广西科学院学报
Journal of Guangxi Academy of Sciences
2010,26(4):510~513
Vol. 26, No. 4 November 2010

一种基于SNMPv3协议的校园网络安全管理方案
A Security Management Solution for Campus Network Based on SNMPv3

骆参驹[1,2],杨 颖[1],张丽勇[2]
LUO Can-ju[1,2], YANG Ying[1], ZHANG Li-yong[2]

(1.广西大学计算机与电子信息学院,广西南宁 530004; 2.广西工商职业技术学院,广西南宁 530003)
(1. School of Computer and Electronics Information, Guangxi University, Nanning, Guangxi, 530004, China; 2. Guangxi Vocational College of Technical and Business, Nanning, Guangxi, 530003, China)

摘要:针对分布式校园网络安全管理问题,分析SNMPv1和SNMPv2协议在构建分布式校园网络管理模式的安全威胁,从而提出运用SNMPV3协议的安全功能和实现方法,以提高分布式网络管理的安全性,为分布式校园网安全提供一种解决方案。

关键词:网络 管理 安全 SNMPv3协议
中图法分类号:TP393.08 **文献标识码**:A **文章编号**:1002-7378(2010)04-0510-04

Abstract: For the security of distributed campus network management, it analyzes the security threats to construct the distributed model with SNMPv1 and SNMPv2 in network management. The security features and implementation methods are proposed by using SNMPv3. It improves the security of distributed network management and provides a solution for the distributed campus network.

Key words: network, management, security, SNMPv3

校园网络作为学校信息化建设重要的基础设施,担负着教学、科研、管理和对外交流的重任,其安全状况直接影响到这些活动的顺利进行。由于校园网络分散面广,安全策略定制合理性不强,导致其面临的攻击呈等比增加,数据信息被窃取和针对网络设备的攻击等潜伏着的安全威胁层出不穷。根据每年全国信息网络安全状况与计算机病毒疫情调查分析报告的统计,教育科研属于发生网络安全事件高比例的行业之一[1]。校园网络信息安全问题不容忽视。

SNMP从1990年发展至今,经历了3个版本的演变。SNMP具备设计简单、扩展灵活、易于使用的特点,得到了广泛应用。它不仅成为网络管理事实上的标准,也成为了网络设备厂商、应用软件开发及终端用户的首选管理协议[2]。本文针对校园网的安全现状,提供一种基于SNMPv3协议的校园网络安全管理方案。

1 SNMPv1和SNMPv2协议在校园网络安全管理中的缺陷

校园网络接入Internet的类型较难控制。校园网络采用集中式网络管理模式,会造成网络信息量过大,占用带宽过多,网管中心负载过重,安全策略定制合理性不强,独立的边界防火墙在校园中的部署不能达到预期安全防范的效果等缺点。校园网络采用分布式网络管理模式,将网络划分为不同的区域和层次,可以充分发挥校园网管理人员的技术优势来对学校边界安全进行管理,有效控制网络主干安全,和达到网络内部的安全防范要求。

SNMPv1协议没有提出支持分布式网络管理,SNMPv2协议支持分布式管理,一些站点可以既充

收稿日期:2010-09-20
修回日期:2010-10-08
作者简介:骆参驹(1978-),男,讲师,硕士研究生,主要从事计算机网络与并行分布式计算技术研究。

