基于GAP的分布式实验室数据安全系统

黄 文 文春生 欧红星
(湖南科技学院网络中心 湖南永州 425100)

摘 要 实时交换型GAP技术是一种新型网络隔离技术,正获得越来越多的重视与应用。本文针对分布式实验数据安全问题多层次、分布性、实时性的特点,提出一个基于GAP的"安全区域"解决方案。然后阐述方案的关键技术,并给出方案的实现方法。

关键词 数据交换,网络隔离,GAP,PC104PLUS

Security System of Distributing Laboratory Data Based on GAP

HUANG Wen WEN Chun-sheng OU Hong-xin
(Network Center, Hunan University of Science and Engineering, Yongzhou Hunan 425006, China)

Abstract The real time exchange GAP is a new technology of network isolation, which is attaching increasing importance and broad application in network security. Aiming at the multi levels, distributing and real time characteristic of distributing laboratory data security problem, this paper presents a "region security" settle project based on GAP. Finally, it explains the key technology of this project, and presents a method to realize this project.

Keywords Data exchange, Network isolation, GAP, PC104PLUS

1 引言

随着Internet的迅速发展,计算机网络已经渗透到了社会生活的各个领域。目前在各高校和科研机构的实验室建设中计算机网络已经成为基础设施,几乎所有的分布实验室群都利用计算机网络进行实验数据的信息收集、加工、存储、交换等处理。但随之而来的网络信息安全问题日益突出,成为实验室数据管理中挥之不去的阴影,网络管理员正面临着最大程度地保护核心实验数据安全的课题。研究分布式实验室数据管理系统中网络安全问题的特点及相关需求,设计满足分布式实验室数据安全的网络安全系统,对现代实验室建设有重要的实际意义。

2 分布式实验室数据管理与网络安全

分布式实验室数据安全涉及的范围很广,包括实验室人员、管理制度、计算机网络安全技术等诸多方面。本文仅限于讨论计算机网络安全技术方面的问题,分布式实验室网络数据安全与实验室网络建设本身的特点、网络数据管理、采用的网络安全技术等密切相关。

分布式实验室的网络建设目前一般设计或改造为3层结构的网络连接,具有多层次的特点。首先,一个实验室的几十台计算机通过接入层交换机连接成一个小的局域网,再通过汇聚层交换机连接到实验室管理中心,成为一个部门的实验室管理专网,最后连接到部门的核心交换机上,出口至Internet。这样多层次的网络拓扑使得分布式实验室数据在网络接入的各个层次都有可能遭受攻击,给网络数据的信息安全带来很大的隐患。

分布式实验室的网络数据管理一般应遵循以下原则[1]:(1)数据库管理系统对用户透明;(2)数据库易扩充;(3)数据库便于检索;(4)数据库应有相应的用户接口。此外,数据传输必须实时,即在实验时间内,具有实时性的特点[2]。如何保证实时网络传输的数据安全,是实验室数据安全系统需要考虑的一个重要问题。

目前对于分布式实验室数据安全系统所采取的网络安全技术措施主要有FIREWALL,IDS,ANTVIRUS等。但不管是以上哪一种或几种技术均有明显漏洞。防火墙缺乏对计算机病毒的防御和对内部网络旁路的控制,入侵检测由于入侵特征库及检测规则的先天缺陷使得漏报误报难以杜绝,防病毒系统对于非法入侵无能为力。因此网络隔离系统应运而生,但是传统的网络隔离技术无论是双网卡还是多系统的网络隔离均无法满足分布式实验室数据实时传输的要求,这就要求有新的网络隔离技术支持。

3 基于GAP的分布式实验室数据安全系统结构

3.1 GAP技术概述

GAP技术最早由以色列和美国军方提出,是目前网络隔离新技术。GAP技术可分成三类[3]:实时交换类型、单向连接类型和网络切换类型。后两种类型因为适合使用的场合有限,不适合分布式实验室数据交换的多层次、分布性与实时性。实时交换类型GAP技术在两个网络中加入一个转发数据的GAP设备(GAP设备是一个在任一时刻只能物理地连接网络一端的硬件设备),使两个网络物理隔离;同时采用GAP控制技术通过GAP设备实现两个网络间的安全数据传输和资源共享,原理如图1所示。

