结合802.1x技术实现网络安全管理

刘海韬,张 浩
(中南大学 信息科学与工程学院,湖南 长沙 410083)

摘 要:网络安全管理是现代通信网络管理的重要组成部分。提供一种结合802.1x技术解决网络安全管理的方法;探讨了网络中的诸多安全问题,通过研究802.1x技术,分析802.1x技术所能解决的各种网络安全问题,提出了结合802.1x技术实现网络安全管理的整体解决方案,同时对系统的实现过程进行了详细分析,并总结该解决方案的优缺点。本系统实现后将有效减少网络中安全问题的出现,并提高用户的网络体验度。

关键词:园区网;802.1x技术;网络安全管理系统解决方案
中图分类号:TP393.08 **文献标识码**:A **文章编号**:1673-629X(2009)07-0170-03

Unifies 802.1x Technology Realization Network Security Management

LIU Hai-tao, ZHANG Hao
(Department of Information Science and Engineering, Central South University, Changsha 410083, China)

Abstract: Network security management is an important component of modern communications networks management. Intent to advance technology about unifies 802.1x technology realization network security management. Through investigating into 802.1x and analysing the network security problem which 802.1x can solve, advance a concrete solution to realization network security management. Simultaneously the systematic realization is analyzed in detailed, also, the advantages and disadvantages of this solution are summarized. After the realization of this solution, network security problem will decrease, at the mean time, people's feeling get better surfing online.

Key words: campus Intranet; 802.1x technology; network security management system solution

0 引 言

随着网络的快速发展和上网用户的急剧增多,网络中的不安全因素日益暴露无遗。由于以太网灵活性高、技术相对简单、易于实现,几乎所有局域网都采用了以太网技术构建网络[1]。但是,以太网技术构建网络却面临着很多安全问题,如:盗用合法IP,DoS,ARP攻击等。传统的网络安全管理主要依靠管理员的经验或根据某些简单的管理协议来实现,而且各种管理机制和管理设备缺乏互操作性,管理效率不高,花费的成本也大。而802.1x技术是基于Client/Server的访问控制和认证协议[2]。它可以限制未经授权的用户/设备通过接入端口访问LAN/WLAN。在获得交换机或LAN提供的各种业务之前,802.1x对连接到交换机端口上的用户/设备进行认证。因此,通过结合802.1x技术能更好地实现网络安全管理。文中将讨论结合802.1x技术实现网络安全管理的问题,并提出了具体解决方案。

收稿日期:2008-10-17;**修回日期**:2008-12-13
基金项目:国家自然科学基金(60673164)
作者简介:刘海韬(1970-),男,湖南邵阳人,副教授,研究方向为计算机网络。

1 网络安全与用户管理

网络安全可以说是一个包含多种领域的问题,既有技术性问题,也包含法律、管理、心理学等非技术性问题。从信息安全的角度出发,让第三者知道的东西越少越好。

而从网络安全管理的角度出发,第三者知道的东西越多越好。如何平衡以上两点,则需要由网络安全管理策略来决定。

广义上来说,网络安全包括网络硬件资源及信息资源的安全性。硬件资源包括通信线路、通信设备(交换机、路由器等)、主机等,要实现信息快速、安全的交换,一个可靠的物理网络是必不可少的。信息资源包括维持网络服务运行的系统软件和应用软件,以及在网络中存储和传输的用户信息数据等。网络安全从其本质上来讲就是网络上的信息安全。信息资源的保密性、完整性、可用性、真实性等是网络安全管理的主要

内容。

网络安全管理[3]的目标在于指导用户合理有效使用计算机网络,杜绝不良现象滋生、严防病毒侵入,确保计算机网络安全运行,服务于工作,服务于经济。

2　802.1x 协议分析

2.1　802.1x 访问控制过程

IEEE802.1x 的体系结构中包括三个部分:Supplicant System 客户端;Authenticator System 认证系统;Authentication Sever System 认证服务器。图 1 清楚地说明了 802.1x 技术的访问控制过程。

