基于物理隔离的安全网闸研究与系统设计*)

屈 波 熊前兴 吴业福 李玉强 陶 强
(武汉理工大学计算机科学与技术学院 武汉430063)

摘 要 基于物理隔离的安全网闸技术是一种新型安全技术,它能够防止已知或未知的针对网络层和操作系统层的攻击,并在内网与外网物理隔断的同时,提供内外网间安全的、实时的数据交换环境。文章分析了基于物理隔离的安全网闸技术,将其与传统网络安全技术进行了对比分析,指出了这种安全技术的优点,并根据其数据交换的基本原理,提出了实现基于物理隔离的安全网闸的方案。

关键词 物理隔离,安全网闸,防火墙,入侵检测

Study of Security Network Gap Based on Physics Isolation

QU Bo Xiong Qian-Xing WU Ye-Fu LI Yu-Qiang Tao Qiang
(School of Computer Science and Technology, WUT, Wuhan 430063)

Abstract The technology of Security network gap based on physics isolation is a new kind of security technology, which can prevent the known or the unknown attak aiming at the network layer and OS layer, and it can also provide a security and realtime data exchange environment between the internal network and the external network when they are disconnected. This paper analyzes the security network gap technology based on physics isolation, and indicates its advantage after comparing this security technology with the traditional security technology. At the same time, according to the primary principle of its data exchange, this paper also brings forward the project of realizing security network gap based on physics isolation.

Keywords Physics isolation, Security network gap, Firewalls, Intrusion detection

1 引言

随着政府上网工程的不断开展,计算机及网络泄密案件(主要指政府机密信息泄漏)逐年增加,物理隔离[1,2]这一技术应运而生,相继而来的便是基于物理隔离的安全网闸的出现。物理隔离是相对使用防火墙、入侵检测等传统的网络安全技术进行逻辑隔离而言的,是指涉密网与公共信息网彼此完全隔开断绝,两个网络之间不存在数据通路。通过这种方式,涉密网的信息无法与公共信息网进行交换,从而保证了涉密网络内部的安全。然而这种安全是有代价的,涉密网与公共信息网完全物理隔离,涉密网就成为一个信息孤岛,这当然不是我们信息化建设所需要看到的。在提高系统安全性的同时,我们需要采用很多传统安全技术来增强系统的安全性,比如防火墙技术,入侵检测技术,防病毒技术等,而这些技术都是基于逻辑检测的,它们对未知攻击、未知病毒的防范上显得捉襟见肘,力不从心,往往会使整个系统处于不安全状态。而基于物理隔离的安全网闸(可简称为安全网闸)技术却能够很好地解决这些问题。

2 安全网闸技术与传统安全技术

2.1 安全网闸的技术分析

安全网闸,它创建一个这样的环境,内外两个网络物理断开,但逻辑地相连。安全网闸在这两个网络之间创建了一个物理隔断,这意味着网络数据包不能从一个网络流向另外一个网络,并且可信网络上的计算机和不可信网络上的计算机从不会有实际的连接。对于有连接的PC,黑客使用各种方法,通过网络能够建立连接来对它们进行控制,然而物理隔断却能杜绝这种情况发生。

安全网闸除可以实现物理隔断外,还可以允许可信网络和不可信网络之间的数据、资源和信息的安全交换。安全网闸带来的最大好处:物理隔断使可信网络安全同时允许在线式实时访问不可信网络。

安全网闸在物理链路层面通过网络开关高速连接两边网络,它物理上决定了用户不可能在两个网络之间保持一个稳定的链接。这样用户的应用仍然是透明的,但底层的传输已经完全改变。确实,黑客完全可能攻陷了外部应用服务器,但即便如此,由于开关的单一连接性,他也无法利用安全网闸为跳板,连接进涉密网服务网络中,这就从根本上保证了涉密网的安全。

