应用系统的安全设计

摘要：

我在某大学网络中心工作，我校数字化建设的主要内容是建立基于千兆主干网络的、提供多种网络服务的网络应用体系。2001 年 3 月，我参加了数字图书馆建设，担任技术部主管职务，负责理解学校和省教委对该项目的要求，根据技术先进、成本适中、充分满足要求为原则，进行应用需求分析，对整个网络进行设计，提出设计方案。

由于该项目规模比较大，提供的服务比较多，作为校园网络的中心和提供网络服务的核心部门，我馆图书馆的许多业务需要在网上展开，各种特色服务所用的平台也是五花八门。这对安全方面的设计提出的较高的要求。我们通过采用保障 Internet 接入的安全、保证干路畅通和合理划分子网、保证软件系统的安全、健全管理机制等措施来设计图书馆网络。这种切合实际、低成本、高技术的设计方案实施后的网络，其安全性大大加强了，同时网络的性能并未受到太多的影响。

正文：

2001 年 3 月，我参加了某大学数字 211 建设图书馆数字化建设部分（分为第一、第二、第三期工程），第二期工程总额 5500 万元。该工程建设项目分为网络部分、软件部分以及资源建设部分。该项目的目标是，将地处该城市的东、西、南、北端的各分校区和总校区的网络联连接成为一个畅通的宽带、高速、高性能的校园网；建立一个文献信息中心，能为读者提供电子期刊服务、图书书目数据服务、图书光盘点播、视频点播服务，并且能够拥有部分自己的特色数据资源；建立一个网络中心，提供 Web 服务、邮件服务、全校的办公自动化服务，它既是全校的应用服务中心、公共数据存储中心，又是全校网络的管理中心。我在该项目中担任技术部主管，任务是进行应用需求分析，对整个网络进行设计，提出设计方案。由于该项目规模比较大，提供的服务比较多，各种特色服务所用的平台也是五花八门。同时，影响网络安全的因数比较多，通常有人的因数、自然因数、病毒因数。如果对这些主要因数防范不得力，将影响网络硬件、网络数据传输、数据服务器的安全。因此对其安全设计，单

一的技术或者设备保护难以保证本校网络的安全，效果往往不理想；所以我们采用多层次的防护体系来保证网络的畅通和网络数据的安全。我们根据业务数据的流动历经的重要环节，来提出具体的安全方案。

1．保证接入的安全

俗话说病从口入，同样一些常有的攻击往往来自外网，同时使用图书馆所购买的外文资料例如 Web Science、EBSCO 等数据库需要访问外网；同时，外网的授权用户需要能够访问我们的数据。所以必须保证接入部分的稳定与安全。在外网联接上，我们租用 2 条光纤线路（100M）分别接入中国电信和 XXX 大学，使用 Cisco 的 7500 系列路由器接入，然后用一台 Sun spark 操作系统为 Solaris 的服务器做防火墙将外网和内网划分开；同时用其做策略路由服务器，使用校园网内的用户可以快捷的访问电信网络和教育网络的资源。在外部用户访问上，我们首先用 Sun spark 服务器防火墙进行 IP 地址过滤掉非法的 IP 地址，然后通过用户名+密码模式登陆，才能通过防火墙访问我们内部资源。

2．保证干路畅通和划分子网

网络干路是指各楼的骨干网、骨干网汇接形成的交换中心及联结 Internet 的接入线路。它的不畅通必然导致大规模的网络瘫痪，外部付费用户访问不到内部资源，这将造成极坏的影响。

在光纤干路上我们采用光纤连接主校区的各大教学楼、南院校区和 XXX 校区，主干路使用 3 对光纤做冗余。由于其它分校区离主校区比较远，光纤连入费用较高，我们采用拨号接入的方式联结。我们采用 3ComRAS1500 作为拨号服务器，分配 32 个校内电话号码给该服务器，用户只需要拨这 32 个其中一个，通过认证后，就可以动态分配一个校内的合法 IP 来访问校内的资源。在干路上，安全的隐患往往来自非技术因素，由于本市修建大学城，道路施工比较多，我们的光纤被人为的挖断;由于，某路段起火烧掉部分光纤。对于这种情况，我们采取紧急修理，租用吉通的 2M 微波通讯线路和将策略路由指向电信线路的办法来保障网路的畅通。

