●智 勇 黄 奇

网络环境下的信息安全

摘 要 如何保证网络环境下的信息安全已成了急待解决的重要问题。信息安全整体模型应包括安全策略、防护、检测和响应四部分。一种新的信息安全模型,是一个动态模型,引入了时间概念,而且对如何实现系统安全并评价安全状态,给出了可操作性描述。网络环境下的信息安全方案包括网络层安全、系统层安全和应用层安全。参考文献 2。

关键词 信息网络 信息安全 安全模型 安全方案
分类号 G250.73

ABSTRACT To ensure the information security in network environment has become an important problem to be solved. In the paper, the authors analyze major parts of a general model for information security, and introduce a new dynamic model. 2 refs.

KEY WORDS Information network. Information security. Security modeling. Security scheme.
CLASS NUMBER G250.73

随着信息传播方式的改变,如何保证网络环境下信息的安全已成为一个急需解决的问题。这里所讲的信息传播并非传统意义上的信息传播,而是指计算机间通过网络进行的双向信息交换。计算机间的信息交换具有物理和逻辑的双重性质,在网络结构的最低层(物理层),信息交换体现为两台机器间无结构的比特流的传输;物理层以上各层,所交换的信息便有了一定的逻辑结构,越往上逻辑结构越复杂。信息交换在网络的低层(ISO/OSI 模型 1 - 2 层)由硬件实现,在高层由软件或软件加硬件实现。当信息在网络中传送时,一般只涉及 ISO/OSI 模型的 1～3 层。

计算机中的信息在进入网络传送之前,要先经过分割、封装发包的过程,然后由各网络节点转发至目的地。我们所指的网络环境下的信息安全包含三部分:网络环境中信息系统(即信息源)的安全、包在网络传输过程中的安全和数据的完整性保证。本文主要讨论网络环境中信息系统的安全。

1 网络环境下的信息安全模型

网络环境下的信息安全是指信息系统(包括网络系统)整体的安全,是指在整体安全策略的控制和指导下,在综合运用防护工具(如防火墙、身份认证、加密等系统)的同时,利用检测工具(如漏洞评估、入侵检测等系统)了解和评估系统的安全状态,然后通过适当的反应将系统调整到"最安全"或"风险最低"的状态。

传统的信息安全技术都集中在系统自身的加固和防护上。比如,采用 B 级操作系统,在网络出口配置防火墙,在信息传输过程中采用加密技术,使用集中的身份认证系统等等。单纯的防护技术所达到的效果并不十分理想。

例如,一个水库的大坝到底应当修多高?大坝有没有漏洞?大坝现在是否处在危险的状态?这就需要相应的检测机制,比如,利用工程探伤技术检查大坝;观察当前的水位是否超出了警戒水位。这样的检测机制对保证大坝的安全至关重要。当发现问题之后就需要迅速做出响应,比如,立即修补大坝的漏洞并进行加固;如果到达警戒水位,大坝就需要有人 24 小时监护,还可能需要泄洪。这些措施实际上就是一些紧急应对和响应措施。

在信息安全领域,对安全问题的理解也是类似的。我们可以提出相应的信息安全整体模型。模型包含 4 个主要部分:Policy(安全策略)、Protection(防护)、Detection(检测)、Response(响应)。防护、检测和响应组成了一个完整的、动态的安全循环。在安全策略的指导下保证信息系统的安全。根据需求,根据对象,根据可能面对的威胁,制定合理的,有效的安全防护策略,在策略的指导下,建立起相应的防护措施、检测机制、响应方式,而且可以根据需求加强或减低部分的措施,达到代价和效果的平衡。

传统的计算机安全模型中,最典型也最成功的代表模型就是美国国防部 NCSC 国家计算机安全中心于 1985 年推出的 TCSEC(计算机安全评估准则)。TCSEC 可称为信息安全发展史上的一个里程碑。这个准则的发布对操作系统、数据库等方面的安全发展起到了很大的推动作用。TCSEC 对信息系统安全进行评估的安全分级,分为 D/C1 C2/B1 B2 B3/A 等级别。类似的评估方法已经得到业界的认可。但是,上述安全评估准则为代表的安全模型,是针对单机系统环境而制订的,没有针对目前广泛存在和应用的网络

环境安全给予指导。在传统的安全模型中,对动态的安全威胁、系统脆弱性没有足够的描述和应对措施。传统安全模型是"静态安全模型"。但是,随着网络的深入发展,这个标准已经不能完全适应当前的技术需要。这个主要基于 Host-Terminal 环境的静态安全模型和标准无法完全反应分布式、动态变化、发展迅速的网络安全问题。

我们提出的信息安全模型是一个动态模型,其中引入了时间的概念,而且对如何实现系统的安全,如何评估安全的状态,给出了可操作性的描述。用数学公式描述如下:

公式 1:P(t) > D(t) + R(t)

