网络信息安全与防范技术

何万敏

(福建水利电力职业技术学院 福建永安 366000)

摘要: 随着现代信息技术的发展和应用, 网络安全问题日益突出。本文概要地介绍了网络信息安全的内容、网络信息安全存在的隐患, 同时介绍了当前网络采用的各种安全防范技术。

关键词: 信息安全; 安全隐患; 安全防范技术

随着计算机和通讯技术的发展, 计算机网络已成为全球信息基础设施的主要组成部分。它为人们交换信息, 促进科学、技术、文化、教育、生产的发展带来了深刻的影响。同时, 网络信息的安全和保密已成为一个至关重要并急需解决的问题。人们对信息的安全传输、安全存储、安全处理的要求越来越显得十分迫切和重要。

一、网络信息安全的内容

计算机网络信息安全是指利用网络管理控制和技术措施, 防止网络本身及网上传输的信息财产被故意的或偶然的非授权泄漏、更改、破坏, 或使网上传输的信息被非法系统辨认、控制。即确保网上传输信息的完整性、保密性、可用性受到保护。其内容大致包括四个方面:

1. 网络实体安全。计算机房的物理条件、物理环境及设施的安全。计算机硬件、附属设备及网络传输线路的安全及配置等件安全。

2. 保护网络系统不被非法侵入, 系统软件与应用软件不被非法复制, 不受病毒的侵害等。

3. 网络中的数据安全。保护网络信息数据安全、数据库系统的安全, 保护其不被非法存取, 保护其完整、一致等。

4. 网络安全管理。运行时突发事件的安全处理, 包括采取计算机安全技术, 建立安全管理制度, 开展安全审计, 进行风险分析等内容。

二、网络信息安全的隐患

网络系统既要开放, 又要安全, 以至于网络安全问题已成为网络应用的焦点问题, 影响网络信息安全的隐患主要来自于网络硬件和网络软件两方面的不安全因素:

1. 计算机病毒。计算机病毒是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。

Internet 的广泛发展, 加速了病毒的传播速度和广度, 本地化和地域化的新病毒随着国家、地区间信息的频繁往来交流, 将上升为全球性病毒。病毒通过 Internet 传播的方式有两种: 一是来自文件下载, 二是来自电子邮件。

2. 人为的恶意攻击。人为的恶意攻击分为两种。一种是主动攻击, 它是以各种方式有选择地破坏信息的有效性、完整性和真实性, 目的在于篡改系统中所含信息, 或者改变系统状态; 另一种是被动攻击, 此类攻击主要威胁信息的保密性, 导致机密数据的泄漏。

3. 网络系统软件自身的安全问题。网络系统软件的自身安全与否直接关系网落安全, 网络软件的功能较少或不全, 是" 黑客 进行攻击的首选目标。

4. 非授权访问。非授权访问指那些预先没有经过同意就使用网络或计算机资源, 如有意避开系统访问控制机制, 对网络设备及资源进行非正常使用或擅自扩大权限, 从而对系统和网络进行非法访问。

5. 传输线路安全与质量问题。信息在传输中和存储介质中易发生有意或无意被泄漏出去或丢失的现象。当线路的质量不太好时, 可能会严重危害通信数据的完整性; 另外, 黑客们常采用窃听方式, 对通信线路中传输的信号进行搭线监听, 截获有用的机密信息等。

6. 破坏数据完整性。破坏数据完整性分为两种: 一是来自非法用户的攻击, 即通过改变信息的标签、内容和属性, 达到用假信息代替原始信息目的。二是来自合法用户的攻击, 即抵赖。

7. 拒绝服务攻击。它不断对网络服务系统进行干扰, 改变其正常的作业流程, 执行无关程序, 使系统响应减慢甚至瘫痪, 影响正常用户的使用。

8. 网络安全管理问题。现有的信息系统大多数缺少安全管理员, 缺少信息系统安全管理的技术规范, 缺少定期安全测试与检查, 更缺少安全审计。随着计算机及通信设备组件数目的增大, 积累起来的安全问题将越来越复杂。

