文章编号:1005-6033(2011)18-0136-03 收稿日期:2011-05-06

金融网络安全策略及关键技术

李伟鸿

(晋城职业技术学院民用工程与商务管理系,山西晋城,048026)

摘 要:金融网络具有先进性、标准性、扩展性和高安全性的特点,要求在金融网络组网和管理中合理运用各种安全策略及各项关键技术,才能保证金融网络运行安全高效地进行。同时金融系统的安全措施对于保证安全运行有着重要意义。

关键词:金融网络;安全策略;关键技术

中图分类号:F830.49 文献标识码:A

随着金融系统信息化程度的不断深入,金融网络业务不断扩展,金融网络应用及业务发展面临着越来越多的安全挑战。按照网络结构的层次化、分组化以及高速化的发展目标,满足金融系统越来越多的日常营业性业务、OA 等管理性业务以及面向多媒体的综合业务的需求,客观上要求必须重视网络系统的高效性和安全性。在金融系统网络整体方案中要充分考虑先进性、标准性、扩展性和高安全性。

1 金融网络的安全策略

1.1 网络协议

一般的 IP 网络模型分为接入层、IP 层、传输层和应用层这 4 个层次。由于传输层及其以下各层都是为网络数据传服务的,通常可以将这几层统称为网络层,而以上各个层次则统称为业务层。

网络层及业务所面临的安全问题特点不同,需要分别进行设计[1]。

1.1.1 网络层面临的安全威胁

网络层面临的安全威胁主要有以下几个方面:

(1)报文窃听。网络信息窃取者使用专用的报文窃取工具,从传输的数据流中截取相应的数据包并进行分析,获取用户的登录信息或其他相关数据,使用户信息的私密性受到威胁。通过公用 Internet 传输的数据,不但存在时间上的延迟,而且存在地理位置上的跨越,要想绝对避免数据在传输途中不受窃听,几乎是不可能的。而对于总线性局域网或位于同一个 VLAN 内的交换性网络用户,所有用户的报文信息对其他用户都是极易获取的。因此,对金融网络系统所有的敏感数据都必须采取数据加密技术,以防止报文窃听。

(2)可用性攻击。攻击者一般通过发送大量无用报文占用目标用户网络带宽,使其网络系统软硬件资源被过度消耗而不能正常开展业务,这对服务性极强和对可用性要求较高的金融网络系统是致命的,要求必须采用网络访问控制技术来限制非法的报文在网络中传递。

(3)IP 地址欺骗。攻击者通过专用软件把自己的 IP 地址修改成目标网络信任的 IP 地址,把自己伪装成目标网络内部用户或可信任的外部用户,通过发送特定的报文来更改路由信息,以窃取敏感信息[1]。可以采用访问控制技术和身份认证方式进行限制。

(4)用户名/口令失密:在一些拨号网络连接时,通常采用的 PPP 协议需要用户口令认证。如果用户账号信息被盗取,就可能会使不法分子登录网络。对此情况可以采用 CallBack 技术解决。

(5)拒绝服务攻击。攻击者的目的是阻止合法用户对资源的访问。流量攻击也是拒绝服务攻击的一种,可以通过网络层和应用层的结合进行防御。

(6)网络设备或软件的后门。不排除国外某些计算机软硬件厂商无意或有意地在其提供的网络软硬件产品中预设有后门陷阱,在利益需要时只要通过发送特定的报文就可以轻松导致用户设备不可用或被恶意操纵,甚至窃取用户重要的信息,使用户遭受巨大损失。

1.1.2 业务层所面临的安全威胁

业务层所面临的安全威胁主要有以下几个方面:

(1)操作系统或应用软件的漏洞。在 Internet 受到攻击最多的就是利用操作系统或者是应用软件的漏洞来进行的。针对操作系统或者是应用软件的漏洞,需要网络用户有较好的网络安全意识和常识,通过周期性给操作系统和相关应用软件安装最新补丁来保证软件的应用安全。

(2)用户名/口令泄密。在使用一些有安全缺陷的 WWW 服务器软件业务时,如果网络数据传输时不加密,则可能造成用户名/口令被窃取,导致严重的后果和损失。因此,在提供网上业务时可以采用 SSL 等加密技术来安全地传输数据。

(3)非法访问。用户访问不受限制,超级访问或跨区域访问。在金融网络中,存在多个部门,包括结算、会计、开发等部门,这些部门之间通常是不允许相互访问的。使用 VLAN 技术进行逻辑隔离可以进行有效地访问控制。