P(t)代表攻破安全目标所花费的时间。

D(t)代表从入侵者发动入侵开始,系统能够检测到入侵行为所花费的时间。

R(t)代表从发现入侵行为开始,系统能够做出足够的响应,对系统进行保护的时间。

对于需要保护的安全目标,如果能满足上述数学公式,即攻破安全目标所花费的时间大于检测时间加上响应时间,那么在入侵者危害安全目标之前攻击行为就能够被检测到并得到及时处理。

公式 2:E(t) = D(t) + R(t), if P(t) = 0

公式的前提是假设攻击时间为 0,即安全目标已被攻击破坏。

D(t)代表从入侵者破坏了安全目标系统开始,系统能够检测到破坏行为所花费的时间。

R(t)代表从发现遭到破坏开始,系统能够做出足够的响应,将系统调整到正常状态的时间。比如,对 Web Server 被破坏的页面进行恢复。

那么,D(t)与 R(t)的和就是该安全目标系统的被破坏的时间 E(t)。对于需要保护的安全目标,如果 E(t)越小,系统就越安全。

通过上面两个公式的描述,实际上给出了安全的全新定义:"及时的检测和响应就是安全","及时的检测和恢复就是安全"。而且,这样的定义为安全问题的解决给出了明确的方向:使系统的攻击时间 Pt 提高,降低检测时间 Dt 和响应时间 Rt。

2 网络环境下的信息安全方案

2.1 网络层安全

网络层采取的安全措施是信息安全的第一道屏障。我们通过控制网络与外界的连接、监测和防御网络入侵攻击、制止非法信息传输来保护信息系统,保证只有授权许可的通信才可以在客户机和服务器之间建立连接,而且正在传输当中的数据不能被读取和改变。

网络层进行的安全防护主要包括如下几个方面。

(1)网络访问控制:在网络节点上进行网络访问控制,提供基于用户的访问规则,针对用户对信息系统的不同访问要求或用户身份授予其不同权限(如基于 IP 地址、TCP 和 UTP 端口号等)。网络节点的访问控制应该具有如下要求:

其一,不仅能按照来访者的 IP 地址区分用户,还可利用 RADIUS 等对来访者的身份进行认证。

其二,可针对应用进行访问控制。对一些复杂的应用协议,如 FTP、UDP、TFTP、Real Audio、RPC 和 port mapper 等,采用特定的逻辑来监视和过滤数据包。

其三,对于现有的各种网络进攻手段,例如:IP Spoofing, TCP sequence number, prediction attacks, Source outing attacks, RIP attacks, ICMP attacks, Data-driven attacks (SMTP and MIME), Domain Name Service attacks, Fragment attacks, Tiny fragment attacks, Hijacking attacks, Dataintegrity attacks, Encapsulated IP attacks 等,提供有效的安全保障。

(2)网络地址翻译:使用网络地址翻译技术,可以让 IP 数据包的源地址和目的地址以及 TCP 或 UDP 的端口号在进出内部网时发生改变,这样可以屏蔽网络内部细节,防止非法用户利用 IP 探测技术发现内部网络结构和服务器真实地址,进行攻击。一般在网络外界接口处实现数据包的网络地址翻译。

(3)可疑网络活动的检测与防御:在网络上,既有来自外部的恶意入侵,也可能存在来自内部的一些恶意攻击和网络误用情况。安全系统应该能够监视内部关键的网段,扫描网络上的所有数据,检测服务拒绝型袭击、可疑活动、怀恶意的 applets、病毒等各种网络进攻手段,及时报告网络管理人员或安全管理人员,使他们能及时采取措施防止这些攻击手段到达目标主机。

2.2 系统层安全

UNIX/ Windows 操作系统本身存在许多安全漏洞和隐患,必须加强这一级别的安全防护,才能保护敏感的信息资源。

(1)使用系统弱点扫描。能够定期扫描操作系统以及数据库系统的安全漏洞以及错误配置。提示管理员进行正确配置。

(2)加强操作系统用户认证授权管理。

(3)限制用户口令规则和长度,禁止用户使用简单口令;强制用户定期修改口令。

(4)按照登录时间、地点和登录方式限制用户的登录请求。

(5)增强访问控制管理。应该从如下方面加强 UNIX 的访问控制机制:

其一,对文件的访问控制除提供读(Read)、写(Write)、执行(Execute)权限外,还应该有建立(Create)、搜索(Search)、删除(Delete)、更改(Update)、控制(Control)等权限,以满足复杂安全环境的需求。