当管理者又充当代理,同时扮演两个角色。SNMPv2 协议提供了两条命令 GetBulk 和 Inform:GetBulk 的作用是减少网络管理时的带宽浪费。Inform 的作用可以提供给 Manager 和地 Manager 之间进行通讯,这有助于实现分布式的网络管理[2]。SNNPv2 协议除了提供访问控制之外,还提供私有服务(保护信息的完整性)和认证服务(确认信息来源的正确性)。但是在建构分布式网络管理模式时会出现较多安全隐患,比如:在以 SNMP 协议架构的网络管理模式中,管理站需要管理一台 SNMP 设备,首先要给设备的 SNMP 代理发送 SNMP 消息,这些消息由 SNMP PDU(协议数据单元)组成。代理接到信息,完成对网络设备的管理请求,并将应答信息返回管理站。在单一的局域网中,这些信息的流动可以看成是安全的,但是在分布式网络管理体系中,不同的管理域内存在相对独立、对等的管理者,这些管理者需要相互联系,交换管理信息,协同工作,以达到对网络的分布式管理。也就是说,一台设备不可能只允许本地管理站对其访问,因此,信息需要跨越中间网段传输。另外,SNMPv2 协议没有提供任何与访问控制相关的功能。这样安全威胁尤其体现在跨网段的信息交互和访问控制上。在这样的交互方式下可能出现安全威胁[3]:(1) 黑客可以截获发送给代理的消息并加以修改,然后再发送出去以达到对管理信息的非法访问。(2) 在跨越局域网进行远程管理或远程控制时当地设备可能会遇到管理站身份伪装,执行对 MIB 的访问操作,从而导致设备被非法控制或恶意破坏。(3) 远程管理站和本地管理站之间的通信可能会被窃听,从而造成信息泄漏的危险。(4) SNMPv2 协议并没有提供任何与访问控制相关的权限分级管理功能,造成访问权限无法划分。这些安全威胁一旦爆发,都可能会使整个网络的运行进入混乱,甚至瘫痪,重要设备的信息和正常运作得不到保护。对于目前的校园网络,分布式管理势在必行,SNMPv1 和 SNMPv2 这两个版本的协议在建构分布式网络管理时会遇到很大的安全威胁,这样造成了管理和安全之间的极大矛盾。

2 SNMPv3 协议建构分布式校园网络的安全管理方案

2.1 分布式校园网络安全管理系统功能

针对 SNMPv1 和 SNMPv2 协议脆弱的安全性能,SNMPv3 协议提供了 3 个安全功能可供开发:访问控制、数据加密、验证密码。通过对 SNMPv3 协议 这 3 个安全功能的开发,可以实现如下安全策略[4]:(1)访问控制(AccessControl)。访问控制的策略可以由校园网的管理者预先设定。SNMPv3 通过使用带有不同参数的原语来灵活地确定访问控制方式。通过通讯实体的身份判断网络管理者和代理是否有权限对 MIB 的数据进行访问。(2) 数据加密(PrivKey)。当用户身份认证合格和用户有访问权限时,才可以进行数据的传送,这时采用加密措施对需要传输的数据进行加密,从而保证其信息传输的完整性,SNMPv3 采用目前公认安全性最高的公钥加密方法。(3) 验证密码(AuthKey)。RFC2104 中定义了 HMAC,这是一种使用安全哈希函数和密码来产生信息验证码的有效工具,在互联网中得到了广泛的应用。SNMP 使用的 HMAC 可以分为两种:HMAC-MD5-96 和 HMAC-SHA-96,前者的哈希函数是 MD5,使用 128 位 AuthKey 作为输入;后者的哈希函数是 SHA-1,使用 160 位 AuthKey 作为输入。此功能可以开发实现身份验证功能。

通过开发 SNMPv3 提供的安全功能,在使用 SNMPv3 架构分布式网络管理模型时,可以制定出相应的安全策略来弥补 SNMPv2 架构下的安全漏洞。考虑运用添加安全功能模块的方法来实现相应的安全策略,具体添加的模块有管理站访问控制模块,消息安全控制模块,设备 MIB 访问控制模块等(图 1)。安全策略主要体现于这三个模块(管理站、当地设备 SNMP 代理、当地设备 MIB)之中,分布式网络管理中不同角色对应不同的安全功能模块,共同构建安全的 SNMPv3 网络管理体系[3]。(1)管理站。管理站访问控制模块限定管理站可以向设备代理发出的命令,对于分布式体系中层次较低的管理站,它们对一些重要设备可以发出的管理命令需要受到限制,这样不同管理站对设备的管理权限得到了划分。管理站的消息安全模块首先起到加密作用,对管理站向被管设备的代理或向其他管理站发出的 SNMP 请求进行加密,保证管理信息在跨越中间网段时不被非法获取,不被非法改动;其次解密传输到本地的加密 SNMP 信息流;再次就是起到身份验证的功能,保证反馈回来的信息是来源于目标设备或管理站,没有被假冒,并确认信息在传输途中没有被篡改。(3)当地设备 SNMP 代理。当地设备 SNMP 代理的消息安全模块首先起到加密作用,对代理向管理站发出的管理应答信息进行加密,保证设备信息不被非法获取,不被非法改动;其次解密