黄 文 副教授,硕士,研究方向为网络信息安全、多媒体技术;文春生 讲师,硕士研究生,研究方向为网络管理、网络安全;欧红星 助教,研究方向为网络管理。

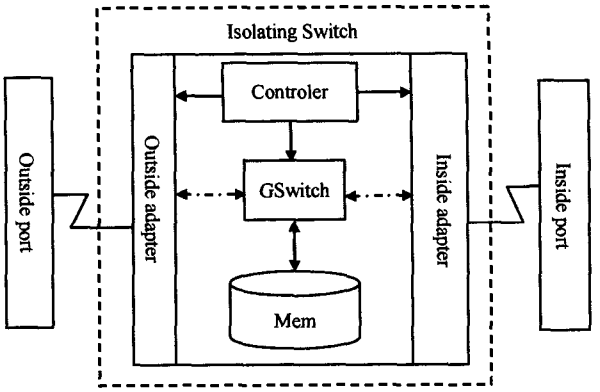

图 1　实时交换型 GAP 结构图

在图 1 中，Outside Port，Inside Port 与 Isolating Switch 构成一个 GAP 系统，外部网络通过 Outside port 与 Outside adapter 连接，内部网络通过 Inside port 与 Inside adapter 连接。在 Controler 的控制下，Outside adapter 或 Inside adapter 通过 GAP Switch 唯一地与 Mem 连接，以完成内外网的数据访问。

3.2　基于 Gap 的分布式实验室数据安全系统架构

高校或科研院所的实验室群是一个典型的涉密区，对网络安全的要求非常高。按照其多层次与分布性，这里不妨对实验室网络及相关网络从安全层次上做如下区域划分：

(1) 涉密区。各独立实验室及实验室管理中心的数据处理中心，这一层次除了收发邮件外，可以浏览信任网页，信息只进不出，成为单向连接。

(2) 核心区。实验室管理中心的数据查询中心，这是一个可信网，这一层次需要对外信息服务，但其数据绝对不能被破坏，对其访问必须经过安全性检测。

(3) 可管区。部门的行政办公网，这一层次需要保证其系统稳定工作，系统稳定性和易恢复性是最主要的需求。

(4) 不可管区。生活小区网等，这一层次以休闲娱乐为主，安全性需求最低，只要能高概率地保证其系统不遭破坏即可，但也可能被要求采用访问控制策略。

这四个安全层次的需求基本覆盖了 Internet 的全部安全层次，但实验室数据管理系统则只在涉密区与核心区，对网络安全要求极高。

利用 GAP 技术可以设计出较好的网络安全体系，能充分满足高校或科研院所内部网络多层次、分布性、实时性特点的需求。基于 GAP 的网络安全系统架构如图 2 所示。

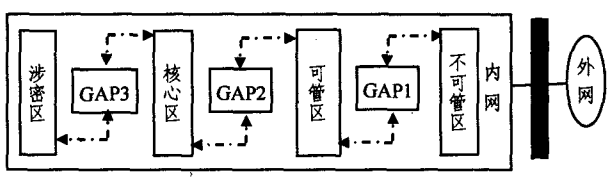

图 2　基于 Gap 的网络安全系统架构

在图 2 中，防火墙部署在外网与内网之间，构成内网的第一道安全屏障。在内网的四个安全区同时部署 IDS，作为内网的第二道安全措施。除不可管区外，在其它三个区部署网络 Antivirus 系统，构筑内网的第三道安全防线。以上措施均可采用第三方的产品和手段能较高概率地保证内网络的安全，但不具备强安全性保证。能给内网带来强安全保证的是 GAP1-GAP3 三个隔离系统，它们隔离了四个不同安全层次的 VLAN，高、低级的安全区的数据传输必须经过 GAP 设备。

这里 GAP1-GAP3 的设计相同，但在各级安全区的代理服务中必须设计不同的安全检测规则，以满足多安全层次特性的需要。同时对各区 VLAN 的 IP 和 MAC 绑定，使之满足分布式访问控制规则并能嵌入第三方检测规则，以满足内网的分布特性的需要。

