文章编号：1674－5566(2010)02－0271－06

校园网络安全与准入身份认证

胡光民，柯立新

(上海海洋大学现代信息与教育技术中心，上海 201306)

摘 要：随着信息化技术在高校的普遍应用，校园网络的安全显得尤为重要。而传统的校园网络一般都重出口轻内部接入，在网络出口处部署了许多网络安全设备，如：防火墙、入侵检测以及流量控制设备等，但在校园网内部的接入安全却没能很好重视。就目前校园网发生的安全事件，90%是来自学校内部，使得校园网局部瘫痪的情况时有发生，网络管理人员十分被动、疲于奔命。为使校园网络的安全化被动封堵为主动防范，大量减少校园内部的网络安全事件发生。从而使校园网络在安全、可控、可用和畅通的环境中运行，有必要在网络的接入层加强安全管理。准入身份认证技术在校园网络安全中起到了很重要的作用，而准入身份认证的WEB化更有助于在高校数字化建设中部署和推进。

关键词：身份认证；网络准入；802.1x；WEB安全插件

中图分类号：TP 393 **文献标识码**：A

Campus network security and access authentication

HU Guang-ming, KE Li-xin

(Modern Information and Education Technology Center, Shanghai Ocean University, Shanghai 201306, China)

Abstract: As information technology is widely used in colleges and universities, the security of network on campus is more and more important. However, in traditional campus network, people always focus more on the exit than the inner access. A number of network security devices are set up at the exit of the network, such as firewall, IDS, Flow Control devices, while the security of inner access is always being ignored. Almost 90 percent of campus network security affairs come from the campus. Partial paralysis of the network happens quite often, and the administration of networks becomes very passive. In order to change this situation to initiative guard to decrease the number of security affairs on campus, it is very necessary to strengthen the control of access. The technology of access authentication has a very significant effect on maintaining the safety of campus network, and also the technology of access authentication is very helpful to improve the digital construction in college.

Key words: authentication; network access; 802.1x; WEB security plug-in

随着计算机网络技术的快速发展以及因特网在人们的日常生活中日益普及，计算机网络已成为人们的一种工作和生活的平台，人们利用这一平台进行信息交流与信息共享，并通过计算机网络来完成各种工作。然而，计算机网络给我们带来生活和工作便利的同时，因其网络的开放性，使其容易受攻击等安全问题日显突出，诸如网络黑客、病毒泛滥、垃圾信息等利用网络进行

收稿日期：2009-10-09

基金项目：上海海洋大学新校区弱电建设项目(B－9400－08－004)

作者简介：胡光民(1957－)，男，工程师，主要从事计算机网络管理方面的研究。E-mail: gmhu@shou.edu.cn

非法活动直接或间接对人们的生活和工作带来了许多负面影响。如何确保校园网络的安全可靠、运行稳定是学校网络管理部门面临的首要课题。

1 校园网络安全与管理现状

由于互联网的开放性、自身的脆弱性、攻击的普遍性和管理的困难性等综合因素使得互联网的安全存在灾难性的隐患。而校园网的规模和用户群又有其独特性。

1.1 速度快和规模大

高校校园网是最早的宽带网络，普遍使用的以太网技术决定了校园网最初的带宽不低于 10 Mbps目前普遍使用了百兆到桌面、千兆甚至万兆实现园区主干互联。校园网的用户群体也比较大，少则数千人、多则数万人。高校学生一般集中住宿，因而用户群比较密集。正是由于高带宽和大用户量的特点，网络安全问题一般蔓延快、对网络的影响比较严重。

1.2 用户计算机种类繁多不便管理

比如学生的电脑一般是学生自己花钱购买、自己维护的，有的院系是统一采购、有技术人员负责维护的，有些院系则是教师自主购买、没有专人维护的。这种情况下要求所有的终端系统实施统一的安全策略 (比如安装防病毒软件、设置可靠的口令)是非常困难的。比较典型的现象是，用户的计算机接入校园网后感染病毒，反过来这台感染病毒的计算机又影响了校园网的运行，于是出现终端用户和网络管理员相互指责的现象。更有些计算机甚至服务器系统建设完毕之后疏于管理，甚至被攻击者攻破作为攻击的跳板、肉机，变成攻击试验床也无人觉察。

