济南人民银行计算机网络安全方案

曲效利（人民银行济南分行科技处 250001）

1 概述

网络环境和网络应用已经成为济南分行各级机构行使职能、处理业务、开展工作的重要基础和必要手段。当前，随着清算系统和信贷登记咨询系统等各种应用系统的开发和推广，与人民银行网络互连的机构也越来越多，同时网络安全隐患也越来越严重。在全国范围内发生的越来越多的面向金融系统的高科技犯罪事件，不断给我们提出警示：网络安全不容忽视。

2 安全需求

2.1 网络环境

济南分行网络系统组成单元包含三部分：分行及各中心支行机关局域网、人民银行内联网、分行及各中心支行与同城商业银行互连网。

从应用的角度来看，济南分行目前的应用主要包括资金清算系统、信贷登记咨询系统、办公自动化系统三部分。

2.2 安全现状

济南分行网络系统安全状况描述如下：

(1) 人民银行各级机构之间的通信以及人民银行与商业银行之间的通信，基本没有安全防护措施，只有少部分单位采用了路由器内置的简单包过滤防火墙。

(2) 服务器操作系统以 Unix、Windows NT 为主，桌面操作系统以 Windows 95/98 为主，基本没有安全保护措施。

(3)对应用系统的访问控制能力较弱。一般是对现有操作系统、数据库系统、电子邮件系统、应用系统安全机制的简单利用。

(4) 部分应用环境具备初级防病毒能力。如在LAN的PC工作站上，一般部署了防病毒软件，但病毒特征数据库的更新一般严重滞后。

(5) 对内、外部攻击缺少基本的监控保护手段。

(6) 缺乏对系统的安全评估手段。

(7) 网络信息传递以明文方式进行，缺乏加密保护。

2.3 安全威胁

通过对济南分行网络结构的分析，我们发现安全威胁主要来自以下方面：

(1) 操作系统的安全性：UNIX、Windows NT 等操作系统均存在网络安全漏洞；

(2) 来自内部网用户的安全威胁；

(3) 来自外部网用户的安全威胁；

(4) 缺乏有效的手段监视和评估网络系统的安全性；

(5) 采用 TCP/IP 协议族软件，本身缺乏安全性；

(6) 应用服务的安全性：许多应用服务系统在访问控制及安全通信方面考虑较少。

为解决网络系统中存在的安全隐患，保障网络及信息的安全，我们设计了计算机网络安全方案并在济南分行及辖内各中心支行组织实施。

3 方案的设计思想与原则

3.1 方案设计思想

考虑安全层次、技术难度及经费支出等因素，在设计方案时我们遵循了如下设计思想：

(1) 尽可能地提高系统的安全性和保密性；

(2) 保持网络原有的性能特点，即对网络的协议和传输具有很好的透明性；

(3) 易于操作、维护，并便于自动化管理，而不增加或少增加附加操作；

(4) 尽量不影响原网络拓扑结构，便于系统结构及系统功能的扩展；

(5) 安全保密系统具有较好的性能价格比，一次性投资，可以长期使用；

(6) 安全与密码产品具有合法性，并便于安全管理单位与密码管理单位的检查与监督。

3.2 方案设计原则

济南分行网络安全方案的设计遵循了如下原则：

3.2.1 需求、风险、代价平衡的原则

对任一网络，绝对安全难以达到，也不一定是必要的。应付一个网络进行实际研究(包括任务、性能、结构、可靠性、可维护性等)，并对网络面临的威胁及可能承担的风险进行定性与定量相结合的分析，然后制定规范和措施，确定安全策略。

3.2.2 综合性、整体性原则

安全模块和设备的引入应该体现系统运行和管理的统一性。一个完整的系统的整体安全性取决于其中安全防范最薄弱的一个环节，必须提高整个系统的安全性以及系统中各个部分之间的严密的安全逻辑关联的强度，以保证组成系统的各个部分协调一致地运行。

3.2.3 可用性原则

安全措施需要人为去完成，如果措施过于复杂，对人的要求过高，本身就降低了安全性。

3.2.4 设备的先进性与成熟性

安全设备的选择，既要考虑其先进性，还要考虑其成熟性。先进意味着技术、性能方面的优越，而成熟性表示可靠与可用。

3.2.5 无缝接入

安全设备的安装、运行，应不改变网络原有的拓扑结构，对网络内的用户应是透明的、不可见的，同时，安全设备的运行应该不会对网络传输造成通信“瓶颈”。

3.2.6 可管理性与扩展性

安全设备应易于管理，而且支持通过现有网络对网上的安全设备进行安全地统一管理、控制，能够在网上监控设备的运行状况，进行实时的安全审计。

4 安全方案

遵照上述设计思想及设计原则，我们确定了济南分行计算机网络安全方案(如图 1 所示)。下面对方案中采用的技术、设备和措施做详细介绍。

4.1 VLAN 技术

济南分行及各中心支行的局域网均采用 Ethernet 技术，为了更好保证局域网的安全，我们选用了具备VLAN支持能力的交换机设备，按照用户群组和系统资源的访问权限进行安全划分。将分行或中心支行的服务器系统单独划作一个 VLAN。也可以按照机构的设置来划分 VLAN，如将领导所在的网络单独作为一个 Leader VLAN(LVLAN)，其他处(科)室分别作为一个 VLAN，并且控制LVLAN与其他VLAN之间的单向信息流向，即允许 LVLAN 查看其他 VLAN 的相关信息，其他 VLAN 不能访问 LVLAN 的信息。