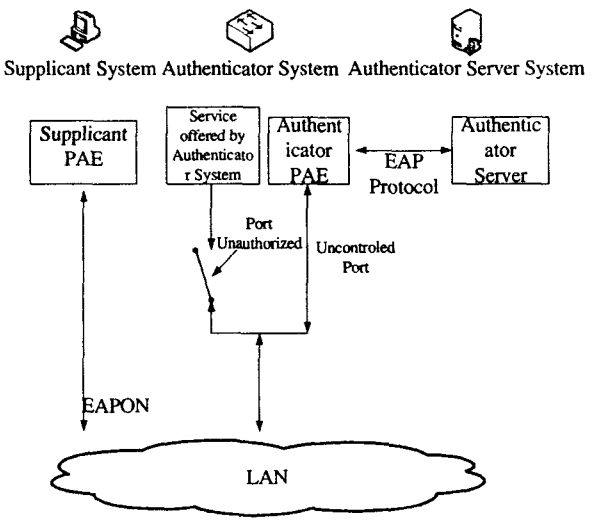

图 1　IEEE802.1x 的体系结构

在用户接入层设备 LanSwitch 实现 802.1x 的认证系统部分,即 Authenticator;IEEE802.1x 的客户端一般安装在用户 PC 中,典型的为 Windows XP 操作系统自带的客户端;而 IEEE802.1x 的认证服务器系统一般驻留在运营商的 AAA 中心。

Supplicant 与 Authenticator 间运行 IEEE IEEE802.1x 定义的 EAPOL 协议;Authenticator 与 Authentication Sever 间同样运行 EAP 协议,EAP 帧中封装了认证数据,将该协议承载在其他高层次协议中,如 Radius,以便穿越复杂的网络到达 AAA 服务器。

Authenticator 每个物理端口内部有受控端口(Controlled Port)和非受控端口(unControlled Port)等逻辑划分。非受控端口始终处于双向连通状态,主要用来传递 EAPOL 协议帧,可保证随时接收 Supplicant 发出的认证 EAPoL 报文。受控端口只有在认证通过的状态下才打开,用于传递网络资源和服务。

2.2　802.1x 认证协议过程

以下为 802.1x 技术的认证流程[4,5]:

(1)输入合法用户名和口令,客户端程序将发出请求认证的报文给交换机,开始启动一次认证过程。

(2)交换机收到请求认证的数据帧后,将发出一个请求帧要求 802.1x 客户端将输入的用户名传上来。

(3)802.1x 客户端程序响应交换机发出的请求,将用户名信息通过数据帧送给交换机。交换机将客户端送上来的数据帧经过封包处理后送给认证服务器进行处理。

(4)认证服务器收到交换机转发上来的用户名信息后,将该信息与数据库中的用户名表相比对,找到该用户名对应的口令信息,用随机生成的一个加密字对它进行加密处理,同时也将此加密字传送给交换机,由交换机传给客户端程序。

(5)客户端程序收到由交换机传来的加密字后,用该加密字对口令部分进行加密处理(此种加密算法通常是不可逆的),并通过交换机传给认证服务器。

(6)认证服务器将送上来的加密后的口令信息和其自己经过加密运算后的口令信息进行对比,如果相同,则认为该用户为合法用户,反馈认证通过的消息,并向交换机发出打开端口的指令,允许用户的业务流通过端口访问网络,并把认证通过的消息传递给数据库。否则,反馈认证失败的消息,并保持交换机端口的关闭状态,只允许认证信息数据通过而不允许业务数据通过,同时,传递认证失败信息到数据库。数据库收集到用户信息以后会和策略管理过程中设置的策略,一起反馈给 802.1x 网络设备。图 2 从发送数据包的角度展示了 802.1x 技术的认证流程。

