

网络环境下数据安全控制技术研究

杨建春

(靖远煤业集团有限责任公司信息中心,甘肃 白银 730913)

摘要:从数据安全问题的需求发展变化出发,阐明了当今网络环境下数据安全控制中的关键问题,分析了数据安全控制层次结构、基本原则及数据安全控制技术。

关键词:网络;数据安全;控制

中图分类号:TP313

随着 Internet 与各行业信息化的迅猛发展,数据安全技术也进入了高速发展的新时期,人们对数据的需求不再是从早期单一概念上的通信保密,而是需要数据在存储、处理或传输过程中不被非法访问或更改,以及确保对合法用户的服务和限制非授权用户的访问等。数据安全技术形成了防火墙技术、入侵检测技术、密码与数字签名技术、风险分析技术等多个安全防御技术门类。

数据安全即要保障数据的机密性、完整性、不可否认性、可用性、可控性等功能特性,其中机密性保证数据不泄露给未授权的用户、实体或过程;完整性保证信息的完整和准确,防止信息被非法修改;可用性保证信息及信息系统确实能力授权者可用;不可否认性保证行为不能否认自己的行为;而可控性保证对信息的传播及内容具有控制的能力,防止为非法者所用。

1 数据安全控制层次结构

系统应提供有效的数据安全控制策略,既注重数据访问的安全性和监督用户的登陆,又兼顾用户在使用数据时对速度性的要求。

目前,数据安全主要是依靠分层技术解决的,安全措施一级级层层设置,真正做到了层层设防。

第一层是注册和用户许可,保护对服务器的基本存取;第二层是存取控制,对不同用户设定不同的权限,使数据得到最大限度的保护;第三层是增加限制数据存取的视图和存储过程,在数据库与用户之间建立一道屏障。

2 数据安全控制的基本原则

基于数据安全控制层次结构的安全体系,提出以下几点实施安全的原则:

1) 选择性访问控制 (Discretionary Access Controls, DAC)。DAC 是基于主体或主体所在组的身份的,这种访问控制是可选择性的,也就是说,如果一个主体具有某种访问权,则它可以直接或间接地把这种控制权传递给别的主体(除非这种授权是被强制型控制所禁止的),选择性访问控制被内置于许多操作系统当中,是任何安全措施的重要组成部分。文件拥有者可以授予一个用户或一组用户访问权,选择性访问控制在网络中有着广泛的应用。DAC 用户决定了用户是否有权访问数据对象。

2) 验证。通过对用户的验证,保证只有授权的合法用户才能注册和访问。

3) 授权。控制谁能够访问数据和进行何种数据操作权限。

4) 审计。监视系统发生的一切事件,对并各类事件按照规定的策略进行记录,并对相应安全行为进行告警。

3 数据安全控制技术

这些技术包括用户身份认证、防火墙 (firewall)、入侵检测 (Intrusion Detection)、数据加密及访问记录及报警等。

3.1 用户身份认证

对数据安全、可靠、有效地存取是数据安全的关键,身份认证技术是主要的实现手段,在生物测定技术还不能大规模使用的今天,用户名加口令方式的仍然是身份认证的主要武器,这种认证方式是保障数据安全最基本的手段之一。用户认证目的是验证用户身份、访问请求的合法性,可有效地防止冒充和非法访问等威胁。例如:对拨号上网的客户或员工,其 IP 地址是 ISP 提供的动态地址,因而必须确认其身份才能保护网络安全。为此,可提供 3 种身份认

证方法:对话式认证、主机式认证、代理式认证。这 3 种认证方法,用户都需要先向防火墙表明其身份,经防火墙认可之后才能连接到目标服务器。采用对话式认证和主机式认证时,用户均要向防火墙输入其真实的登陆用户名和口令。在代理式认证方式下由代理程序替用户代行身份认证,因此用户并不会感觉到有认证操作的发生。

3.2 防火墙

防火墙技术是建立在现代通信网络技术和信息安全技术基础上的应用性安全技术,越来越多地应用于内、外网的互连环境中,它在内、外网之间建立起一个安全网关(Security Gateway),从而保护内网免受非法用户的侵入。防火墙主要由服务访问政策、验证工具、包过滤和应用网关 4 个部分组成。防火墙通过控制和监测信息交换和访问行为来实现对数据安全管理,基本功能为:过滤进、出网络的数据;管理进、出网络的访问行为;封堵某些禁止行为;记录通过防火墙的数据内容和活动;对网络攻击进行检测和告警。

防火墙总体上分为包过滤、应用级网关和代理服务几种类型:

1)数据包过滤(Packet Filtering)技术是在网络层对数据包进行选择,选择的依据是系统内设置的过滤逻辑,被称为访问控制表(Access Control Table)。通过检查数据流中每个数据包的源地址、目的地址、所用的端口号、协议状态等因素,或它们的组合来确定是否允许该数据包通过。数据包过滤防火墙逻辑简单,价格便宜,易于安装和使用,网络性能和透明性好,它通常安装在路由器上。路由器是内部网络与 Internet 连接必不可少的设备,因此在原有网络上增加这样的防火墙几乎不需要任何额外的费用。数据包过滤防火墙的缺点有二:一是非法访问一旦突破防火墙,即可对主机上的软件和配置漏洞进行攻击;二是数据包的源地址、目的地址以及 IP 的端口号都在数据包的头部,很有可能被窃听或假冒。