1.3 活跃的用户群体

高等学校的学生通常是最活跃的网络用户，对网络新技术充满好奇，勇于尝试。如果没有意识到后果的严重性，有些学生会尝试使用网上学到的、甚至自己研究的各种攻击技术，可能对网络造成一定的影响和破坏。

1.4 开放的网络环境

由于教学和科研的特点决定了校园网络环境应该是开放的、管理也是较为宽松的。比如，企业网可以限制允许 Web浏览和电子邮件的流量，甚至限制外部发起的连接不允许进入防火墙，但是在校园网环境下通常是行不通的，至少在校园网的主干不能实施过多的限制，否则一些新的应用、新的技术很难在校园网内部实施。

1.5 有限的投入

校园网的建设和管理通常都轻视了网络安全，特别是管理和维护人员方面的投入明显不足。在中国大多数的校园网中，通常只有网络中心的少数工作人员，他们只能维护网络的正常运行，无暇顾及、也没有条件管理和维护数万台计算机的安全。

1.6 盗版资源泛滥

由于缺乏版权意识，盗版软件、影视资源在校园网中普遍使用，这些软件的传播一方面占用了大量的网络带宽，另一方面也给网络安全带来了一定的隐患。比如，Microsoft公司对盗版的 XP操作系统的更新作了限制，盗版安装的计算机系统今后会留下大量的安全漏洞。另一方面，从网络上随意下载的软件中可能隐藏木马、后门等恶意代码，许多系统因此被攻击者侵入和利用。

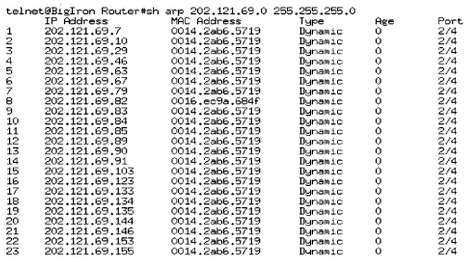
1.7 校园网拓扑结构重出口轻接入

传统的校园网络结构一般都比较重视出口的安全管理以及核心应用服务器的安全管理，轻视和疏于对接入终端的安全管理。而对于目前校园网络的攻击一般都是由校园用户终端发起的。这些攻击大量是终端用户无意的，比如计算机中了病毒，也有少量有意使用黑客工具对服务器进行攻击。常见的病毒如 ARP攻击和欺骗、DDos攻击。ARP攻击和欺骗将会使整个接入网段瘫痪，用户的 IP地址被发起 ARP攻击的主机所占用，使其他用户无法接入网络，如图 1所示；DDos攻击是用户终端成为肉机对特定网络或服务器发起攻击，使的某个网络的带宽堵塞或服务器的资源耗尽而拒绝服务，如图 2所示。

2 校园网准入身份认证

目前校园网采用的身份认证主要有 2种形式。一种是基于校园网出口处的网关型的 WEB身份认证，另一种是基于 802.1x的接入交换机端口的身份认证[1]。基于校园网出口处的网关型的 WEB身份认证只能对用户访问互联网做身份认证及审计，而对于其在校园网内部的行为不能

做控制和审计。基于 802.1x的接入交换机端口的身份认证能对接入用户的身份合法性认证和审计，但如果是单纯的 802.1x的接入交换机端口的身份认证对接入用户的合法性作了认证，但对接入的终端设备对网络的有意或无意的攻击却不能防范[2]。这里所论述的网络准入身份认证是从网络接入终端的安全控制入手，结合身份认证服务器，安全策略服务器和网络设备，以及第三方软件系统（杀毒软件和系统补丁服务器），完成对接入终端用户的强制认证和安全策略应用，从而达到保障整个网络安全的目的[3]。