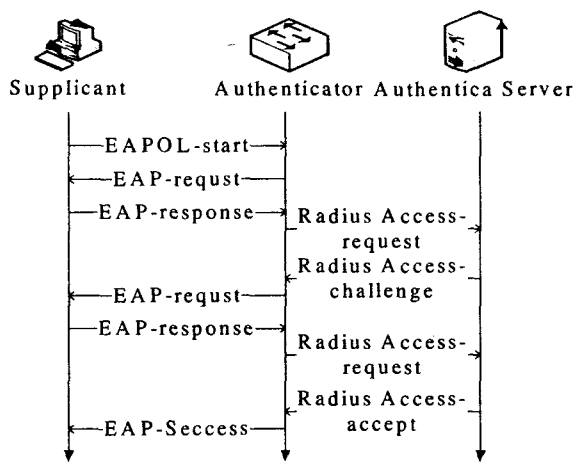

图 2　802.1x 的认证过程

3　结合 802.1x 实现网络安全管理总体解决方案

为了更好实现网络管理,增强网络的安全性、易管理性,本系统的设计思想是:外网和内网通过防火墙隔开,在接入层采用集成了标准的 802.1x 模块的网络设备,在用户端安装 802.1x 客户端,从网络中的 IDS,日

志系统等获取网络安全数据,通过核心层的 802.1x 服务端数据库对用户终端进行集中式的安全管理,最终达到对整个网络实现安全管理,其网络安全管理架构如图 3 所示。

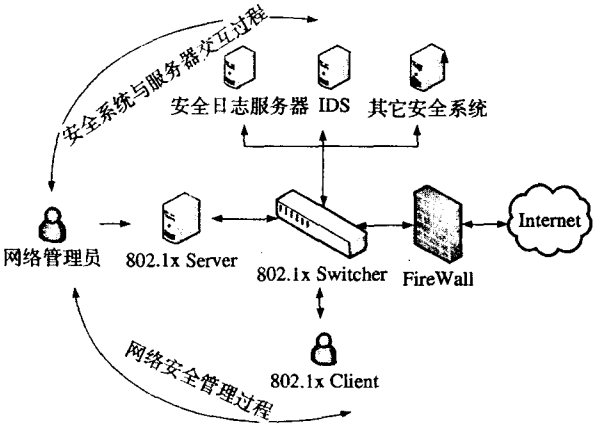

图 3 网络安全管理框架图

从上图可以看出整个网络安全管理中包含两个主要环节:外围安全系统与 802.1x 服务器数据库交互过程;基于 802.1x 技术的网络安全管理过程。

3.1 安全系统与 802.1x 服务器端数据库交互过程

网络中的各种安全问题需要网络安全设备监视并获取,这些网络安全设备包括防火墙,IDS,日志服务器等。通过监视网络运行,将网络中的运行数据存入特定数据库,通过数据挖掘技术提取出可能存在安全问题的数据,网络安全设备可通过 802.1x 服务器端数据库提供的接口向其传入各种数据,如:盗用与被盗用的 IP,MAC;对网络进行 APR 攻击的终端主机 IP,MAC;DoS 攻击源等。文中主要讨论 802.1x 技术在网络安全管理中的应用,对此过程不做过多讨论。

3.2 基于 802.1x 技术的网络安全管理过程

802.1x 服务器端数据库具备与其它网络安全设备(IDS,日志服务器,802.1X 交换机等)进行数据交互的能力。可以从这些外围安全设备得到的各种所需数据,基于 802.1x 技术的网络安全管理过程主要是通过得到这些数据来对网络进行安全管理,可以从以下几个方面来实现对不合法使用网络的终端用户进行管理[6]:

(1)用户假冒 ip/mac 对网络进行攻击。

如果出现终端假冒 ip/mac 攻击网络的行为,网络安全设备可以通过数据包分析得出攻击网络终端的真实 ip,并把此 ip 传给 802.1x 服务器数据库。802.1x 技术是基于接入设备端口的控制,可将此终端断绝在网络之外。