1.2 金融网络的分层结构

通常的组网模型分为接入层、交换层和核心层 3 个层次内部网络结构，同时还有访问公网和提供公网用户访问的业务两个需求。这些决定了必须考虑内部网络与外部网络之间的安全连接。

1.2.1　接入点的安全

接入点主要是指各营业网点，通常分布在不同的地理位置，必须考虑本地主机对节点的访问控制、节点与中心数据传输、节点接入网络中心等的安全和保密。目前主要有 3 种不同的接入方式，也对应有 3 种不同的安全技术。

⑴ 拨号接入。拨号线路最大的缺点是全网可达，因此存在密码泄露后非安全用户接入及线路被窃听的可能，此时线路的安全是首位的，采用加密技术将报文加密后传输是一种不错的选择。

⑵ DDN 接入。DDN 接入是一种传统接入方式，物理层采用的是类似透明通道的方式传递数据，线路提供商在两全节点之间建立半永久连接，因此，通常认为线路有比较高的安全性，一般只需要考虑网络的安全访问控制及认证互联就可以了。

⑶ 宽带城域网 VPN[3,4] 接入。公网的安全性较低，因此要采用加密技术。对关键业务采用更强的加密算法和更高的密钥更换频率；对一般的数据流采用普通强度的加密算法即可。

1.2.2　交换层的安全

交换层主要是指分中心，承担着各业务网点之间以及业务网点和数据中心之间相连的作用，环境较复杂。对于交换层与业务网点之间的互联，主要的接入方式同边缘接入点，其安全策略也相同；对于交换层与核心网络层来说，主要有 DDN 以及通过公网的 VPN 这两种方式，其安全策略也对应于边缘接入点的相应方式。

1.2.3　核心层的安全

核心层一般采用以交换以太网方式建成一个高速局域网，数据经汇聚层交换后传递到核心层。核心层通常不会直接被外部网络攻击，其主要威胁来自于网络内部[5]。一般采用直接的物理隔离或是 VLAN 技术实现访问控制功能。对于与外部网络有联系的情况，相关业务主机与 Internet 物理隔离，并且上网需要进行 NAT 或通过 PROXY 进行。对于为外部用户提供开放的业务，如网上银行等对外业务必须部署在 DMZ 中，外部网络只能访问 DMZ 中的主机，而不能访问内部网络。

2　金融网络安全的关键技术

2.1　VLAN 技术隔离不同的业务

金融网络系统中存在如办公自动化、会计、验印系统、自动提款机 ATM 等多种业务，要实现这种多业务网的统一互联，同时又要保证各个子网络的安全，除了通过加密、签名等手段在应用层上避免数据泄露和篡改外，在局域网中应该采用 VLAN 技术进行逻辑隔离，将相同业务子网的设备划分在同一个 VLAN 中，而将不同业务划分在不同的 VLAN 中，避免各业务子网之间的直接相互访问。目前，一般交换机都支持按物理端口、IP 地址，或用户主机物理地址等方式来划分 VLAN，因此，通过 VLAN 技术实现各业务子网之间的逻辑隔离是局域网安全的首要选择。

2.2　防火墙访问控制技术保证核心安全

为了保证核心数据的访问高度安全性，应采用网络防火墙来保护核心设备的安全。基于管理方便化和网络结构简单化的原则，通常部署一个高速防火墙或 VPN 综合网关[6]，对所有进出网络中心的数据包进行安全检测和过滤，保证访问网络核心的安全。要求该网关设备具有电信级的可靠性、分布式处理、任意板件的热插拔和接口 *N*+1 备份等特点，以适应金融系统的非常高的要求。

2.3　数据加密技术

为了防止传输过程中的数据被截取、修改或伪造，可采用数据加密技术。一般有链路加密、端到端加密和混合加密。加密算法有 DES 数据加密标准、RSA 公钥密码体制、MD5 加密算法和 PGP 安全加密系统。在金融网络中要求支持 IPSEC 安全加密体系、L2TP 隧道安全技术和支持 384 (3DES) 位以上长密钥加密算法。

2.4　路由认证技术

中心与下属分中心节点之间互联的路由器在交换路由信息时，要求通过路由认证，防止路由信息扩散到不安全区域。

2.5　双 DMZ 防火墙技术

在外部 DMZ 区的网段上部署对外部网络用户提供服务的网上银行服务器、门户网站等，外屏蔽路由器用户防范外部攻击，如源地址欺骗和源路由攻击，并管理 Internet 至外 DMZ 的访问；与其他商业银行之间的互联部署在内部 DMZ 区，设置集中认证点对接入用户进行安全认证，业务通过代理服务器进行交换，严格禁止内外部网络直接进行数据传输。

