文章编号:0438-0479(2004)S-332-04

办公业务网信息监控系统设计

吴晓昶,李名世
(厦门大学计算机科学系,福建 厦门 361005)

摘要: 政府办公网络可以划分为两种类型:办公内网(涉密办公网)和办公外网(非涉密办公网). 前者与互联网物理隔离,后者则采用逻辑隔离. 两者对信息安全都是高度敏感的,加强对办公网信息的监控显得尤为必要. 办公网存在的某些安全问题是一般的网络安全系统无法解决的. 本文设计了政府办公业务网信息监控系统的基本框架,内容涉及受控计算机标志信息的收集、涉密网中违规接入互联网的监测、办公外网中异常占用带宽的监控,并对其中的关键技术问题提出解决方案.

关键词: 电子政务;办公业务网;信息监控系统;物理隔离;带宽监控
中图分类号: TP 393 **文献标识码**:A

办公业务处理的自动化网络化已成为发展的大趋势. 政府办公业务网可分为办公内网(涉密办公网)和办公外网(非涉密办公网)两种类型. 两者都包含了对安全高度敏感的信息. 而当前计算机信息网络管理存在的问题相当突出,涉密办公网没有切实做到与非涉密网物理隔离,非涉密网中也经常存在着某些人异常占用带宽的情况,造成办公业务无法正常开展. 这些问题是一般的网络安全系统无法解决的,因此需设计一个系统对办公业务网进行监控,保证涉密办公网和非涉密办公网的安全和正常使用.

1 系统体系结构与功能模块

系统的体系结构如图 1,整个监控系统包含以下几个方面的基本功能:

1) 受控计算机标志信息的收集.

2) 对办公内网(涉密办公网)中违规接入互联网的行为进行监测,使涉密网切实做到与互联网物理隔离.

3) 对办公外网(非涉密办公网)中异常占用带宽,导致正常办公业务无法顺利进行的行为进行监控,保证非涉密网的正常使用.

收稿日期:2004-05-09
作者简介:吴晓昶(1982 -),男,硕士研究生.

2 受控计算机标志信息的收集

首先应当严格界定受控对象,即受控计算机的范畴,可能是全部的内网或是各部门的专网等,这是规划系统建设规模和设计网络拓扑结构的依据.

为实现监控首先需对受控计算机进行基本的数据登记,收集所监控的计算机信息. 这些信息包括计算机名、计算机 IP 地址、网卡 MAC、CPU 序列号、硬盘序列号,计算机的使用者的姓名、身份、联系方式等等,形成了较为完整的档案. 对该档案数据进行管理,可以了解和掌握受控计算机的使用和流向情况,将泄密风险减少到最小.

在收集一般信息的同时,应该收集计算机涉密级别信息. 因为在专网中,不同的机构部门可能保密程度不同,不同的计算机也需要对应运行处理及保存不同保密级别的信息数据,有的计算机甚至可能不涉及保密数据. 因此,需要对每一台计算机的涉密级别进行判断并收集相关的信息,这对以后对每一台计算机进行针对性的处理具有很大的参考意义.

对以上信息,可以使用人工方式收集并由网络管理员将数据登记到数据库中. 也可以通过计算机的注册认证机制来收集,其中计算机的相关信息可以由分发到每个受控计算机终端的注册认证软件自动完成收集,计算机用户的相关信息则由软件提供一个方便的交互式界面,由计算机的使用者配合提供. 收集到的信息传送给设置在监控中心的信息管