传输到本地的加密SNMP信息流；再次就是起到身份验证的功能，保证管理信息是来自有权的管理站，管理站身份没有被假冒，并确认信息在传输途中没有被篡改。(3)当地设备MIB。由MIB库访问控制模块确定有权的管理站可以访问该设备的MIB的有效部分，重要的MIB信息只有权限高的管理站才可以访问或者修改。

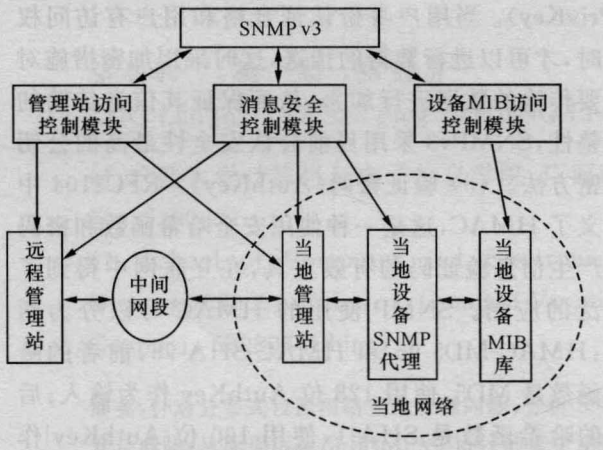

图1 SNMPv3协议架构下信息的交互方式

2.2 系统框架

校园网络络管理系统设计的目的是利用SNMPv3协议以及相关协议，试图实现校园网络管理中的五大基本管理功能：配置、故障、性能、计费及安全管理。在校园网络管理中，它的要求与目标和一般通用的网络管理系统是有很大的区别的，有不同的侧重点。本管理系统框架如图2所示。

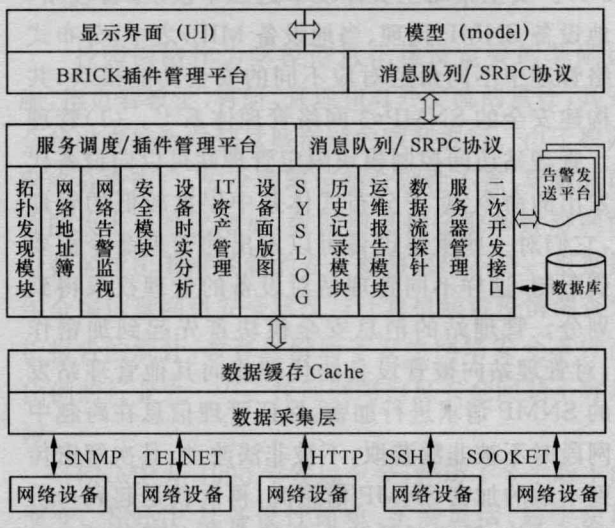

图2 分布式校园网络安全管理系统整体框架

2.3 密钥生成算法

分布式校园网络安全管理系统的客户端和服务器端都需要维护一个鉴别密钥和加密密钥，这些密钥不存在于MIB中，也不能通过SNMP消息来访问。我们可以采用RFC2574提供的方法：每个用户使用1个密码，对于不同的授权实体生成不同的密钥。这就意味着，1个用户或者1个授权实体的密钥泄露，不会危及到其他授权实体。