2.6　ACL 访问控制技术

在网点的路由器上设置访问控制表和相应的访问权限，只有满足过滤规则的数据包才被转发至相应的路由器端口，而其余的数据包则被丢弃，为网络访问提供了第一层访问控制。

3　结语

以上安全策略和技术措施保证了金融网络的安全需求，但是，我们也清醒地认识到包过滤、加密技术、防火墙技术并不能解决所有的网络安全问题。对于来自内部网络的攻击和病毒危害必须要加强管理，给予足够重视。只有采用安全措施（包括行政法律手段、各种制度以及专业措施），才能使安全策略和技术更好地保证金融网络的安全。

参考文献

[1]　陈性元，杨艳.网络安全通信协议[M].北京：高等教育出版社，2008.

[2]　陆军.防信息泄露技术[J].计算机安全，2005，6(2)：14-16.

[3]　Jazib Frahim，Qiang Huang.SSL 与远程接入 VPN[M].王酷，

文章编号 :1005-6033 (2011) 18-0138-03 收稿日期 :2011-04-27

对湖南商学院数字化校园建设的研究

王 枢

(湖南商学院现代教育技术中心,湖南长沙,410205)

摘 要 :分析了湖南商学院数字化校园建设现状和存在的具体问题,在此基础上提出了详细的建设方案。

关键词 :数字化校园建设 ;基础设备 ;系统安全 ;网络安全 ;湖南商学院

中图分类号 :G647 文献标识码 :A

数字化校园建设的实质,是以覆盖全校的校园网络为基础,利用先进的信息化手段和工具,实现对各种资源的有效集成、整合和优化,实现从环境(包括设备、教室等)、资源(如图书、讲义、课件等)到活动(包括教学、管理、服务、办公等)的全部数字化[1],并实现数字化信息的管理和共享,以形成高度信息化的办公教学和人才培养环境。

1 数字化校园建设

数字化校园建设主要包括网络基础设施建设、网络基础服务建设、网络应用系统建设等几部分。其中网络基础设施建设主要包括校园网络的搭建以及工作在这些网络环境之上提供服务的服务器构架等。网络基础服务建设主要包括最常用的 Internet 服务和实现上层网络应用所依赖的基础服务。网络应用系统是数字化校园的核心部分,它包括数字化图书馆、网上教学系统、办公自动化系统、教学资源库等[2]。

2 我校数字化校园建设现状

我国的"211 工程""985 工程"的顺利实施带动了高校信息化的快速发展,使高校公共服务体系初具规模。全国高等教育的数字化信息平台已具雏形。在随后的几年里,各类学校纷纷加大了信息化教育的投入。到目前为止,许多高校的校园网建设已取得阶段性成果[3]。

湖南商学院(以下简称我校)数字化校园工程建设于 1999 年启动,于 2006 年实施校园网全面整网改造,建成了目前万兆核心、千兆主干、百兆桌面、网络全覆盖的高质量校园网。全校数设信息点 4 000 多个。校园网采用天融信 NFGW4000 硬件防火墙,核心路由器采用锐捷 S8606,在一办公楼、二办公楼、图书馆建立 3 个万兆节点,形成环行网络,以千兆光纤接通每一栋办公楼、教师宿舍、学生宿舍和所有实验实训室。学校中心机房共有 28 台服务器,容量 16 TB 的磁盘阵列。学校各院系大小网站共

译.北京 :人民邮电出版社,2009.

[4] 韩儒博,邬钧霆,徐孟春.虚拟专用网络及其隧道实现技术[J].微计算机信息,2005,21(8):1-3.

[5] 谢小军. 内部网络的安全保护措施 [J]. 现代电子技术,2003,4(1):9-11.

[6] 张卫,王能,俞黎阳,等.计算机网络工程 [M].北京 :清华大学出版社,2004 :289-293.

(责任编辑 :白尚平)

第一作者简介 :李伟鸿,男,1971 年 10 月生,2008 年获北京工业大学软件工程专业工程硕士学位,讲师,现任晋城职业技术学院民用工程与商务管理系副主任,山西省晋城市,048026.

Financial Network Security Policies and Key Technologies

LI Wei-hong

ABSTRACT: The financial network, which possesses many features such as the advancement, standard, scalability and high security, requests the rational use of various security strategies and the key technologies in the networking and management of the financial network in order to ensure the safe and efficient operation of the financial network. Meanwhile, the safety measures of the financial network have the vital significance for ensuring its safe operation.

KEY WORDS: financial network; security strategy; key technology