文章编号:1006-7639(2011)-02-0257-04

浅析气象信息网安全策略及技术

孙志强, 贾海源, 朱恩超

(甘肃省天水市气象局,甘肃 天水 741000)

摘 要:随着互联网络技术的发展,气象信息网络的规模越来越大,在信息处理能力提高的同时,基于网络连接的安全问题也日益突出。本文在分析气象信息网安全需求的基础上提出了气象信息网基本安全策略,并引入了相应的安全技术。

关键词:信息网络;网络安全;安全策略;安全技术

中图分类号:TP311.563 **文献标识码**:A

引 言

气象信息网是气象部门为满足本单位业务工作的需要而建造的专用网络,伴随着计算机网络与信息技术迅速发展,网络规模越来越大,使得网络从狭义的局域网络延伸到远程分支机构和合作伙伴,并通过网络扩展带来的访问便捷性促进了现代化业务设备在气象业务中越来越多地投入运行。然而,网络规模的急剧扩充以及网络访问方式的增加也为网络安全提出了新的挑战。保障网络安全,必须建立良好的网络安全策略。安全策略是网络安全的生命,是灵魂,没有正确安全策略的安全系统就像没有灵魂的躯壳,是不能够完成保障安全的使命的。本文在深入分析气象信息网安全现状及安全需求的基础上,提出了相应的安全策略,并引入了相应的安全技术。

1 气象信息网安全需求

气象信息网作为气象系统的专用网络,与同样采用互联网技术的因特网在安全需求及安全现状上有很大的区别:

(1)因特网的开放性使得网络安全难以控制,而气象信息网由于受限于接入地点和接入人员以及与公用网的隔离,安全策略部署和实施相对简单一些;

(2)因特网的主要目的是实现开放性的互联及多样性的服务,而气象信息网络的拓扑结构相对固定,业务专一,因此引入的网络设备或安全设备及相应技术满足的需求不同;

(3)因特网的最大安全威胁来自于窃取主机控制权,而气象信息网的最大安全威胁来自越权访问及信息泄露;

(4)因特网主要提供信息资源和资源共享,气象信息网除了提供信息资源和资源共享外,最主要是提供信息交换(报文发送、信息采集等),更加强调实时性。

除了上述区别之外,解决气象信息网络安全问题还需考虑气象信息网络自身的建设和发展过程,从物理安全需求、系统和应用以及数据各方面的安全防护需求、加密需求、产品的重新部署和升级需求、安全管理方面的需求考虑。信息安全防范是一个动态循环的过程,从总体上考虑气象信息网络安全问题,制定有效的网络安全策略来部署与配置各种设备,引入先进的安全技术,做好事前、事中和事后的各项防范工作,应对不断出现的各种安全威胁,从而增强气象信息网安全性能是非常必要的、迫切的。

2 气象信息网安全策略

安全策略是指在一个特定的环境里,为保证提供一定级别的安全保护所必须遵守的规则。安全策略是一套文档化的规则,用来限制由一组或多组元素组成的一组或多组与安全相关的行为。面对日益复杂的气象信息系统与日益严峻的安全威胁,通过

收稿日期:2010-08-04;**改回日期**:2010-10-22

作者简介:孙志强(1975-),男,甘肃天水人,电子信息技术工程师,主要从事气象信息网络和多普勒天气雷达工作. E-mail:gsszq@163.com

安全需求的分析和制定安全策略,把气象信息网络安全集中到最高决策层来关注与实施,从而明确如何达到预期的安全效果。

2.1 气象信息网安全设计方案

设计网络安全方案应该考虑技术、策略和管理,技术是关键,策略是核心,管理是保证。依据安全到边缘、全局安全、全程安全的设计思想,从 3 个方面设计实现气象信息网安全:事前的准确身份认证、事中的实时处理、事后的完整审计。事前的准确身份认证包括用户的用户名和密码、用户 PC 的 IP 地址和 MAC 地址、用户 PC 所在交换机的 IP 地址和端口号、用户被系统定义的允许访问网络的时间。网络攻击的防范包括常见网络病毒的防范、未知网络病毒的防范、防止 IP 地址盗用和 ARP 攻击、防止假冒 IP 地址和 MAC 地址发起的 MAC Flood 和 SYN Flood 攻击、非法组播源的屏蔽、对 DOS 攻击和扫描攻击的屏蔽等。事后的完整审计是指当用户访问完网络后,会保存有完备的用户上网日志记录:包括某个用户使用的 IP 地址和 MAC 地址、通过的交换机和交换机的端口、访问网络开始和结束的时间以及产生的流量。如果安全事故发生,可以通过查询该日志,来唯一的确定该用户的身份,便于事情的处理。