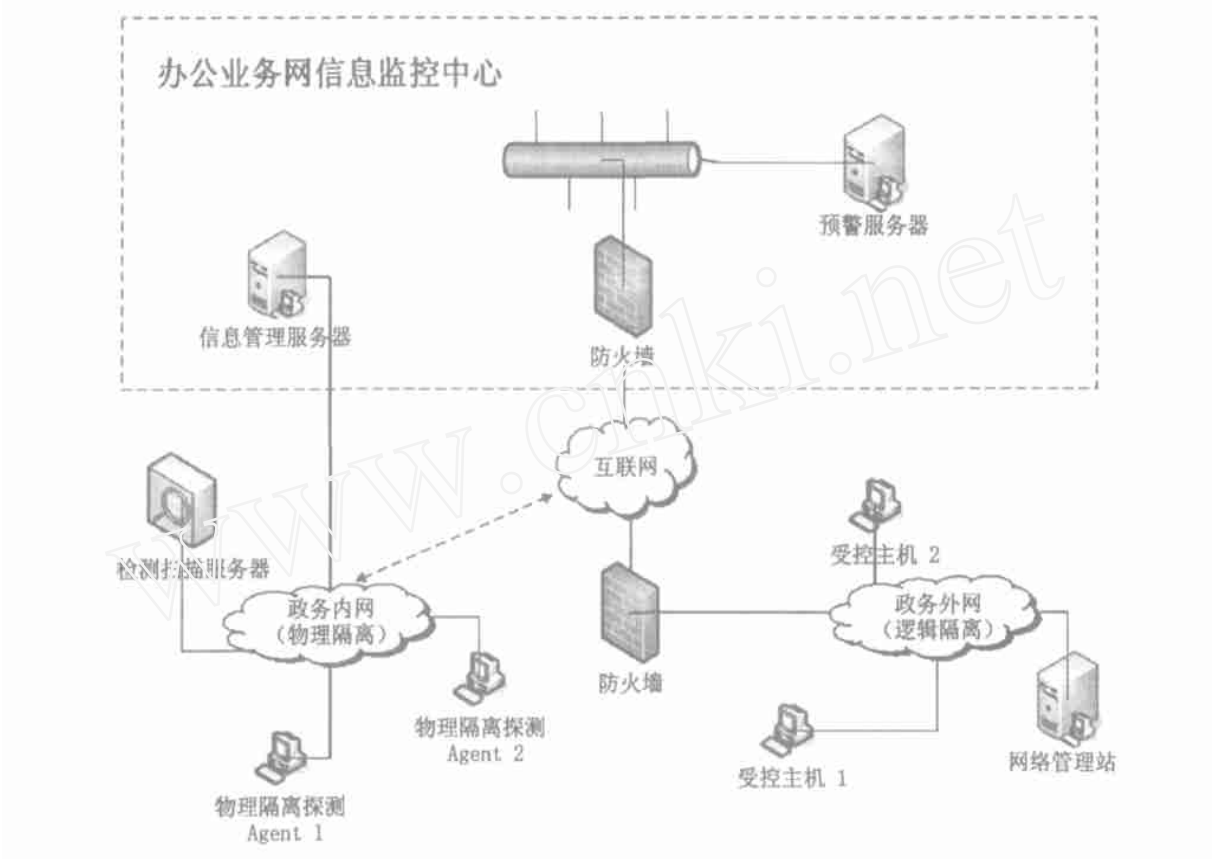

图 1　办公业务网信息监控系统体系结构图

Fig. 1　The architecture of official business network information monitoring system

理服务器,在信息传输过程中应采用加密校验机制以防止网络监听.

以下给出在 Windows 平台下收集其中一些标志信息的技术途径:

1) 使用手工收集方式

(a)计算机名,IP 地址,网卡 MAC:在命令行终端下使用 ipconfig/ all 命令可显示计算机名、每块网卡的 IP 地址和 MAC. (b) CPU 序列号:早期 CPU 产品无序列号,CPU 序列号只对 Intel PIII 以上的 CPU 有效. 可使用 Intel 公司开发的 Intel Processor Frequency ID Utility[1]软件来读取 Intel CPU 的序列号. (c)硬盘序列号:可以使用 DiskId32[2]或其他软件来读取硬盘序列号.