telnet@BigIron Router#sh arp 202.121.69.0 255.255.255.0

	IP Address	MAC Address	Type	Age	Port
1	202.121.69.7	0014.2ab6.5719	Dynamic	0	2/4
2	202.121.69.10	0014.2ab6.5719	Dynamic	0	2/4
3	202.121.69.29	0014.2ab6.5719	Dynamic	0	2/4
4	202.121.69.46	0014.2ab6.5719	Dynamic	0	2/4
5	202.121.69.63	0014.2ab6.5719	Dynamic	0	2/4
6	202.121.69.67	0014.2ab6.5719	Dynamic	0	2/4
7	202.121.69.79	0014.2ab6.5719	Dynamic	0	2/4
8	202.121.69.82	0016.ec9a.684f	Dynamic	0	2/4
9	202.121.69.83	0014.2ab6.5719	Dynamic	0	2/4
10	202.121.69.84	0014.2ab6.5719	Dynamic	0	2/4
11	202.121.69.85	0014.2ab6.5719	Dynamic	0	2/4
12	202.121.69.89	0014.2ab6.5719	Dynamic	0	2/4
13	202.121.69.90	0014.2ab6.5719	Dynamic	0	2/4
14	202.121.69.91	0014.2ab6.5719	Dynamic	0	2/4
15	202.121.69.103	0014.2ab6.5719	Dynamic	0	2/4
16	202.121.69.123	0014.2ab6.5719	Dynamic	0	2/4
17	202.121.69.133	0014.2ab6.5719	Dynamic	0	2/4
18	202.121.69.134	0014.2ab6.5719	Dynamic	0	2/4
19	202.121.69.135	0014.2ab6.5719	Dynamic	0	2/4
20	202.121.69.144	0014.2ab6.5719	Dynamic	0	2/4
21	202.121.69.146	0014.2ab6.5719	Dynamic	0	2/4
22	202.121.69.153	0014.2ab6.5719	Dynamic	0	2/4
23	202.121.69.155	0014.2ab6.5719	Dynamic	0	2/4

图 1　ARP攻击截图

Fig 1　ARP Attack Screenshot

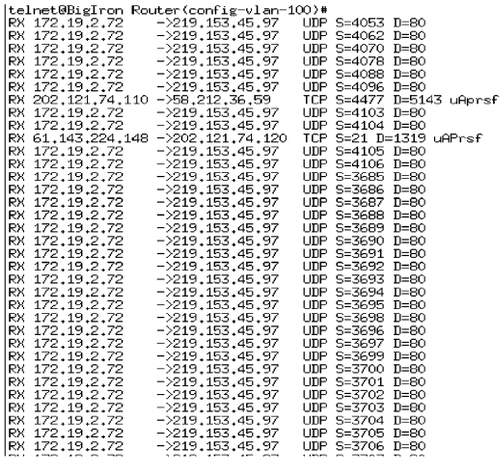

```
telnet@BigIron Router(config-vlan-100)#
RX 172.19.2.72     ->219.153.45.97    UDP S=4053 D=80
RX 172.19.2.72     ->219.153.45.97    UDP S=4062 D=80
RX 172.19.2.72     ->219.153.45.97    UDP S=4070 D=80
RX 172.19.2.72     ->219.153.45.97    UDP S=4078 D=80
RX 172.19.2.72     ->219.153.45.97    UDP S=4088 D=80
RX 172.19.2.72     ->219.153.45.97    UDP S=4096 D=80
RX 202.121.74.110 ->58.212.36.59     TCP S=4477 D=5143 uAprsf
RX 172.19.2.72     ->219.153.45.97    UDP S=4103 D=80
RX 172.19.2.72     ->219.153.45.97    UDP S=4104 D=80
RX 61.143.224.148 ->202.121.74.120   TCP S=21 D=1319 uAPrsf
RX 172.19.2.72     ->219.153.45.97    UDP S=4105 D=80
RX 172.19.2.72     ->219.153.45.97    UDP S=4106 D=80
RX 172.19.2.72     ->219.153.45.97    UDP S=3685 D=80
RX 172.19.2.72     ->219.153.45.97    UDP S=3686 D=80
RX 172.19.2.72     ->219.153.45.97    UDP S=3687 D=80
RX 172.19.2.72     ->219.153.45.97    UDP S=3688 D=80
RX 172.19.2.72     ->219.153.45.97    UDP S=3689 D=80
RX 172.19.2.72     ->219.153.45.97    UDP S=3690 D=80
RX 172.19.2.72     ->219.153.45.97    UDP S=3691 D=80
RX 172.19.2.72     ->219.153.45.97    UDP S=3692 D=80
RX 172.19.2.72     ->219.153.45.97    UDP S=3693 D=80
RX 172.19.2.72     ->219.153.45.97    UDP S=3694 D=80
RX 172.19.2.72     ->219.153.45.97    UDP S=3695 D=80
RX 172.19.2.72     ->219.153.45.97    UDP S=3698 D=80
RX 172.19.2.72     ->219.153.45.97    UDP S=3696 D=80
RX 172.19.2.72     ->219.153.45.97    UDP S=3697 D=80
RX 172.19.2.72     ->219.153.45.97    UDP S=3699 D=80
RX 172.19.2.72     ->219.153.45.97    UDP S=3700 D=80
RX 172.19.2.72     ->219.153.45.97    UDP S=3701 D=80
RX 172.19.2.72     ->219.153.45.97    UDP S=3702 D=80
RX 172.19.2.72     ->219.153.45.97    UDP S=3703 D=80
RX 172.19.2.72     ->219.153.45.97    UDP S=3704 D=80
RX 172.19.2.72     ->219.153.45.97    UDP S=3705 D=80
RX 172.19.2.72     ->219.153.45.97    UDP S=3706 D=80
```

