计算机网络安全研究

作者：浙江财经学院东方学院　黄俊

［摘要］随着信息技术的飞速发展，网络及网络信息安全技术已经影响到社会的政治、经济、文化和军事等各个领域。网络技术的成熟使得网络连接更加容易，人们在享受网络带来便利的同时，网络的安全也日益受到威胁。

［关键词］网络安全；　网络技术；　网络管理

一、网络安全含义及特征

网络安全从其本质上讲就是网络上的信息安全，指网络系统的硬件、软件及数据受到保护。不遭受偶然的或者恶意的破坏、更改、泄露，系统连续可靠正常地运行，网络服务不中断。从用户的角度，他们希望涉及到个人隐私和商业利益的信息在网络上传输时受到机密性、完整性和真实性的保护，避免其他人或对手利用窃听、冒充、篡改、抵赖等手段对自己的利益和隐私造成损害和侵犯。同时他们希望自己的信息保存在某个计算机系统上时，不受其他非法用户的非授权访问和破坏。从网络运营商和管理者的角度来说，他们希望对本地网络信息的访问、读写等操作受到保护和控制，避免出现病毒、非法存取、拒绝服务和网络资源的非法占用和非法控制等威胁，制止和防御网络“黑客”的攻击。

网络安全根据其本质的界定，应具有以下基本特征：1、机密性。是指信息不泄露给非授权的个人、实体和过程，或供其使用的特性。在网络系统的各个层次上都有不同的机密性及相应的防范措施。在物理层，要保证系统实体不以电磁的方式向外泄露信息，主要的防范措施是电磁屏蔽技术、加密干扰技术等，在运行层面，要保障系统依据授权提供服务，使系统任何时候都不被非授权人使用，对黑客入侵、口令攻击、用户权限非法提升、资源非法使用等采取漏洞扫描、隔离、防火墙、访问控制、入侵检测、审计取证等防范措施。在数据处理、传输层面，要保证数据在传输、存储过程中不被非法获取、解析，主要防范措施是数据加密技术。2、完整性。是指信息未经授权不能被修改、不被破坏、不被插入、不延迟、不乱序和不丢失的特性。对网络信息安全进行攻击其最终目的就是破坏信息的完整性。在运行曾面，要保证数据在传输、存储等过程中不被非法修改。要保证数据的发送源头不被伪造，对冒充信息发布者的身份、虚假信息发布来源采取身份认证技术、路由认证技术，这类属性也称为真实性。3、可用性。是指合法用户访问并能按要求顺序使用信息的特性，即保证合法用户在需要时可以访问到信息及相关资料。在物理层，要保证信息系统在恶劣的工作环境下能正常进行，主要防范措施是对电磁炸弹、信号插入采取抗干扰技术、加固技术等。在运行层面，要保证系统时刻能为授权人提供服务，对网络被阻塞、系统资源负荷消耗、病毒、黑客等导致系统崩溃或死机等情况采取过载保护、防范拒绝服务攻击、生存技术等防范措施。保证系统的可用性，使得发布者无法否认所发布的信息内容。接受者无法否认所接收的信息内容，对数据抵赖采取数字签名。

二、网络安全现状分析

随着计算机和通信技术的发展，网络信息的安全和保密已成为一个至关重要且急需解决的问题。计算机网络所具有的开放性、互连性和共享性等特征使网上信息安全存在着先天不足，再加上系统软件中的安全漏洞以及所欠缺的严格管理，致使网络易受黑客、恶意软件的攻击，因此针对网络的安全所采取的措施应能全方位地针对各种不同的威胁，保障网络信息的保密性、完整性和可用性。现有网络系统和协议还是不健全、不完善、不安全的；有的思想麻痹，没有清醒的意识到黑客入侵会导致严重的后果，有的没投入必要的人力、财力和物力来加强网络的安全性；没有采用正确的安全策略和安全机制；缺乏先进的网络安全技术、

工具、手段和产品；有的尚缺乏先进的灾难恢复措施和悲愤意识等。

网络安全是研究与计算机科学相关的安全问题，具体地说，网络安全研究了安全的存储、处理或传输信息资源的技术、体制和服务的发展、实现和应用。每个计算机离不开人，网络安全不仅依赖于技术上的措施，也离不开组织和法律上的措施。客户/服务器计算模式下的网络安全研究领域，一是 OSI 安全结构定义的安全服务：鉴别服务、数据机密性服务、数据完整性服务、访问控制服务、不可抵赖服务。二是 OSI 安全结构定义的安全机制：加密、数字签名机制、访问控制机制、数据完整性机制、鉴别交换机制、通信填充机制、路由控制机制、公证机制、可信功能、安全标签、事件检测、安全审查跟踪、安全恢复。三是访问控制服务：从逻辑上划分网络，并实际控制对这些网络的访问。访问控制服务中的关键安全技术有静态分组过滤、动态分组过滤、链路层网关、应用层网关。四是通信安全服务：用语保护这些网络间的通信。OSI 结构通信安全服务包括鉴别、数据机密性和完整性，以及不可抵赖服务。五是网络存活性：目前对 Internet 存活性的研究目的是开发一种能保护网络和分布式系统免遭拒绝服务攻击的技术和机制。

