都能在 IPS 设备中被清除掉。IPS 在网络边界检查到攻击包的同时将其直接抛弃，则攻击包将无法到达目标，从而可以从根本上避免黑客的攻击。

5 总结

网络安全是一个综合性的课题，它所需要的知识涉及物理、数学、生物学和计算机科学等多个学科，不是靠一两种网络技术就能够解决的。想保证网络的绝对安全是不可能的，但是要最大限度地阻击各种网络入侵，就需要各种网络安全技术共同协作，构筑防御系统。目前，各种网络安全硬件、软件的开发都已经取得了很大成绩，接下来，我们还需要在构筑网络安全体系、完善安全协议等几个方面继续开展研究。

https://doi.org/10.35534/mcta.0403014c

参考文献

［1］翟军．计算机网络安全分析与探讨［J］．科技信息，2006（S4）：22.
［2］吴钰锋，刘泉，李方敏．网络安全中的密码技术研究及其应用［J］．真空电子技术，2004（6）：19–21.
［3］李春旺．网络环境下信息安全认证［J］．图书馆杂志，2003（2）：25–27，32.

Analysis of Computer Network Security

Wang Yong

Liaoning Agricultural Vocational and Technical College, Yingkou

Abstract: The popularization of the use of computers and the extensive and in-depth network applications, making the computer network security problems become increasingly complex and prominent. This paper analyzes the current situation of computer network security and security threats and the causes and ways, and then discusses the main network security technology.

Key words: Network security; The main factors affecting network security; Network security technology