三、网络安全防范技术

1. 防火墙技术

作为加强网络间访问控制的网络互连设备, 防火墙是在内部网与外部网之间实施安全防范的系统, 它保护内部网络免受非法用户的侵入, 过滤不良信息, 防止信息资源的未授权访问。防火墙是一种基于网络边界的被动安全技术, 对内部未授权访问难以有效控制, 因此较适合于内部网络相对独立, 且与外部网络的互连途径有限、网络服务种类相对集中的网络。防火墙的实现技术主要有: 数据包过滤, 应用网关和代理服务等。

(1) 包过滤技术。依据系统内事先设定的过滤逻辑, 检查数据流中每个数据包, 根据数据包的源地址、目的地址、所有的 TCP 端口与 TCP 链路状态等实施有选择地通过。包过滤技术的实现方式有: 路由设备除完成路由选择的数据转发外, 还进行包过滤, 这是较常用的方式; 在工作站上使用软件进行包过滤, 价格较贵, 在屏蔽路由器上启动包过滤功能。

包过滤技术的优点是简单实用, 实现成本较低, 在应用环境比较简单的情况下, 能够以较小的代价在一定程度上保证系统的安全。但包过滤技术的缺陷也是明显的, 包过滤技术是一种完全基于网络的安全技术, 只能根据数据包的来源、目标和端口等网络信息进行判断, 无法识别基于应用层的恶意侵入。

(2) 应用网关技术。基于应用层协议, 利用特别的网络应用服务协议分析过滤数据包, 并形成相关的报告。应用网关一般运行在专用工作站上, 对易登录、控制的网络系统实施严格控制, 确保网络安全。

(3) 代理服务(ProxyServer) 技术。防火墙网关上建立的专用代码由服务器端程序和客户端程序组成, 客户端程序与代理服务连接, 代理服务与将访问的外部服务器连接。与包过滤技术和应用网关技术不同, 代理服务技术的内部网与外部网间不存在直接连接, 实现了防火墙内外计算机系统的隔离, 同时, 代理服务技术可实施较强的数据流监控、过滤、日志(Log) 和审计(Audit) 等服务。

从理论上讲, 防火墙是系统管理员能够采取的最严格的安全措施, 但使用防火墙对网络将带来不利影响。表现在: 防火墙严格的安全性削弱了有用的网络服务功能, 无法防护内部网络用户的攻击, 无法防范通过防火墙以外的其他途径的攻击, 不能完全防止传送已感染病毒的软件或文件, 无法防范数据驱动型的攻击, 另外防火墙不能防备新的网络安全问题。因此, 为了保护重要数据, 建议不要使用单一的安全措施。

2. 数据加密技术

数据加密技术作为主动网络安全技术, 是提高网络系统数据的保密性、防止秘密数据被外部破析所采用的主要技术手段, 是许多安全措施的基本保证。加密后的数据能保证在传输、使用和转换时不被第三方获取。数据加密技术可以分为三类: 对称型加密、不对称型加密和不可逆加密。

(1) 对称型加密。使用单个密钥对数据进行加密或解密, 其特点是计算量小、加密效率高。但是此类算法在分布式系统上使用较为困难, 主要是密钥管理困难, 使用成本较高, 保密性能也不易保证。这类算法的代表是在计算机专网系统中广泛使用的 DES(DigitalEncryptionStandard) 算法。

(2) 不对称型加密算法。也称公用密钥算法, 其特点是有两个密钥(即公用密钥和私有密钥), 只有二者搭配使用才能完成加密和解密的全过程。由于不对称算法拥有两个密钥, 特别适用于分布式系统中的数据加密, 在 Internet 中得到广泛应用。其中公用密钥在网上公布, 为数据源对数据加密使用, 而用于解密的相应私有密钥则由数据的接收方妥善保管。不对称加密的另一用法称为" 数字签名(Digitals ignature) , 即数据源使用其密钥对数据的校验和(ChenckSum) 或其他与数据内容有关的变量进行加密, 而数据接收方则用相应的公用密钥解读" 数字签名 , 并将解读结果用于对数据完整性的检验。在网络系统中得到应用的不对称加密算法有 RSA 算法和美国国家标准局提出的 DSA 算法(DigitalSignatureAlgorithm) 。不对称加密法在分布式系统中应用时需注意的问题, 是如何管理和确认公用密钥的合法性。