2) 使用开发的注册认证软件来收集

软件实现时可利用 Windows 操作系统提供的 API 函数来获取所需的计算机信息. (a)计算机名:使用 gethostname 函数可获得主机名(b) IP 地址:先使用 gethostname 函数获取的主机名,然后使用 gethostbyname 函数从主机名获取主机信息,函数返回值是一个 hostent 结构,该结构的 h-addr-list 成员包含了主机的 IP 地址列表. (c)网卡 MAC:调用 IPHelper API 中的 GetAdaptersInfo 函数可返回一 IP-ADAPTER-INFO 结构,该结构的 Address 成员为网卡的 MAC 地址. (d) CPU 序列号:可参照 Intel 公司的文档 AP-909: Intel Processor Serial Number[3],通过汇编指令来读取 CPU 序列号. (e)硬盘序列号:读取硬盘的物理序列号需要从操作系统的 Ring3 切换到 Ring0 特权级下,并使用 I/O 指令来读取,但不是所有的硬盘都有物理序列号,具体实现时可参照 DiskId32 的源代码[2].

由于这些标志信息具有可修改性和不确定性,如机器名、IP 地址、网卡物理地址都是可修改的,而 CPU 序列号和硬盘序列号具有不确定性,并不是所有的主机上都有,实践中应该综合利用这些特征数据来辨识违规主机.

3　涉密网中违规接入互联网的监测

政务办公内网即涉密办公网中承载着数量庞大的政府信息数据,有很多信息都是需要保密的. 如果

专网中有计算机通过某种手段直接或间接连接到互联网,那么,无疑给互联网中的计算机从专网窃取数据信息打开了一扇门,整个专网的信息数据安全都将受到巨大的威胁.另一方面,来自互联网的病毒、网络攻击也将直接威胁到专网的安全.因此,严格地保证专网计算机不得访问互联网并对其进行管理监测非常重要.因此,涉密专网都与互联网实施了物理隔离.任何外部攻击都无法存取政务内网内部资源,在物理信道上隔断两个网络环境.

一种方法是使用监控方式,信息监控系统应向受监测的每台专网计算机分发注册软件,专网计算机都通过注册认证的方式上报信息,确认身份,接受管理.通过注册的专网计算机中将安装物理隔离探测代理(Agent).该 Agent 将定期通过往特定的端口发出特征数据与信息监控中心设置在外网的预警服务器联系.该方法具有隐蔽性和穿透性,预警服务器通过判断是否有特征数据发送给它来确定主机是否非法外联.除支持监控方式外,还可以使用扫描方式的物理隔离检测.这种情况下,必须在专网内部设置一个检测扫描服务器,对专网计算机进行循环扫描,扫描速度、频度可根据管理员的要求设置调整.扫描服务器向管理范围的计算机发送特定的指令,计算机接收到指令后,Agent 根据该指令要求向设置在监控中心的预警服务器发送特征数据,通过预警服务器是否收到特征数据判断是否有专网计算机违规外连.

进行物理隔离检测时,无论采用哪种方式,都需要在受控主机上安装 Agent,预警服务器才可能通过特征数据检测用户是否接入外网.为了避免用户卸载掉 Agent,势必要在专网内部设置检测扫描服务器,通过定期扫描的"心跳机制"监测 Agent 的存在.

通过这种方式可以对任意的违规外联情况进行报警监测,包括专网计算机通过网卡连接专网的同时通过其他网卡或 Modem 拨号访问互联网;专网计算机断开与专网的连接并通过网卡或 Modem 拨号访问互联网;专网用户携带专网计算机到专网外访问互联网;互联网用户通过拨号非法访问专网等.

对于违规外联的计算机,预警服务器可以和 Agent 配合对其进行处置及阻断,具体的方式包括:弹出信息提示、重新启动该计算机、强制关闭计算机等;也可根据具体情况设置为不作处置.

4 办公外网中异常占用带宽的监控

鉴于严格的物理隔离在保障安全性的同时,也将对电子政务某些业务的展开带来负面影响.因此对政务办公外网某些环境可以实行逻辑隔离的方式.办公外网中某些人异常占用带宽导致正常办公业务无法顺利进行是机关中存在的突出问题.