2.2 安全网闸技术与传统安全技术的对比分析

传统的安全技术[3,5,6],其安全保护是基于逻辑

*)该课题得到湖北省自然科学基金项目(编号:2002S2047)的资助。屈 波 在读硕士,主要从事计算机应用支撑技术和电子商务方面的研究。

检测的。防火墙通过过滤规则来检测进出的数据包是否合法；防病毒通过病毒库的特征码来判定是否感染了病毒；NIDS 通过匹配规则库来判定是否有黑客入侵等等，这些产品的保护方法无一例外都是基于一种条件判定逻辑，但是这种逻辑判定的方法有它的局限性和不完整性，比如：防火墙不能检测所有数据包的具体内容；新病毒出来前，无法做出预先的判定；同样，新的攻击手段也不能被预先了解等等。这样，传统安全产品的判定逻辑就不可能保证是没有漏洞和错误的，这就给安全留下了隐患。

因此，无论防火墙设计得如何安全，入侵检测系统设计的功能如何强大，都不能保证自身不被黑客攻破，而一旦被攻破，整个安全体系就处在非常危险的情况中，退一步，它也会成为黑客进一步攻击网内其他机器的跳板。

安全网闸采用以物理隔离交换为核心的策略，从根本上与以逻辑判定为核心的传统安全产品区分开来，从而具有更高的安全性。安全网闸能够防止已知或未知的针对网络层和操作系统层的攻击，并在内网与外网物理隔断的同时，提供内外网间安全的、实时的数据交换环境。

3 基于物理隔离的安全网闸的设计与实现

3.1 安全网闸数据安全转发框架

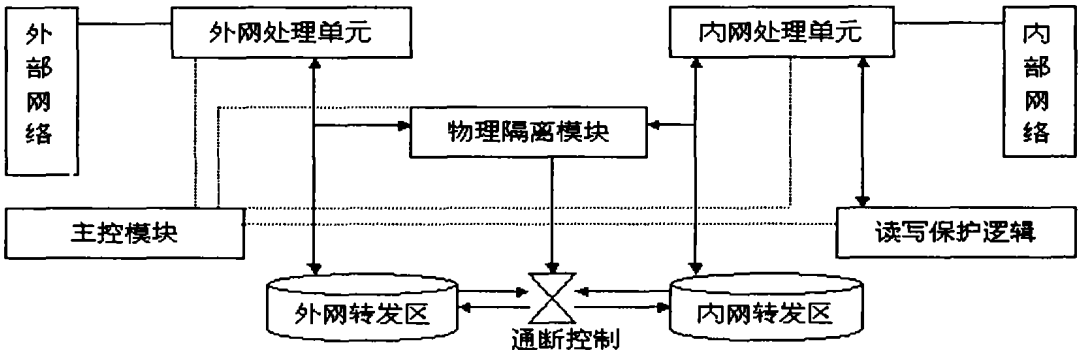

图1 安全网闸数据安全转发框架图

安全网闸数据存储转发的构架[1,2,4]由外网处理单元、数据转发区、内网处理单元、物理隔离模块、通断控制电路、读写保护逻辑、主控模块等功能部分组成。其中：

(1)主控模块主要协调各个功能部分的统一工作。同时还能集成安全操作系统、入侵监测内核、病毒查杀技术、身份认证、访问控制和安全审计等多种安全技术，以实现对内外网之间转发数据的类型、内容等进行严格的检查和过滤。

(2)数据转发区或称中间缓冲器，负责内外网数据的暂存、转发工作。在数据交换的过程中，内网处理单元把数据导出到内网转发区或者外网处理单元把数据导入到外网转发区，而内网转发区与外网转发区是否有数据交换由物理隔离模块根据用户的转发权限决定。用户没有数据转发的权限时，外网转发区与内网转发区是完全隔断的。