图 2　DDos攻击截图

Fig 2　DDos Attack Screenshot

准入身份认证是一种主动式网络安全管理技术，用户终端在接入网络之前，必须先接受身份识别和安全状态评估，使得只有符合安全标准的终端才准许访问网络，有助于确保拒绝不符合策略的设备接入，将其放入隔离区加以修复，或者仅仅允许其访问有限的资源。

终端安全状态是指操作系统补丁、第三方软件版本、病毒库版本和是否感染病毒等反映终端防御能力的状态信息。另外，安全状态是动态的，这意味着终端系统会随着时间迁移，可能由安全状态转变为不安全状态。用户上网过程中，如果终端发生感染病毒等安全事件，准入控制系统可实时隔离该“危险”终端[4]。

通过网络准入身份认证后，将大为改善校园网络的运行环境，减少了接入终端有意或无意地对校园网络的各种攻击，比如 ARP欺骗和攻击[5]、DDos攻击[6]等等。

3　准入身份认证的实现

3.1　准入身份认证组成

准入身份认证由 6个部份组成：接入交换机；身份认证服务器；安全策略管理平台；入侵检测 IDS；用户认证客户端；第三方软件系统（杀毒软件和系统补丁服务器）

3.2　准入身份认证工作原理

用户使用网络前，首先由接入交换机和身份认证服务器对其进行身份认证。

身份认证服务器检查用户身份，批准或拒绝用户的接入请求。

安全管理平台学习用户的身份、主机环境等信息，并将制定好的策略下发到用户认证客户端。

用户认证客户端对用户主机进行检查，并将检查结果反馈回安全管理平台服务器。

IDS对网络安全事件进行检测收集，将安全事件反馈回安全管理平台。

安全管理平台对 IDS反馈的安全事件进行统一管理，将安全事件关联至用户。

安全管理平台对每个用户的检测结果和安全事件进行处理，生成相应的策略，并将 IP地址与用户机的 MAC地址作动态绑定，然后下发至交换机执行。

通过以上准入身份认证系统的管理和控制，接入端对网络的安全危害大为减少。

4　准入身份认证的前后对比

在没有准入身份认证部署前，网络中的 ARP病毒几乎天天发生，如图 1所示。网络管理人员为查找攻击源主机疲于奔命，由于不能主动地去安全防御，只能被动地去查找攻击源，校园网中