(2)ARP 攻击。

ARP 攻击是利用了 ARP 协议的不完善性对网络设备的一种攻击,严重的话可以造成网络设备处于不响应状态,同时合法网络用户不能接入网络。网络安全设备通过监视网络接入设备的 CPU 利用率,丢包率,分析数据包协议等可判断网络是否受到 ARP 攻击,通过分析数据包可以得到中了 ARP 病毒的终端真实 ip,同样 802.1x 技术可以利用关闭此终端的接入端口来实现清除 ARP 攻击。

(3)DoS 攻击。

DoS 攻击行为比较好识别,受攻击的网络或设备表现为响应时间增加,甚至是不可用,分析数据包可以得到被攻击的网络或设备在极短时间内要响应极多来自不同 ip 或相同 ip 的数据包。如果这些数据包是来自外网,可以通过设置防火墙来过滤掉那些数据包,如果这些数据包是来自内网,则可以通过数据包分析得到这些主机的真实 ip,同样可以利用 802.1x 技术将这些终端隔绝在网络外[7]。

(4)利用 802.1x 技术完善网络安全管理。

从以上 3 点中可以看到如果直接把网络中的不安全终端隔绝在网络外,无法保障用户的知情权,同时也降低了用户体验,这是一种不人性的处理安全问题的做法。而利用 802.1x 技术的 Server/Client 结构,可以通过 802.1x 客户端程序提供告知功能,如:用户中了木马病毒,用户在进行 ARP 攻击,用户的系统有漏洞等,而用户可通过这些警告信息进行相应操作,如:查杀病毒,下载补丁等。这些都是可以通过编写相应的 802.1x 客户端程序来做到的。文中提出一种网络安全管理的方案,在此不涉及具体代码的编写。

4 结束语

通过以上描述,给出了结合 802.1x 技术实现网络安全管理的解决方案。本方案具有两个可取之处:

(1)802.1x 技术是基于端口的访问控制,利用这点可以方便地做到对终端用户的接入管理。同时,利用 802.1x 技术的 Server/Client 结构可以方便地做到对终端用户的指导与控制,提高用户终端安全等级。

(2)本系统完成后可起到完善网络安全管理功能的作用,将网络安全管理与用户管理的操作整合在 802.1x 服务器上,同时可供用户及网管人员查询,增加用户使用网络的透明度,同时减少网管人员的工作量。

同时也应该看到,对于网络安全管理,此系统并不是很完善。比如:集中式的网络管理对核心设备的运作要求较高,802.1x 认证系统需要用户安装客户端程序,802.1x 技术本身还存在安全方面的隐患[8,9]等。

(下转第 176 页)

签名;

SigPack1 = Sign(HV1, CliPriKey)

④发送方用接收方的公钥加密对称密钥 KEY;

Ekey1 = Eec(key1, SerPubkey)

⑤发送方将交易数据密文、数字签名、加密密钥放置数字信封,发送给接收方;

Send(Dpack1, SigPack1, Ekey1)

●接收:(资金划转数据的验证)

①接收方使用公钥算法,用私钥解密对称密钥 key; Key1 = Dec(Ekey1, SerPubkey)

②接收方用发送方的公钥解密数字签名,得到发送的 Hash(V1); HV1 = DEC(SigPack1, CliPubKey)

③接收方用匹配的对称密钥 key1 解密交易数据密码,获得 V1; V1 = Dec(Dpack1, key1)

④接收方用发送方相同的散列函数生成交易数据的 Hash(V1); HV2 = Hash(V1)

⑤比较两个散列值是否相等,验证交易数据的真实性。

若 HV1 = HV2,表明数据传送真实有效,根据指令进行资金的划转。

3 结束语

针对目前网上证券交易系统安全性的不足,设计了基于 PKI 的网上证券交易系统。采用了安全认证服务器证书,实现了客户端和服务器的双向认证,确保了网上客户端和服务器端的真实性和唯一性,防止了伪造攻击。同时利用对称密码技术加密交易数据,临时产生对称密钥,不重复使用,有效防范强力攻击。然后使用公钥算法将对称密码密钥加密再传送的数字签名技术,保证了交易双方的不可抵赖性。数据在客户端和证券公司服务器端传送采用 SSL 安全协议,大大加强了数据的机密性,防止了对交易数据的截取和篡改攻击。在客户端采用客户端证书加 USB Key 的强身份认证方式,确保证券帐户的安全。因此,使用基于 PKI 体系的信息安全技术保证了证券交易数据的真实性、完整性、保密性、不可抵赖性和银行资金的安全。