(3)外网处理单元或称为数据采集器，负责对外网数据目标的确定、采集工作，由内网用户需求而定，例如指定访问目标的网站、网页、邮件地址等。

(4)内网处理单元或称数据分析器，将按照预先给定的安全计划(公共的、扩展的、限制性的)对进出的数据内容进行扫描分析、筛选过滤。来自于外网的 HTTP，FTP，SMTP 数据或发往外网的 HTTP，FTP，SMTP 数据，如果违反既定安全规则就被阻止进出。

(5)通断控制电路负责控制内网转发区与外网转发区的线路连接，同时控制对数据转发区中的数据进行转发或清除。通常，只有授予数据转发权限的用户和角色，在通过物理隔离模块检查后认定数据转发权限与对象列表中的权限相符的情况下，通断控制电路才会连通内外转发区，并按其数据流向实施数据的转发工作。

(6)读写保护逻辑负责控制内网处理单元中的导出数据是否写入内网转发区，以及外网处理单元所采集的导入数据是否可从内网处理单元转播至内网。数据转发前，网络管理员通过设置内容 ID、用户 ID、特征 ID 等一些 Exchange 参数类的关键字；数据转发时，要求在用户填写 Exchange 域；读写保护逻辑监视这些关键字来决定将内网处理单元中的导出数据写入内网转发区，或者将外网处理单元所采集的导入数据读到内部网络中。

(7)物理隔模块实现在物理传导上使内外网络隔断；在物理辐射上隔断内部网与外部网；在物理存储上隔断两个网络环境。物理隔离模块被设置在最低的物理层上，内外网的数据转发由物理隔离模块操纵通断控制电路来执行，在同一时段内，物理隔离模块只能接受来自内网处理单元或者外网处理单元转发数据的请求，不能同时接收来自内网处理单元和外网处理单元转发数据的请求，使内网转发区和外网转发区双向进行数据转发操作。而且它的失效

只会影响内外网数据交换的性能，而不会影响内网的安全性。

3.2 安全网闸的设计实现

根据图1中数据安全转发的框架图，我们可以设计并实现一安全网闸的原型，其体系结构如下图2。

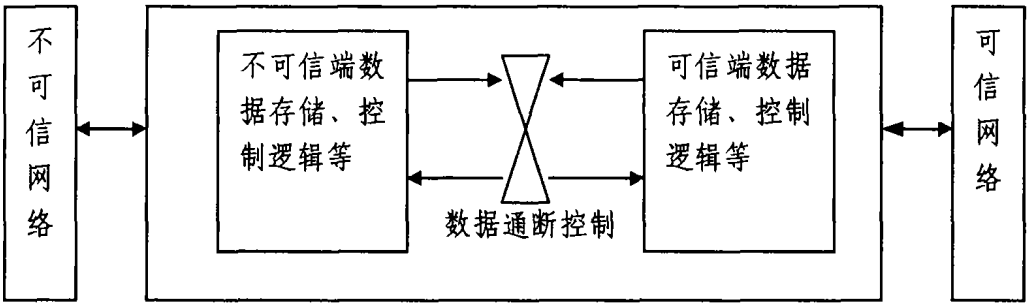

图2 安全网闸体系结构

具体实现采用的是“2+1”模式实现，即通过两台所谓的单边计算机主机和一套固定介质存储系统的隔离开关来实现整个系统，其体系结构见图2。不可信端数据存储、控制逻辑指的是连接不可信网络的单边计算机主机，而可信端数据存储、控制逻辑指的是连接可信网络的单边计算机主机，在两台单边计算机主机之间有一套固定介质存储系统的隔离开关来实现通断控制和数据转发。

所谓的单边计算机主机，是相对于传统的防火墙和网络设备而言的。传统的防火墙和物理设备，网络的数据从一边流入，经过 OSI 模型的某层或多层处理后，从另一边流出。而网络上的数据包经单边计算机主机处理后只能停留在应用层，并被还为文件数据，然后脱离 OSI 的网络模型，采用非网络方式进行文件数据交换。网络上的任何行为，无论是正常的，还是非正常的，都到此为止。