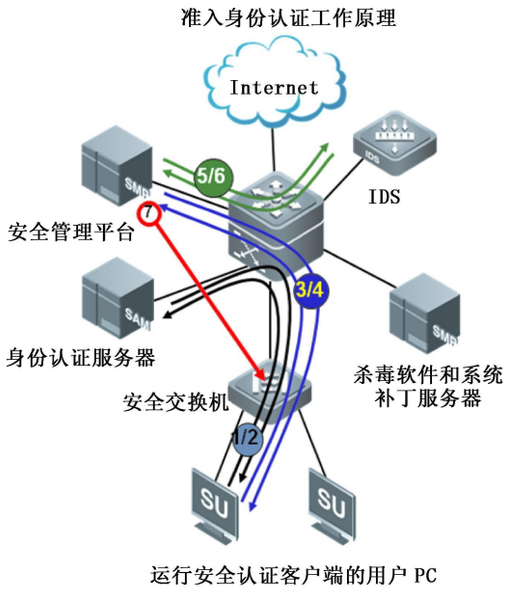


图 3 准入身份认证原理图

Fig 3 Schematic diagram of access authentication

部分网段网络瘫痪频繁发生就不足为奇了。

在部署准入身份认证系统后，网络的安全隐患大为改观，用户的计算机在上网时主机系统都进行了检查，确认没有安全隐患后才准接入网络。在发现客户计算机有危险隐患时就及时提示用户，并将其放入隔离区加以修复，对特别严重的攻击就提示后直接阻断。并且准入身份认证系统具有审计功能，其日志对有意的黑客攻击的定位提供了可能。由于部署了主动式安全防范机制—准入身份认证系统，大大提高了校园网的安全机制，也大大减少了网络管理人员疲于奔命的状况。

5 WEB准入身份认证

前述的准入身份认证系统的部署对整个校园网的安全起到了非常大的作用，然而对用户来说却增加了不少麻烦，因为每个用户上网必须安装定制的安全客户端程序，这对于初次使用校园网的新生来说怎样获取安全客户端程序就成了问题了，另外对于临时来学校开会的外来人员的上网也成了问题。我们先前提到的 WEB网关型出口身份认证，因其不能对接入实现身份认证，然而它却能很方便的实现出口身份认证。如果将准入身份认证实现 WEB化，用户就可直接使用浏览器进行准入身份认证，这就大大方便了用户，通过 WEB准入身份认证，实现动态自动的 IP＋MAC＋端口绑定、防 ARP欺骗、防 DHCP欺骗、访问控制（ACL），对于校内师生还可做 WEB控制插件下发，以实现对客户计算机安全的检查。具有 WEB准入身份认证就实现了可控性和安全性、易用性和兼容性、高性能和高可用、智能性和融合性的完美结合。

身份认证是网络准入的基础、网络准入是真实地址的基础、真实地址是安全可信的基础。只有接入层的安全得到了保障，整个校园网的安全才能得以实现，网络安全需要准入身份认证，方便用户使用需要 WEB准入身份认证。

参考文献：

[1] 谭丽莎，刘威. 浅谈 802.1x认证技术在校园网中的应用[J]. 网络与信息，2008，10：31－31.

[2] 段海新. 802.1x技术和准入控制技术[J]. 中国教育网络，2008，(2)：12－13.

[3] 魏克，段海新. 身份认证管理与准入控制[J]. 中国教育网络，2005，(9)：13－15.

[4] 李兴国，雷若寒. 利用准入控制实现校园网的安全管理[J]. 微计算机信息，2008，24：47－48.

[5] 何云强，符兴华. 高校机房病毒及 ARP欺骗的应对策略[J]. 信息系统工程，2009，6：94－97.

[6] 曾文权，向友君，尚敏. DDos攻击原理及防御方法分析[J]. 计算机技术与发展，2009，19(7)：156－158.