2)应用级网关(Application Level Gateways)是在网络应用层上建立协议过滤和转发功能。它针对特定的网络应用服务协议使用指定的数据过滤逻辑,并在过滤的同时,对数据包进行必要的分析、登记和统计,形成报告。实际中的应用网关通常安装在专用工作站系统上。

数据包过滤和应用网关防火墙有一个共同的特点,就是它们仅仅依靠特定的逻辑判定是否允许数

据包通过。一旦满足逻辑,则防火墙内外的计算机系统建立直接联系,防火墙外部的用户便有可能直接了解防火墙内部的网络结构和运行状态,这有利于实施非法访问和攻击。

3)代理服务(Proxy Service)也称链路级网关或 TCP 通道(Circuit Level Gateways or TCP Tunnels),也有人将它归于应用级网关一类。它是针对数据包过滤和应用网关技术存在的缺点而引入的防火墙技术,其特点是将所有跨越防火墙的网络通信链路分为两段。防火墙内外计算机系统间应用层的“链接”,由两个终止代理服务器上的“链接”来实现,外部计算机的网络链路只能到达代理服务器,从而起到了隔离防火墙内外计算机系统的作用。此外,代理服务也对过往的数据包进行分析、注册登记,形成报告,同时当发现被攻击迹象时会向网络管理员发出警报,并保留攻击痕迹。

3.3 入侵检测

入侵检测是数据安全的一个重要组成部分,入侵检测按照一定的安全策略,对网络、系统的运行状况进行监视,尽可能发现各种攻击企图、攻击行为或者攻击结果,以保证网络系统资源的机密性、完整性和可用性。

我们做一个形象的比喻:假如防火墙是一幢大楼的门锁,那么 IDS 就是这幢大楼里的监视系统。一旦小偷爬窗进入大楼,或内部人员有越界行为,只有实时监视系统才能发现情况并发出警告。

不同于防火墙,入侵检测系统(Intrusion Detection Systems,IDS)是一个监听设备,没有跨接在任何链路上,无须网络流量流经它便可以工作。因此,对 IDS 的部署,唯一的要求是:IDS 应当挂接在所有所关注流量都必须流经的链路上。在这里,“所关注流量”指的是来自高危网络区域的访问流量和需要进行统计、监视的网络报文。在如今的网络拓扑中,已经很难找到以前的集线器、总线方式的共享介质冲突域的网络,绝大部分的网络区域都已经全面升级到交换式的网络结构。因此,IDS 在交换式网络中的位置一般选择在尽可能靠近攻击源和尽可能靠近受保护资源,比如:服务器区域的交换机上、Internet 接入路由器之后的第一台交换机上、重点保护网段的局域网交换机上。

入侵检测系统能判断出目前进入的数据包是否合法,并能对多种攻击行为进行检测,包括 Ipspoofing、SYNflooding、Portflooding、Portscanning 及 Pingdeath。管理者可以自行选择设

定或更改相关策略决定是否拦截这些数据包的攻击行为。

3.4 数据加密

防火墙等技术是一种被动的防卫技术,而数据加密技术则是一种主动的防卫措施。数据加密是数据保护技术措施中最古老、最基本的一种。加密的主要目的是防止数据的非授权泄漏。加密方法多种多样,在网络中一般是利用变换规则把易懂的数据变成不可懂的数据。即可对传输数据加密,也可对存储数据加密,把数据变成一堆乱七八糟的数据,攻击者即使非法获得加密数据时,也不过是一串看不懂的毫无意义的字符序列。加密可以有效地对抗截取、非法访问等威胁。现代密码算法不仅可以实现加密,还可实现数字签名、鉴别等功能,有效地对抗截取、非法访问、破坏数据的完整性、冒充、抵赖、重演等威胁,因此密码技术是数据安全的核心技术之一。常见的数据加密算法有 DES 算法、RSA 算法、IDEA 算法、DSA 算法等。

3.5 访问记录及报警

当用户访问数据对象时,系统将自动把用户访问数据对象的相关信息实时记录下来,访问记录的内容主要有用户名称、来源、访问日期与时间、访问内容、规则等等,如果用户访问数据对象非法或可能危及或使数据泄露时,甚至会发出相关告警。记录

与告警信息也按分级方式进行记录或告警,如正常、警告、危险、错误等。

虽然通过各类防范技术措施与手段可以在一定程度上解决某些数据安全隐患,但仍无法彻底消除数据安全风险,绝对安全是不存在的。因此,从技术层面而言,用户应继续健全数据安全保障体系,从使用层面而言,应养成良好的习惯,强化数据安全防范意识与数据安全控制策略的应用,意识到数据安全不可能通过系统得到彻底解决,它不仅是一种技术问题,更是有关业务和管理的问题,只靠技术是不能保证数据安全的,因此数据安全有赖于技术与管理相互作用,才能使数据最大限度免受各类威胁,从而保证数据安全。

参考文献:

- [1] 王德军. 容灾技术研究[M]. 武汉:武汉大学出版社, 2004.
- [2] 方勇,刘嘉勇. 信息系统安全导论[M]. 北京:电子工业出版社,2003.
- [3] 卢开澄. 计算机密码学[M]. 北京:清华大学出版社, 1990.
- [4] 段云所. 信息安全概论[M]. 北京:高等教育出版社, 2003.
- [5] 姚翌. 谁来保护中小企业内部数据安全,计算机与网络[J]. 2005(6):24.