其二,应该能够限制资源被访问的时间和日期。

其三,即使超级用户也不应透过安全屏障去访问未经授权的文件。

其四,对计算机进程提供安全保护,防止非法用户启动或停止关键进程。

其五,控制对网络访问和端口的访问控制。

(6)在大型主机上安装入侵侦测软件,提供预警功能,使系统管理员能及时采取相应的安全防护措施。

(7)计算机病毒防护。自从 80 年代计算机病毒出现以来,已经有数万种病毒及其变种出现,给计算机系统和其中的数据造成了极大的破坏。一些恶性病毒如 CIH 等甚至能够破坏计算机硬件,使整个计算机瘫痪。据统计,99. 3 %的美国公司都受到过病毒的侵袭,修复每次事故平均要花费 8300 美元。如何保证企业内部网络抵御网络外部和内部的病毒入侵,从而保障信息系统的安全运行是目前计算机系统管理员最为关心的问题。所以,强大的计算机病毒防护功能是实现系统层安全必不可少的。

2. 3　应用层安全

对于应用系统,由于其数据包含用户信息、各种应用数据,因此是非常关键和重要的,因此需要对应用系统采取必要的安全措施。

(1)实施统一的用户和目录管理机制。

随着企业分布式计算环境的发展,需要管理的资源越来越多,如用户、用户组、计算机之间的信任关系、不同操作系统、不同通讯协议、不同的数据库系统、不同的服务器和桌面机等等。随着资源的增加,要实现安全管理就越来越困难。单独地维护多种目录体系既费时费力,又容易出错,还难以保证系统的总体安全性和一致性。管理企业内部的用户资源也变得越来越重要和困难。在通常的管理模式中,每种系统都有自己的系统管理员,如 UNIX 的超级用户为 root、Windows NT 的管理员为 administrator、Sybase 和 MS SQL Server 的系统管理员为 sa 等等。IT 管理人员每天都要和这些繁杂的系统打交道,不同的系统管理员在管理这些用户时,就有可能采用不同的用户名,不同的管理策略,以适应各类系统的需要。好的安全管理模式应该帮助用户解决上述问题,允许用户在单一的界面中管理不同系统的用户和目录结构,可以同时在多个不同的操作系统平台上创建、修改和删除用户,提供跨平台的用户策略一致性管理。可以实施基于策略的管理以确保系统安全,可以减少 IT 管理人员管理目录和用户的时间和精力,可以隐藏不同操作系统的差异。

做类似工作的所有用户可能需要类似的安全权限,安全管理应该提供角色的概念。可以将不同平台上有类似安全权限需求的用户规划成组,将用户账号归为角色的概念之下,用户可以对同一角色的用户进行相同的管理,不管这些用户是属于哪个平台、从事何种功能,使得管理员可迅速地在企业内不同操作系统下迅速地创建所需的用户账号。

(2)加密通讯机制。

对于信息系统中的数据通过加密算法进行主动的加密通讯,使通过网络传送的信息不被窃取。

(3)认证授权机制。

对于重要的信息系统需要提供完善的认证授权机制,通过建立良好的认证体系可防止攻击者假冒合法用户,确保对网络服务使用的授权。

(4)备份和恢复机制。

重要的信息系统中的数据需要具备良好的备份和恢复机制,可在受攻击造成损失时,尽快地恢复数据和系统服务。在以前的中美黑客大战中,美方的信息系统有很好的备份恢复机制,因此在攻击中所受损失很少,而中方很多信息系统没有备份恢复机制,被攻击后基本瘫痪。由此可见数据备份及恢复机制的重要。

参考文献

1　周明天,汪文勇. TCP/ IP 网络原理与技术. 北京:清华大学出版社,1997

2　GB17859 —1999. 计算机信息系统安全保护等级划分准则(S)

智勇　南京大学信息管理系研究生。通讯地址:南京大学。邮编 210093。

黄奇　南京大学信息管理系主任。通讯地址同上。

(来稿时间:2001-10-31)

“全国公共图书馆计算机应用知识大赛”圆满结束

由文化部主办、国家图书馆承办、中国数字图书馆有限责任公司协办的“全国公共图书馆计算机应用知识大赛”,于 2001 年 12 月 4 日至 6 日在北京举行。全国 27 个省、自治区、市代表队参加了比赛。

12 月 6 日,在中央电视台演播大厅进行决赛。决赛现场,著名学者朱家[illegible]、杨镰畅谈了图书馆在社会发展进程中的作用,北京大学教授梅宏向观众描绘了图书馆未来的发展方向 ——数字图书馆的前景。大赛组委会主任、主化部副部长周和平,文化部社会文化图书馆司和国家图书馆领导,大赛顾问、特邀评委和嘉宾、在京各大型图书馆馆长及各省参赛队选手共计 200 余人观看了比赛。

经过激烈争夺,浙江省代表队问鼎金奖,辽宁省代表队获得银奖,北京市代表队获得铜奖,湖北省代表队、江苏省代表队、河北省代表队获得优秀奖。北京市代表队刘婕获得最佳选手奖。获得本次大赛组织奖的是:北京市文化局、天津市文化局、河北省文化厅、辽宁省文化厅、上海市文广局、山东省文化厅、江苏省文化厅、浙江省文化厅、湖北省文化厅、广西壮族自治区文化厅。　(张小平　白雪华)