(3) 不可逆加密。不可逆加密算法的特征是加密过程不需要密钥, 并且经过加密的数据无法被解密, 只有同样的输入数据经过同样的不可逆加密算法才能得到相同的加密数据。不可逆加密算法不存在密钥保管和分发问题, 适合在分布网络系统上使用, 但是其加密计算工作量相当可观, 所以通常用于数据量有限的情形下的加密, 如计算机系统中的口令就是利用不可逆算法加密的。近来随着计算机系统性能的不断改善, 不可逆加密的应用逐渐增加。

3. 网络安全漏洞扫描技术

漏洞扫描是自动检测远端或本地主机安全脆弱点的技术。它查询 TCP/ IP 端口, 并记录目标的响应, 收集关于某些特定项目的有用信息, 如正在进行的服务, 拥有这些服务的用户是否支持匿名登录, 是否有某些网络服务需要鉴别等。这项技术的具体实现就是安全扫描程序。扫描程序是一个强大的工具, 它可以用来为审计收集初步的数据。在任何一个现有的平台上都有几百个熟知的安全脆弱点, 人工测试单台主机的这些脆弱点要花几天的时间, 而扫描程序可在很短的时间内就能解决这些问题。扫描程序开发者利用可得到的常用攻击方法, 并把它们集成到整个扫描中, 输出的结果格式统一, 容易参考和分析。

4. 网络入侵检测技术

试图破坏信息系统的完整性、机密性、可信性的任何网络活动, 都称为网络入侵。入侵检测(IntrusionDeteetion) 的定义为: 识别针对计算机或网络资源的恶意企图和行为, 并对此作出反应的过程。它不仅检测来自外部的入侵行为, 同时也检测来自内部用户的未授权活动。入侵检测应用了以攻为守的策略, 它所提供的数据不仅有可能用来发现合法用户滥用特权, 还有可能在一定程度上提供追究入侵者法律责任的有效证据。

入侵检测通常采用 IDS。所谓 IDS 就是一个能够对网络活动进行实时监测的系统, 它能够发现并报告网络中存在的可疑迹象, 为网络安全管理提供有价值的信息。从入侵检测基于的技术来划分, IDS 可以划分为两类: 基于知识的入侵检测和基于行为的入侵检测。现在, 大多数的 IDS 产品综合采用三个基本方法来检测网络入侵: 追踪分析、网包分析及实时活动监控。

5. 其它防范措施

(1) 备份和镜像技术。用备份和镜像技术提高完整性。备份技术是最常用的提高数据完整性的措施, 它是指对需要保护的数据在另一个地方制作一个备份, 一旦失去原件还能使用数据备份。镜像技术是指两个设备执行完全相同的工作, 若其中一个出现故障, 另一个仍可以继续工作。

(2) 防病毒技术。为使计算机系统免遭病毒的威胁, 除了建立完善的管理措施之外, 还要有病毒扫描、检测技术, 病毒分析技术, 软件自身的防病毒技术, 系统防病技术, 系统遭病毒破坏后的数据恢复技术, 以及消除病毒的工具及其技术等。

四、结 语

因特网的安全是一项复杂的长期性的系统工程, 不是单一的产品和技术可以完全解决的。这是因为网络安全包含多个层面, 既有层次上的划分、结构上的划分, 也有防范目标上的差别, 层次上涉及到网络层、传输层、应用层的安全等, 在结构上不同结点考虑的安全是不同的。制定适当完备的网络安全策略是实现网络安全的前提, 高水平的计算机网络安全技术是保证, 严格的管理落实是保证。

参考文献:

! 刘 娜、王巍、李可∀入侵检测技术概论#. 中国数据通信, 2004, 1.

刘 宏毅∀分析与探讨网络信息安全与防范技术#. 现代情报, 2004, 4.

% 王 斌∀浅析计算机网络的安全#. 河南职业技术师范学院学报, 2004, 6.

&陈兵∀网络安全与电子商务#. 北京. 北京大学出版社. 2002.