连接不可信网络的单边计算机主机只有连接不可信网络的网卡，没有连接可信网络的网卡，该主机是安全网闸在外网和不可信网络上的“代理”，它是属于不可信网络的一部分，可信网络如果需要信息，会以“代理”的名义去互联网上获取信息，通过这种方式，可以保护可信网络。

连接可信网络的单边计算机主机只有连接可信网络的网卡，没有连接不可信网络的网卡，该主机是安全网闸可信网络的连接点，属于可信网络的一部分。所有的可信网络的计算机要获得互联网上的信息，都必须通过这台主机来“代办”。这台主机并不算简单的代理所有的请求，而是执行严格的安全策略来处理访问请求。它从固定的地方取回请求的文件信息，检查请求回来的数据是否安全或带有病毒，建立内部的 TCP/IP 网络连接，将文件数据发回给请求者。

基于固态存储介质的网络开关是物理隔离的核心。连接不可信网络的单边计算机主机和连接可信网络的单边计算机主机是永远断开的，因此安全网闸是物理隔离的。隔离开关在逻辑上是由两个开关组成，一个开关处在连接可信网络的计算机和 dump 固态存储介质之间，我们称其为 Switch1，另一个开关处长连接不可信网络计算机和 dump 固态存储介质之间，我们称其为 Switch2。Switch1 和 Switch2在任何一个时候至少有一个是断开的，即 Switch1×Switch2＝0，这是物理上固定的，不受任何控制系统的控制。

从不可信网络发送数据到安全网闸的连接不可信网络的单边计算机主机上，在那里基于 TCP/IP 的数据包被拆除，然后裸数据被通过固定介质存储系统的隔离开关以硬件数据反射方式传送到连接可信网络的单边计算机主机上，在那里将已被按照内部格式重新编码的数据块，通过固定介质存储系统的隔离开关送到连接可信网络的单边计算机主机的内存缓冲区中，再由计算机对数据进行处理，如可以进行内容审查、病毒检测等项工作，安全数据在这里被重新加装成 TCP/IP 数据包，然后将数据包按照其目的地传送到可信网络上。所有数据通断控制的逻辑由硬件控制，不能被软件修改，即使在不可信网络上有计算机黑客恶意操控和攻击内部的可信网络，但也无法通过安全网闸实现其目标。

安全网闸数据交换直接通过数据通断控制硬件实现，是不依赖任何网络协议和 OS 服务，因此它的后端能防止已知的和未知的基于网络层和 OS 层的攻击。

3.3 实现方案

笔者参加了某电子政务网络安全的设计与实施，采用了如图3所示的网络安全解决方案。传统应用中，通常把各项服务器放置在防火墙的 DMZ(停火区)来对外提供服务，但防火墙的 DMZ 区在黑客的攻击下可能被攻破，导致服务器直接面临黑客的攻击。在 DMZ 区安装安全网闸可保证对外服务的服务器更安全。