三、网络安全解决方案

网络安全是一项动态、整体的系统工程，从技术上来说，网络安全有安全的操作系统、应用系统、防病毒、防火墙、入侵检测、网络监控、信息审计、通信加密、灾难恢复、安全扫描等多个安全组件组成，一个单独的组件是无法确保信息网络的安全性。1、防病毒技术。 网络中的系统可能会受到多种病毒威胁，为了免受病毒所造成的损失，可以采用多层的病毒防卫体系。即在每台计算机安装单机版反病毒软件，在服务器上安装基于服务器的反病毒软件，在网关上安装基于网关的反病毒软件。做到每台计算机不受病毒的感染，从而保证整个企业网不受病毒的感染。由于病毒在网络中存储、传播、感染的方式各异且途径多种多样，故相应地在构建网络防病毒系统时，应利用全防卫的企业防毒产品，实施层层设防、集中控制、以防为主、防杀结合的策略。2、防火墙技术。防火墙技术是近年发展起来的重要网络安全技术，其主要作用是在网络入口处检查网络通信，根据用户设定的安全规则，在保护内部网络安全的前提下，保障内外网络通信。在网络出口处安装防火墙后，防火墙可以对内部网络和外部网络进行有效的隔离，所有来自外部网络的访问请求都要通过防火墙的检查，提高内部网络的安全。防火墙可以完成具体任务：通过源地址过滤，拒绝外部非法 IP 地址，有效的避免了外部网络上与业务无关的主机越权访问；可以只保留有用的服务，将其他不需要的服务关闭，这样做可以将系统受攻击的可能性降低到最小限度，使黑客无机可乘；制定访问策略，只有被授权的外部主机才可以访问内部网络的有限 IP 地址，保证外部网络只能访问内部网络中的必要资源，与业务无关的操作将被拒绝；由于安装防火墙后，网络的安全策略由防火墙集中管理，黑客无法通过更改某一台主机的安全策略来达到控制其他资源访问权限的目的，而直接攻击防火墙是不可能的。3、入侵检测技术。入侵检测系统是近年出现的新型网络安全技术，目的是提供实时的入侵检测及采取相应的防护手段，如记录证据用于跟踪和恢复、断开网络连接等。实时入侵检测能力之所以重要，是因为它能够对付来自内外网络的攻击。如在需要保护的主机网段上安装了入侵检测系统，可以实时监视各种对主机的访问要求，并及时将信息反馈给控制台，这样全网任何一台主机受到攻击时系统都可以及时发现。4、安全扫描技术。这是又一类重要的网络安全技术。安全扫描技术与防火墙、入侵检测系统互相配合，能够有效提高网络的安全性。通过对网络的扫描，网络管理员可以了解网络的安全配置和运行的应用服务，及时发现安全漏洞，客观评估网络风险等级。网络管理员可以根据扫描的结果更正网络安全漏洞和系统中的错误配置，在黑客攻击前进行防范。如果说放火墙和网络监控系统是被动的防御手段，那么安全扫描就是一种主动的防范措施，可以有效避免黑客攻击行为，做到防患于未然。安全扫描工具源于黑客在入侵网络系统时所采用的工具，商品化的安全扫描工具为网络安全漏洞的发现提供了强大的支持。5、网

络安全紧急响应体系。网络安全作为一项动态工程，意味着它的安全程度会随着时间的变化而发生变化。在信息技术日新月异的今天，需要随着时间和网络环境的变化或技术的发展而不断调整自身的安全策略，并及时组建网络安全紧急响应体系，专人负责，防范安全突发事件。

四、网络安全管理

网络安全管理是指对所有计算机网络应用体系中各个方面的安全技术和产品进行统一的管理和协调，进而从整体上提高整个计算机网络的防御入侵、抵抗攻击的能力体系。通常，建立一个安全管理系统包括多个方面的建设，如技术上实现的计算机安全管理系统，为系统定制的安全管理方针，相应的安全管理制度和人员等。最初人们对网络安全的普遍认识是单点式的、分散的安全管理。一个系统中采用各类不同的安全设施实现不同的安全功能，而这些设备需要分别采用不同的软件和方法进行配置和管理，目前大部分单个的网络安全管理工具比较分散，各个安全功能需要分别进行配置，不同的管理工具之间缺乏连通性，但是由各种技术和产品构成的系统日益复杂，例如，IDS 系统要采用厂商的控制端软件实现系统状态监控，身份验证系统需要采用相应的控制中心进行管理。管理员如果要实现一个整体安全策略需要对不同的设备分别进行设置，并根据不同设备的日志和报警信息进行管理，难度较大，特别是在全局安全策略需要进调整时，很难考虑周全和实现全局的一致性。目前而言系统管理人员普遍需要的是具备自动响应能力的综合管理体系。

网络管理的趋势是向分布式、智能化和综合化方向发展。1、基于 Web 的管理。www 以其能简单、有效地获取如文本、图形、声音与视频等不同类型的数据在 Internet 上广为使用。作为一种全新的网络管理模式，基于 Web 的网络管理 WBM 应运而生。WBM 提供给普通拥护非常熟悉的 Web 浏览器的单一用户借口，以实现透明地访问分布在 Internet 上的各类信息，并且很容易支持大多数现有的标准网络管理协议框架。2、基于 CORBA 的管理。公共对象请求代理体系结构 CORBA 是由对象管理小组为开发面向对象的应用程序提供的一个通用框架结构。3、采用 Java 技术管理。Java 用于异购分布式网络环境的应用程序开发，它提供了一个易移植、安全、高性能、简单、多线程和面向对象的环境，实现“一次编译，到处运行”。将 Java 技术集成至网络管理，可以有助于克服传统的纯 SNMP 的一些问题，降低网络管理的复杂性。

总之，计算机技术和网络技术已深入到社会的各个领域，人类社会各种活动对计算机网络的依赖程度已经越来越大。增强社会安全意识教育，普及计算机网络安全教育，提高计算机网络安全技术水平，改善计算机网络的安全现状，成为当务之急。

[参考文献]

[1]张世永 .《网络安全原理与应用》. 科学出版社
[2]李明之. 《网络安全与数据完整性指南》. 机械工业出版社
[3]张仕斌. 《网络安全技术》. 清华大学出版社