我们使用两台 3Com 的 CB9000 中心交换机连接各教学单位过来的光纤，并且将华中分配的 16 个 C 类地址分成为 32 个 VLan。子网的划分使安全性得到了很大的提高，同时各单位的网络组织成独立的虚网。同时，每个教学单位指定专人负责网络地址的分配，这样盗用 IP 地址的情况大大的减少了。

我们采用 3Com 的 Transcend 作为网管平台，实施对网络干路和各个子网的监控和进行网络优化。当网络有人恶意下载资源和蠕虫病毒群发邮件时，我们可以立即找出攻击源而进行相应的措施。

3．保证软件系统的安全

由于操作系统是软件系统的基础，所以，保护好操作系统是必须的，对于 Windows 系统（提供 CNKI 和 VIP 镜像等服务）保护，我们主要采取取消 Guest 帐号、取消不必要的服务（如远程注册表操作）安装诺顿防火墙和相应的杀毒软件、定时查看有无异常的程序运行等方式来保证其安全。对于 Linux 或者 Unix(提供邮件、网络计费、主页、论坛等服务)，我们关闭许多不必要的端口、定时对系统打包升级等措施来保证其安全。

对于数据库系统的保护，主要集中在保证数据的完整性、正确性和安全性方面。在数据存储介质方面，我们采用磁盘阵列、NAS、San 结合 RAID5(无独立校验磁盘的奇偶校验磁盘阵列)方式存储数据。

4．健全的安全管理机制

管理安全数字图书馆的工作状态在很大程度上取决于是否有良好的管理机制。如果制度合理、管理得当、执行得力就能有效的预防和控制安全事故的发生。反之，则会引发各种安全隐患。

我们规定工作人员每日必须检查服务器的日志，通过日志可以清楚的看到有无外来人员登陆服务器，并且做了何种修改。对重要的数据服务器，每日必须做异地数据备份。同时管理员的密码必须达到一定的长度并且每周建议修改一次。

一般而言，网络安全是网络服务效率的保障。没有了数据安全，网络服务成为无源之水；没有网络系统的安全，网络服务将成为无本之木。当然没有效率的网络传输是得不偿失的。

所以，我们要合理的规划好网络及软、硬件的合理利用。

在接入上，由于全校有 3000 多台机器也要通过该做防火墙的服务器接入 Internet，这将给该服务器造成较大的负担，同时数据传输量大时，该服务器处理速度相对将成为瓶颈。我们采取单独使用两台 Spark 主机做代理服务器，代理服务器同时启动用户认证服务，由于代理服务器的缓存保证了出校的流量大大减少，同时认证功能使得非法用户无法登陆网络。这样的冗余设计使得网络的安全性能和效能得到了大幅度的提高。

在子网划分上，连接各教学单位过来的光纤的 2 台中心 3Com CB9000 交换机之间用两根光纤作一个串口，这样跨子网的访问无需通过交换能力不强的 Cisco 路由器 7500，子网间传输数据的瓶颈问题消失了。

在数据存储上，由于我们提供 CNKI 和 VIP 等服务，这些服务器的访问量、存储的数据量都十分庞大，单个的数据检索查询都会占据大量的 CPU 时间。我们使用 SAN 和 NAS 存储大量的数据，当用户提出一个检索的申请时，检索服务将在服务器上运行，当用户提出一个下载的服务时候，下载的服务由 SAN 和 NAS 去完成，这样使得 SAN 和 NAS 的效能比磁盘阵列要高。由于 SAN 和 NAS 都可以做 RAID1~5，所以数据安全性能比普通的硬盘要高。采用新技术和冗余使得我们的网络服务效率和安全性能得到了大幅度的提高。

本项目的网络系统还有许多问题，一次网络发生了大规模的网络风暴，从子交换机扩散到中心交换机，主机与主机之间的数据传输丢包率达到了 75%几乎是不通了，最后我们发现一个施工的单位将一根漏电的线缆搭在网路上。但是为什么会造成跨虚网的网络风暴，从技术上我们无法解决，只能是严格检测各子网和主干网络是否达到屏蔽的要求，并且将电路和网路尽量的分开。