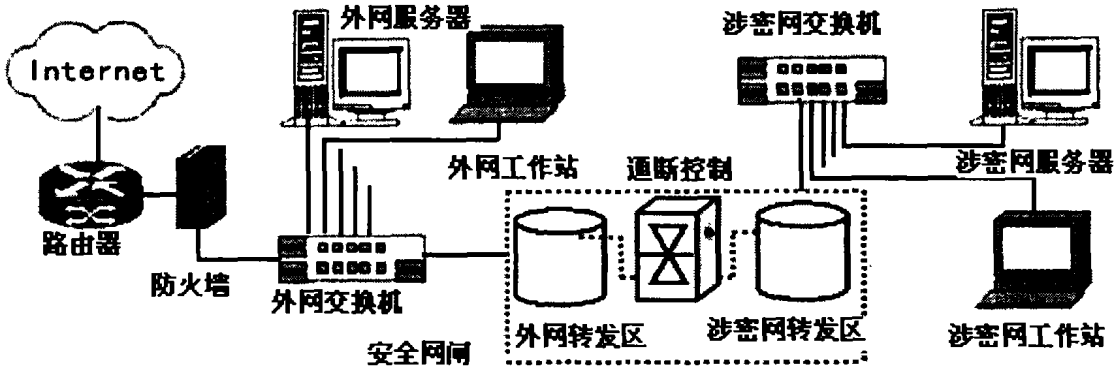

图3 在某电子政务中安全网闸的具体应用

结束语 随着政府上网的规模不断扩大，以及电子政务对安全要求，使得对基于物理隔离的安全网闸的研究如火如荼，国内外出现了一些安全网闸产品，但它们仍然面临着数据吞吐量、支持并发用户数等的限制。这并没有影响其发展，它已成为与传统安全产品相配合使用的构筑安全电子政务的网络设备。我们希望在未来的研究中，使安全网闸技术更加成熟。

参 考 文 献

1 Liu Peng, Jajodia S, McCollum C D. Intrusion confinement by isolation in information systems[J]. Journal of computer security 2000,(7):23～28

2 Bass T. Intrusion detection systems and multisensor data fusion [J]. Communications of the ACM,2000,(2):35～40

3 陈科，李之棠. 网络入侵检测系统和防火墙集成的框架模型[J]. 计算机工程与科学，2001,23(2):26～28

4 张薄生. 基于物理隔离的数据交换及安全性研究[J]. 中国数据通信，2002,(5):19～22

5 Ziegler R L 著. 余青霓，周钢译. Linux 防火墙[M]. 北京：人民邮电出版社，2002

6 Saadat Malik 著. 王宝生，朱培栋，白建军译. 网络安全原理与实践[M]. 北京：人民邮电出版社，2003

(上接第221页)

3 水印检测

针对本文的数字水印嵌入算法，满足文[5]中的水印检测要求。我们可以通过文[5]中的检测技术进行水印检测。我们随机取1000个样本，其中第500个为原水印置乱序列。设定水印相关性检测的相关度最大峰值为 T。应用 matlab 进行仿真各种攻击，相关度检测结果如下：

同时，我们还对嵌入水印后的图像进行了(5 * 5)中值滤波攻击、拷贝攻击、jpeg2000压缩和旋转几何攻击的试验，然后对检测出的水印序列做相关性测试，检测结果如下：

各种攻击：	5 * 5中值滤	拷贝攻击	剪切攻击(剪切率15%)	jpeg2000压缩	旋转180度
阈值 T	6.5	7.6	6.5	6	4.5

结束语 本文提出一种基于小波包分解的数字水印算法。可以根据不同频带的特点及其抗攻击性，将经过加密的水印信息嵌入到特定的频带内。本文的水印嵌入算法可以很好地抵抗拷贝、滤波、剪裁等攻击，对常见的 jpeg 压缩也有很好的鲁棒性；特别是对下一代静态图像压缩标准(jpeg2000)具有不错的鲁棒性。

参 考 文 献

1 潘蓉，高有形，等. 基于小波变换的图像水印嵌入方法[J]. 中国图象图形学报，2002,7

2 曹长修，柏森，张邦礼. 改进的图像小波域水印嵌入算法[J]. 贵州科学，2002,12

3 Zhu Wenwu, Xiong Zixiang, Zhang Ya-Qin. Multiresolution Watermarking for Image and Video. IEEE TRANSACTION ON CIRCUITS AND SYSTEMS FOR VIDEO TECHNOLOGY, JUNE 1999,9(4)

4 刘九芬，等. 数字水印中的双正交小波基. 中山大学学报(自然科学版)，2002,7

5 Cox I J, Miller M L, Bloom J A. Digital Wtermarking. Morgan Kaufmann Publishers, 2929 Campus Drive, Suite 260, San Mateo, CA 94403, USA, 2002