参考文献:

[1] 关振胜. 公钥基础设施 PKI 及其应用[M]. 北京:电子工业出版社,2008.

[2] PSTN. 电子签名基础知识[EB/OL]. [2005 - 01 - 04]. http://tech. ccidnet. com/pub/artic le/c1096_a198449_p1. html.

[3] Jacob E, Liberal F, Unailla J. PKIX-based certification infrastructure implementation adapted to non - personal end entities [J]. Future Generation Computer Systems, 2003(19):263 - 275.

[4] 张书杰,潘兴庆,李 健. 基于 PKI/CA 的银行与基金公司在线交易系统的构建[J]. 北京工业大学学报,2006,32(5):477 - 480.

[5] 时贵霞,杨家明. 基于 PKI 技术的网上交易系统[J]. 东华大学学报:自然科学版,2006,32(6):83 - 85.

[6] 刘 渊,周世民,孙亚民. 网上在线支付的数字签名的研究与设计[J]. 计算机应用研究,2003(11):110 - 112

[7] 雷 蕴. 基于 SSL 协议的网上证券交易系统的安全方案[J]. 北京电子科技学院学报,2007,15(2):17 - 20.

[8] 吕格莉,王 东,戴 骥,等. 基于 PKI 的网上交易安全中间件的研究与实现[J]. 微型电脑应用,2005,21(12):52 - 54.

[9] 将 韬,伍 萍,徐正文. 一种基于 PKI/PMI 技术的安全的网上证券交易模型的研究与实现[J]. 信息安全与通讯保密,2007(10):44 - 46.

[10] 王淑清,齐景佳. 兴安证券网上交易安全方案[J]. 哈尔滨金融高等专科学校学报,2006(1):50 - 52.

(上接第 172 页)

参考文献:

[1] 石 静,王 平. 论校园网的安全和防护[EB/OL]. 2008 - 08. http://www. 60553878. com/Article/ShowArticle. asp?ArticleID=40.

[2] 杨富华,彭 钢,潘 宏. 关于 802.1x 认证技术在校园网应用中问题的探讨[J]. 中国医学教育技术,2006(6):260 - 263.

[3] 马育峰,胡修林,张蕴玉. 网络管理热点问题研究的现状、问题与展望[J]. 计算机应用研究,2005(10):10 - 13.

[4] 董贞良,吕述望,王昭顺. 内网安全管理系统认证模块的设计基于 802.1X 的内网安全管理系统认证模块设计[J]. 计算机工程,2007(6):193 - 198.

[5] 王 倩,薛德黔. 802.1x 接入认证技术分析及展望[J]. 福建电脑,2007(8):8 - 10.

[6] 秦 刘,智英建,贺 磊,等. 802.1x 协议研究及其安全性分析[J]. 计算机工程,2007(4):153 - 157.

[7] Carey N. The evolving virus threat[C]//23th NISSC Proceedings. Baltimore, MD, USA:[s. n.],2000:141 - 153.

[8] Mishra A, Arbaugh W A. An Initial Security Analysis of the IEEE 802.1x Standard[EB/OL]. 2002 - 02. www. ieee802. org/1/files/public/docs2000/ieee_plenary. PDF.

[9] Anthon J. Using IEEE 802.1x to Enhance Network Security [EB/OL]. 2002 - 10 - 28[2005 - 12 - 20]. http://whitepapers. zdnet. co. uk/0,39025945,60043454p - 39000378q,00. htm.