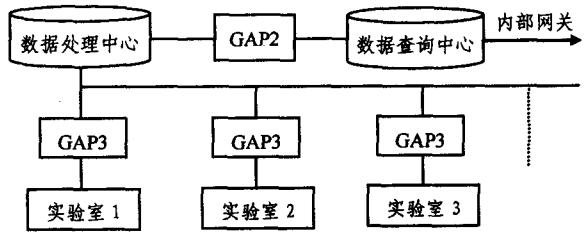

图 3　分布式实验室数据安全系统

依据图 2 图形基于 GAP 的分布式实验室数据安全系统架构如图 3。图中的 GAP2，GAP3 与图 2 中的 GAP2，GAP3 功能相同。

3.3　系统功能描述

不可管区部署外围代理服务器 WEB PROXY，不可管区用户通过 WEB PROXY 与外网连接。WEB PROXY 其实也就是一般意义上的 WEB SERVER，这一安全区不必用 GAP 隔离。首先，这一层次安全需求决定不必使用 GAP；其次，这一区域用户群体庞大，数据流量极大，GAP 切换造成的延迟对用户带宽会带来不必要的损失。

可管区部署 WEB PROXY1，不可管区的 WEB PROXY (可管区的 WEB PROXY1)根据配置将应用层数据处理后交 GAP1 的 Outside adapter(Inside adapter)，经 Controler 控制对 Mem1 进行存取访问。经 GAP1 到 WEB PROXY1 的数据，在 WEB PROXY1 中经过可管区的安全检测，连接可管区真正的 WEB SERVER1，完成从不可管区到可管区的逻辑通道。若经 GAP1 到 WEB PROXY1 的数据在 WEB PROXY1 中不能通过安全检测，则链路被安全隔离。

与前面所述相似，核心区部署 WEB PROXY2，可管区与核心区通过 WEB PROXY1，GAP2 和 WEB PROXY2 进行数据传输。涉密区部署 WEB PROXY3，核心区与涉密区通过 WEB PROXY2，GAP3 和 WEB PROXY3 进行数据传输。但是 WEB PROXY1-3 的安全检测规则是不同的，必须满足各自的安全需求，并且 VLAN 段的 IP 和 MAC 是不相交的。

这里的描述仅对 WWW 服务，对于其它服务需要相应的代理，基本原理是一致的。

4　系统主要模块的设计

实时交换型 GAP 技术目前还是网络隔离的前沿技术，国内面市的产品不多，且报价高得惊人，若按本文方案部署，耗资巨大。这里提出一个基于 PC104PLUS[4] 高速 SCSI 通讯模块的解决方案[5]，方案以成熟的 PC104PLUS 模块为硬件，配以自主开发的软件模块，能够较好地满足系统的设计要求。

4.1　硬件系统设计

本文采用 MSMS PC104PLUS 通讯模块，该模块最高存取速度为 40MB/s，支持多操作系统，PCI 接口，32k BIOS，256k DDR，是理想的 SCSI 通讯模块。本方案用两个

PC104PLUS模块分别作为GAP的Outside adapter和Inside adapter,配以电子开关,构成如图3所示的GAP。

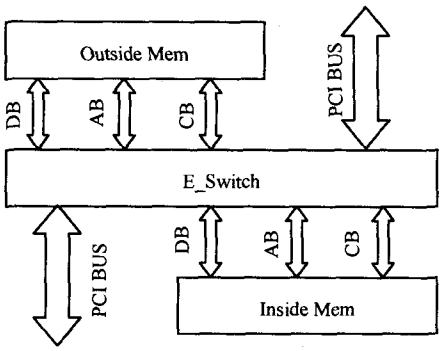

图4 基于PC104+的GAP结构

图3的核心是电子开关E_Switch,E_Switch可以通过对两个PC104PLUS模块编程来约定实现。Outside adapter的PCI BUS工作时,E_Switch连接Inside Mem,做只读操作,将Inside Port的数据读取到Outside Port。Inside Mem数据读空时,E_Switch切换到Outside Mem,做只写操作,Outside Mem满或Outside Port发送队列空则Outside adapter挂机,同时启动Inside adapter。Inside adapter的工作机制与Outside adapter相似,只是Outside Mem与Inside Mem的作用正好相反。

不管是Outside adapter还是Inside adapter,其工作状态均由另一方的挂机信号驱动,本方无自启动权限。这样就保证了在任一时刻只有一方在对Mem进行读写操作,实现了对两个网络的物理隔离。

4.2 软件系统设计

软件系统主要有二[7]:一是控制E_Switch和adapter的驱动引擎,因为本方案采用SCSI通讯模块,所以不妨称为G_SCSI。二是代理服务系统PROXY,负责真正服务器的数据转发,并且进行对接收数据的安全检测。