对网络带宽进行监控可采用网络监听和协议分析机制,在专网网络主交换机中增加一台网络管理站即可.通过端口映像将其他端口的流量映像到管理站的端口,管理站就可以监听到所有的网络通讯情况;当网络管理站的网卡状态设成混杂模式时,它就对所碰到的每一个帧都产生一个硬件中断,通知操作系统响应,监听程序就可以收集到这些信息,并捕获通过的数据帧.然后通过协议分析从捕获的原始数据帧中提取出需要的信息.通过对监听到的 IP 数据报进行协议分析可以得出某个 IP 地址的主机在一定时间内收发的数据包个数和大小,从而得到该主机在这段时间内的平均带宽.

另一种方式是通过 SNMP 协议中的 Get 命令来对网络设备的状态进行查询.将 Get 命令封装在 SNMP 协议报文中发送给网络设备(如交换机、路由器等)上的代理,代理根据请求查询相应的网络设备的状态,并向管理站返回响应报文.管理站从响应报文中就可以获得所需的网络参数.一般的交换机上面都实现了 SNMP v2 和管理信息库 MIB II,从接口组(interfaces group)中 if Table 表中的 if InOctets 和 if OutOctets 列可以得到到目前为止各个接口发送(if OutOctets)和接收(if InOctets)的数据包个数.根据在一段时间内收发数据包个数的变化和这段时间的长度就可以计算出这段时间内接口的平均带宽.

通过协议分析和 SNMP 获知网络带宽状况后,可进行实时反馈控制,包括:1)利用 Windows 操作系统提供的信使服务通过发送网络消息的方式来对用户进行警告.2)通过网络攻击的方式来中断非法用户的网络.3)一般的可网管的网络设备如交换机和路由器等都可以通过 Telnet 进行远程登陆配置,可以通过用程序模拟 Telnet 协议的方式来对这些设备进行配置,对不同的情况发出不同的配置命令,从而动态改变网络环境,对带宽进行限制.4) SNMP 配置:许多可管的网络设备都支持 SNMP 协议,可以通过标准的 SNMP 的 SET 命令来对网络设备进

行配置[4].

5 结 束

本文讨论了办公业务信息监控系统的基本设计,内容涉及受控计算机标志信息的收集、涉密网中违规接入互联网的监测、办公外网中异常占用带宽的监控,并对其中的关键技术问题提出解决方案,初步建立了一个实用、保密、可靠、高效的监控系统原型.

参考文献:

[1] Intel Corporation. Intel Processor Frequency ID Utility. http://www.intel.com/support/processors/tools/frequencyid/,2002-09-20.

[2] WinSim Inc. DiskId32. http://www.winsim.com/diskid32/diskid32.html,2003-11-25.

[3] Intel Corporation. AP-909: Intel Processor Serial Number. http://developer.intel.com/design/pentiumiii/applnots/245125.htm,2000-02-25.

[4] 吴晓昶,李名世. 网络流实时监控系统研究[A]. 2003'全国计算机新科技与计算机继续教育论文集(中集)[C]. 成都:西安交通大学出版社,2003.6-8.

[5] 唐正军,田仲,王兵,等. 网络入侵检测系统的设计与实现[M]. 北京:电子工业出版社,2002.

[6] (美)马赛厄斯,海因,戴维,格里菲思. 简单网络管理协议的理论与实践[M]. 邢国光,杨永亭,王培良,译. 北京:国防工业出版社,1999.

Information Monitoring System Design in Official Business Network

WU Xiao-chang, LI Ming-shi

(Dept. of Computer Science, Xiamen Univ., Xiamen 361005, China)

Abstract: There are two types of official business network: private official business network (confidential official business network) and public official business network (non-confidential official business network). The former must be isolated physically from Internet and the latter should be logically isolated. For both, the information is sensitive. So it's necessary to intensify monitoring the information of them. This paper discusses the basic design of the official business network information monitoring system, covering the information collection of controlled computers and the monitoring of invalid access to Internet in confidential network and exceptional bandwidth in public official business network. Solutions of the key problems are found.

Key words: e-government; official business network; information monitoring system; physically isolation; bandwidth monitoring