2.2 建立网络安全策略

安全体系结构[1]和安全管理是信息网络安全的核心,安全标准和系统评估是信息网络安全的基础。建立网络安全策略,应从 4 个方面予以考虑:安全检测评估、安全体系结构、安全管理措施和网络安全标准(图 1)。由于安全是一个动态过程,这 4 个方面组成了一个循环系统。安全检测与评估随着安全标准的改变而进行,评估结果又会促进网络体系结构的完善,安全管理措施也会随着其他方面的变化而增强。由于技术的进步及对网络安全要求的提高,又会促使网络标准的改变。最后形成一种动态的螺旋上升的发展过程。

2.3 气象信息网安全策略

综合上面的分析,在制定详细、具体的气象信息网络安全策略时,可以遵循以下几条基本安全策略。

(1)尽可能地考虑物理安全问题。物理安全策略的目的是保护计算机系统、网络服务器、打印机等硬件实体和通信链路免受自然灾害、人为破坏和搭线攻击;验证用户的身份和使用权限、防止用户越权操作;确保计算机系统有一个良好的电磁兼容工作环境;建立完备的安全管理制度,防止非法进入计算机控制室和各种偷窃、破坏活动的发生。

图 1 建立网络安全策略

Fig. 1 Establishment of meteorological network security strategy

在气象信息网络中考虑对重要设备、通信连路等的备份,同时提高机房的电磁屏蔽能力。

(2)加强访问控制策略。访问控制是网络安全防范和保护的主要策略,它的主要任务是保证网络资源不被非法使用和非法访问。为了加强访问控制策略,在控制用户和数据权限的同时,考虑建立基于业务流的安全模型和基于最大隔离准则的设备配置方案[2]。

建立基于业务流的安全模型。为了增强气象信息网安全,可将气象信息网上各个业务机关之间存在的信息流(包括平级业务机关在同一个网内的信息流和上下级业务机关之间跨网络的信息流)进行细致的区分,根据不同业务机关不同的安全需求,制定各信息流的安全策略,建立基于业务流的安全模型,同时严格控制除业务关系之外出现的信息流动。按这一基本策略来制定具体的设备部署与配置策略。

基于最大隔离准则的设备配置方案。应用最大隔离准则,目的是实现气象信息网中信息节点逻辑上尽量隔离,尽量避免不必要的网络联通。在建立了基于业务流的安全模型的基础上,为了防范气象信息网上的越权访问、网络监听等引起的信息泄露,在部署与配置气象信息网网络设备及安全设备时,采用基于最大隔离准则的设备配置方案。

(3)端点安全和网络安全合理、协同部署。当信息流转在网络里时,有 2 个逻辑单元在保证信息

的传递,一个是端点,一个是网络。那么网络与端点,该在哪里部署安全措施? 我们不能说在端点做和在网络做谁好谁坏,真正好的策略是需要两者的协同的。有些防护需要在网络侧做,比如发现一些服务器的漏洞,但是终端的应用需求使得不能轻易通过升级终端程序来解决,这时就需要在网络侧部署一些防攻击的手段,将攻击控制在远端。当然,也有很多防护需要在端点做,例如一些针对系统应用的,如果在网络做,会耗费大量的资源。我们需要通过合理和协同部署,实现网络对端点的识别和判断,并赋予相应的权限。

(4)加强安全管理制度,建立应急响应体系。为了快速、有效地解决气象信息网发生的恶意攻击、网络病毒发作等安全事件,在制定气象信息网安全策略时,还必须制定严格的安全管理制度,建立应急响应体系。通过安全管理制度及应急响应体系,可以提高气象信息网内人员的安全意识,增强协同处理气象信息网内紧急安全事件的能力,从而快速发现并排除网络安全引起的故障。

3　气象信息网应引入的安全技术

在以上安全策略的指导下,为了增强气象信息网的安全性,在实施过程中,必须引入以下安全技术。

(1)防火墙技术。防火墙是一种隔离控制技术,通过预定义的安全策略,对内外网通信强制实施访问控制,常用的防火墙技术有包过滤技术、状态检测技术、应用网关技术。防火墙技术在气象信息网的实际应用中,最普遍采取的手段是对防火墙、路由器等配置访问控制列表以达到限制越权访问和防止信息泄露。

(2)逆向代理技术。防火墙不宜开放过多的端口,但不得不多开放端口时最好的解决方案之一是采用逆向代理。逆向代理的位置介于互联网和本地需要开放多个端口的服务器之间。这样设置后,服务器不需要再开放大量的端口,而外界对服务器的连接请求会先经过逆向代理进行拦截和过滤,并传递给服务器。这种设计不但能让服务器在外网前隐藏起来,还能帮助确保外部的恶意请求不会到达服务器。

(3)VLAN 技术。VLAN(Virtual Local Area Network),又称为虚拟局域网,它遵循的是 IEEE 802.1Q 协议标准。它是一种不拘泥于网络中站点所处的物理位置,根据功能、应用等因素将局域网内的设备逻辑地而不是物理地划分成一个个网段从而实现功能相对独立的虚拟工作组的技术。划分的各个 VLAN 之间不能直接进行数据通信,需要借助路由器来转发数据实现 VLAN 之间的数据通信,因此,在不配置路由器的 VLAN 之间是相互隔离的,各个 VLAN 相当于一个独立的局域网。利用 VLAN 技术,可以较大程度地提高网络的安全性。VLAN 技术需要网络设备的支持,配置了 3 层交换机的气象信息网络可以按照基于业务流的安全模型对本级局域网进行 VLAN 划分,从而保证不同的业务流相互隔离,防范网络监听手段的入侵。