4.2.1 G_SCSI的设计

G_SCSI采用标准SCSI-II协议与通讯模块进行实时通讯,实现对图3所示硬件的I/O操作,包括E_Switch的切换、检测己方adapter是否启动、对Mem的读写、将己方adapter关闭同时启动对方adapter以及对读写数据按SCSI-II协议封装解封等。其流程描述如下:

(1) 检测己方adapter是否启动,是则转(2),否则等待。

(2) E_Switch打到对方Mem,有待读数据则读取数据,解封,交PROXY。

(3) E_Switch打到己方Mem,有待写数据则封装,写数据。

(4) 待写数据队列空或Mem满,关闭己方adapter同时启动对方adapter。

4.2.2 PROXY的设计

PROXY与G_SCSI接口将应用层的数据请求转发给另一个同类代理,以连接远端服务器。同时,也将接收到数据做安全性检测,将通过检测的应用服务请求连接到本地服务器。其流程如下:

(1) 检测G_SCSI接口有无数据发送,否则等待。

(2) 对接收数据进行安全性检测,通过则交本地服务器处理,否则丢弃。

(3) 检测本地服务器有无数据发送至G_SCSI,否则转(1);是则发送,直到G_SCSI写队列满。

5 系统性能分析

按照上面的软硬件设计,在嵌入式LINUX系统[5]下实现了GAP系统。系统采用两块PC104PLUS通讯模块,内核选择LINUX2.4,利用LINUX的SCSI Generic Interface[8]实现G_SCS对GAP设备的I/O操作。利用HTTP,SMTP和POP3的RFC开发PROXY代理服务。经测试,系统具备了较好的性能,达到了设计要求。

5.1 系统性能评估

(1) 安全性测试。对涉密区、核心区做攻击测试,这两个区的服务器对进行测试的5个DDOS攻击和ARP欺骗攻击软件均能成功防御,包括网管的跨段入侵尝试。

(2) 速度测试。实验平台为10M以太网,在核心区向外网群发邮件,与常规方案对比,测试结果如表1。

表1 速度测试对比结果

环境	单个2MB邮件	并发50个40kB邮件
通过GAP与PROXY	<7s	<70s
不通过GAP与PROXY	<6s	<40s

比较单个邮件发送,两者差别不大。群发时两者有明显差异,这主要是二级代理导致的速度下降。这是以速度换取安全的必然结果。

5.2 与普通实验室信息管理系统的安全性对比

目前流行的普通的实验室信息管理系统在安全性方面只是设置了权限管理,无法满足重点实验室对数据的安全性要求。我们对一个著名的实验室信息管理系统由网管用ARP欺骗进行攻击,轻松获取全部实验信息,这种攻击对部署了GAP的管理系统是无效的。

结束语 系统利用GAP技术,将内网进行安全区隔离,较好地解决了分布式实验室网络多安全层次、分布性和实时性的安全问题。不过,本文的方案对1000M主干内网明显带宽不够。改进办法可以采用其它的高速通讯模块,目前PC104PLUS模块国内最高带宽已达到400M/s,国外已有800M/s以上带宽的模块面市,基本可以满足需要。

参考文献

[1] 慕强,丁晓玲. 国家重点实验室网络安全及防范措施. 实验技术与管理,2004,21(5):67-70

[2] 罗家融,季振山,熊斌,等. 一种大规模分布式实验数据管理系统. 测控技术,2000,19(10):16-18

[3] Bobbitt M. (Un) Bridging the Gap [J]. Information Security, 2000,3(7):35-47

[4] PC/104 Embedded Consortium. PC104 Specification (version2.5)[EB/OL]. http://www.winsystems.com/specs/pc104spec.pdf, 2005-06-08

[5] 陈睿,田忠和. 物理隔离网闸数据交换技术的研究. 计算机与数字工程, 2005,33(2):47-49

[6] 岳红梅,石冬雪,等. 基于嵌入式LINUX的网络隔离系统研究与实现. 计算机工程与应用,2005,40(5):141-143

[7] 邹思轶. 嵌入式Linux设计与应用[M]. 北京:清华大学出版社,2002

[8] Gilbert D. The Linux SCSI HOWTO[EB/OL]. http://linux.cis.nctu.edu.tw/docs/woven/HOWTO/SCSI-HOWTO.html, 2005-07-13