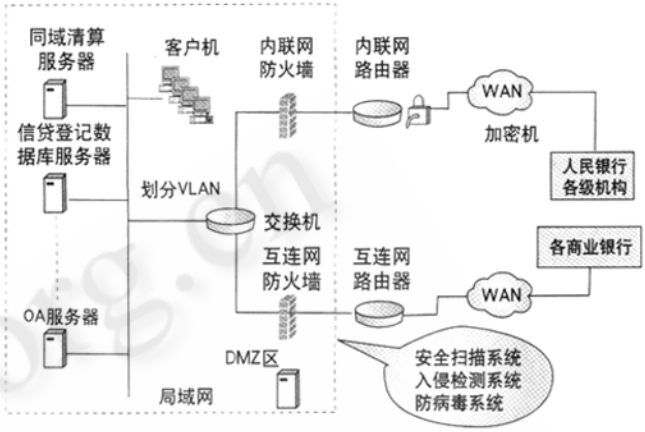

图 1 网络安全方案

4.2 加密技术

济南分行网络系统采用国家公共网传输数据，在广域网上进行传输的信息容易被不法分子截取、利用。

为保障信息传输的安全性，我们在内联网系统中采用了链路加密机，对传输的信息进行加密；在互连网络上运行的关键业务系统中也利用了加密算法对传输的数据进行加密。

4.3 防火墙

根据济南分行网络系统的安全需要，我们在人行内联网以及人行与商业银行互连网上分别布置了内联网防火墙和互连网防火墙(如图 1 所示)。

防火墙在网络入口点检查网络通信，屏蔽非法侵入，其安全作用体现于：

(1) 有效地防止外来的入侵；

(2) 控制进出网络的信息流向和信息包；

(3) 提供使用和流量的日志和审计；

(4) 隐藏内部 IP 地址及网络结构的细节。

4.4 入侵检测系统

利用防火墙技术，经过仔细的配置，通常能够在内外网之间提供安全的网络保护，降低了网络安全风险。但是入侵者可寻找防火墙背后可能敞开的后门，入侵者也可能就在防火墙内。

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以及采取相应的防护手段。入侵检测系统包括基于主机的入侵检测系统和基于网络的入侵检测系统两种。我们在济南分行网络系统中布设了基于主机的入侵检测系统，用于保护关键应用的服务器，实时监视可疑的连接和非法访问的闯入，并对各种入侵立即进行反应，如断开网络连接等。

4.5 安全扫描系统

安全扫描系统是现阶段最先进的系统安全评估技术，它能够测试和评价系统的安全性，并及时发现安全漏洞。安全扫描系统包括基于服务器的安全扫描系统和基于网络的安全扫描系统。我们布设了基于网络的安全扫描系统，用于扫描设定网络内的服务器、路由器、变换机、防火墙等设备的安全漏洞，并可设定模拟攻击，以测试系统的防御能力。

4.6 防病毒措施

计算机病毒对信息安全具有灾难性的影响。在济南分行网络系统中，我们建立了多层次的病毒防卫体系，以保证信息的安全和系统的正常运行。其具体内容包括：

(1) 在系统的每个台式机上要安装台式机的反病毒软件；

(2) 在服务器上要安装基于服务器的反病毒软件；

(3) 加强员工教育，使每一个员工做到个人使用的台式机上不受病毒的感染，从而保证整个企业网不受病毒的感染。

4.7 增强操作系统的安全性

济南分行采用的操作系统以SCO Unix、AIX、Windows NT、Windows 95/98等为主。以上所有的操作系统均存在一定的安全漏洞，并且越流行的操作系统(如Windows NT、Windows 95/98)发现的问题越多。

操作系统的安全性能对于整个应用系统的安全性至关重要。为增强系统安全性，我们对现有各种操作系统进行安全性增强和合理配置，具体内容包括：

(1) 跟踪系统应用动态，不断地增加安全补丁。

(2) 检查系统设置(敏感数据的存放方式，访问控制，口令选择/更新)。

(3) 将系统的安全级别设置为最高级。

5 结束语

目前，济南分行计算机网络安全系统的建设已顺利完成，但是制定系统安全方案、安装网络安全系统只是网络系统安全性实施的第一步，只有当济南分行各级机构均严格执行网络安全的各项规定，认真维护各自负责的分系统的网络安全性，才能保证济南分行网络的整体安全性。■