(4)VPN 技术。VPN (Virtual Private Network),又称为虚拟专用网,是对通过共享公用网络(如 Internet)并使用封装、加密和身份认证等技术进行连接的内部网络的扩展。提出该技术是为了方便在公用网络基础设施之上建立专用网络。在气象信息网中对路由器、防火墙等设备进行配置,采用 VPN 技术将不同节点间有业务关系的计算机连通,可以实现气象信息网中的虚拟网。由于 VPN 提供了对 VPN 隧道两端的身份认证和访问控制及对传输数据的信息加密和信息认证,因此能够有效防范截断攻击和窃听攻击。而且良好的 VPN 应用可在不同层次实现不同的 VPN 隧道协议对数据进行保护。

(5)防病毒技术。随着计算机技术的不断发展,计算机病毒变得越来越复杂和高级,对计算机信息系统构成极大的威胁。在病毒防范中普遍使用的防病毒软件,从功能上可以分为网络防病毒软件和单机防病毒软件两大类。单机防病毒软件一般安装在单台计算机上,即对本地和本地工作站连接的远程资源采用分析扫描的方式检测、清除病毒。网络防病毒软件则主要注重网络防病毒,一旦病毒入侵网络或者从网络向其它资源传染,网络防病毒软件会立刻检测到并加以删除。

(6)系统补丁程序的安装。及时地安装补丁程序也是很好的维护网络安全方法。有很多病毒就是应用了系统的漏洞,对计算机达到破坏作用。很多的“黑客”也能够通过系统漏洞侵入对方计算机,对其计算机进行破坏的。

(7)安全管理队伍的建设。在计算机网络系统中,绝对的安全是不存在的,制定健全的安全管理体制是计算机网络安全的重要保证,只有通过网络管理人员与使用人员的共同努力,运用一切可以使用

的工具和技术,尽一切可能去控制、减小一切非法的行为,尽可能地把不安全的因素降到最低。同时,要不断地加强计算机信息网络的安全规范化管理力度,大力加强安全技术建设,强化使用人员和管理人员的安全防范意识。

4 结束语

网络安全涉及技术、管理、使用等诸多方面的问题,在信息网络方面,新的技术不断超越先前的最新技术,网络安全会不断面临新的挑战。我们必须综合考虑安全因素,定期对气象信息网络安全设计进行评估,制定合理的安全策略和安全技术,积极有效地制定安全策略可以指导气象信息网的建设和安全规划以达到预期的安全效果。应用本文提出的气象信息网安全策略,并引入新型的安全技术,可以提高气象信息网的安全性。

参考文献:

[1] (美)Sean Convery 著. 王迎春,谢琳,江魁(译). 网络安全体系结构[M]. 北京:人民邮电出版社出版,2005.

[2] 郭文普,任俊. 专用网安全策略及技术研究[J]. 计算机与信息技术,2008(1):15.

Analysis of Security Strategy and Technology of Meteorological Information Network

SUN Zhiqiang, JIA Haiyuan, ZHU Enchao

(*Tianshui Meteorological Bureau of Gansu Province*, *Tianshui* 741000, *China*)

Abstract: With the development of internet technology, the extent of meteorological information network becomes more and more large. At the same time, the information processing ability is improving. The security problems based on the network connecting become outstanding gradually. This paper gives the basic security strategy and the corresponding security technology of meteorological information network.

Key words: information network; network security; security strategy; security technology

(上接第 239 页)

Application Analysis of T639 Product on a Heavy Rainfall Process in Central Tianshan Mountain

GUO Jinqiang[1], WANG Xiaojuan[2], ZHANG Zhixiong[3]

(1. *Shihezi Meteorological Bureau of Xinjiang*, *Shihezi* 832003, *China*; 2. *Key Laboratory of Oasis Ecology Agriculture of Xinjiang Production and Construction Corps*, *Shihezi* 832003, *China*; 3. *Dushanzi Meteorological Bureau of Xinjiang*, *Dushanzi* 833600, *China*)

Abstract: Based on "T_{639}" 0 field forecast product, the heavy rainfall weather occurred on May 25 – 26, 2009 in central Tianshan Mountains was analyzed. The results indicated that the convergence line, shear line and the southwest jet at the level of 700 hPa and 850 hPa were the direct influence system of this weather event, the convergence of southwest jet and the cold air formed a strong convergence of power and moisture, which played an important role for this weather process. Heavy rainfall occurred in the strong energy front, high humidity area and water vapor flux convergence zone. The effect of high and low level jet stream and middle – high frontal zone resulted in this weather event.

Key words: central Tianshan Mountains; heavy rainfall; products of T_{639}; cause analysis