首先利用MD5消息摘要算法使用用户密码和snmpEngine生成出一个16字节的字符串。

```
Voidpassword_to_key_md5(char * password, int passwordlen, char * enginelD, int engineLength, char * key)
{
//算法使用通过 password 和 snmpEngineID 生成 16 字节的字符串，
//指针 key 指向生成出的字符串
MD5_CTX MD;
char * cp, password_buf[6,4];
long password_index= 0 ;
long count= 0,i;
MD5 Init(&MD); /* initialize MD5 */
while (count< 1048576){
cp = password_buf;
for (i=0;i <64; i++){
* cp++ = password[password_index++%passwordlen];
}
MD5Update (&MD,password_buf,64);
Count+= 64 ;
}
MD5Final( key,&MD);
}
```

上述过程中的MD51nit，MD5Update和MD5Final等都在RFC1321中都有所定义。调用上述过程将生成一个16字节的字符串，在这里我们称之为ku。下一步是通过MD5散列算法利用ku生成最后的密钥kul，算法如下：

```
porceduer OctetString:: GetLocalized-KeyMD5(u serName,ad dr)
{
//use rName 表示需要生成密钥的用户，addr 表示授权引擎的 IP 地址
password = GetPassword(userName)
passwordLen= LengthOf(password)
engineID =GetEngineID(addr)
engineIDLen= LengthOf(enginclD)
password _ to _ key _ md5 ( password, passwordlen,engineID,engineLength,&ku)
```

```
ku1= MD5 (ku+engine+ku);
retunr kul ;
}
```

以上过程称为密钥的本地化,服务器端(代理)为它的每一个客户端用户保存一个密钥,客户端用户的密钥在不同的服务器中是不同的,这样就可以大大提高密钥的安全性。

3 结束语

通过开发 SNMPv3 的安全功能,可以实现以上的模块所提供的安全策略。这样以 SNMPv3 协议架构分布式校园网络管理系统,体现了模块化的设计思想,可以在模块中简单地实现功能的增加和修改。对于不同的网络,用户也可以在模块中加入自定义的访问控制函数或者加密,身份验证函数,使安全性能得到进一步的完善,达到对网络的自主安全管理。

参考文献:

[1] 公安部公共信息网络安全监察局. 2009 年全国信息网络安全状况与计算机病毒疫情调查分析[C]. 信息网络安全,2009.

[2] 周启明,李方敏. 防火墙与入侵检测系统的立体防御体系研究[J]. 网络安全技术与应用,2006(5):22-24.

[3] WilliamStallings. SNMP 网络管理[M]. 胡成松,汪凯,译. 北京:中国电力出版社,2001.

[4] 李连焕. 防火墙与入侵检测在校园网中的应用[J]. 计算机与信息技术,2007(15):54.

(责任编辑:邓大玉)

(上接第 509 页)

4 结束语

在经历了 ASP 模式和 SaaS 模式发展后,PaaS 模式越来越多地受到软件厂商和用户的青睐。本文提出了基于 PaaS 模式下的电子政务信息平台架构和有关规范,并在此基础上构建省级 PaaS 平台,市、县级信息系统通过使用 PaaS 平台提供的服务和接口快速地定制、开发出个性化的政务信息系统。在遵循统一的数据结构和接口标准的情况下,PaaS 模式不但使得政务信息能得到有效共享,还能极大程度地降低了系统的开发成本和难度,对于推动政务信息化进程具有强大优势。

参考文献:

[1] 李智. SaaS、PaaS 和云计算搅动未来软件发展[J]. 中国计算机报,2008(31):B2.

[2] 曹薇,张乃洲. 企业 SaaS 应用分析[J]. 计算机时代,2010 (2):63-67.

[3] 谢琴,方芳. 基于 SaaS 形式的探讨[J]. 科技信息,2009(10):200.

[4] 温静,任铄. SaaS 模式下的信息安全探讨[J]. 电脑知识与技术,2009(18):4947-4948.

(责任编辑:邓大玉)