计算机网络终端准入控制技术①

周 超，周 城，丁晨路

(重庆通信学院 研究生管理大队，重庆 400035)

摘 要: 终端准入控制根据预定安全策略，对接入网络的终端进行身份认证和安全性检查，确保可信、安全的终端访问网络，拒绝或限制不安全终端的接入，体现了终端安全与准入控制的结合，可以有效提高网络对安全威胁的主动防御能力。现行部署的解决方案在身份认证、安全状态检查中存在缺陷，容易受到中间人攻击、会话劫持攻击等，并且对虚拟化应用适应性不足。可考虑通过完善认证过程、改善交互机制等方法加以改进。

关键词: 主动防御；终端安全；准入控制；网络安全；端点准入防御；802.1x 协议

Technology of Endpoint Admission Control in Computer Networks

ZHOU Chao, ZHOU Cheng, DING Chen-Lu

(Graduate School of Chongqing Communication Institute, Chongqing 400035, China)

Abstract: Endpoint Admission Control technology takes authentication and security state checking on endpoints accessing to network on the basis of pre-determinate security policies. It makes sure that only the trustworthy and secure endpoints could access to networks while rejects or limits the accessing of insecure endpoints. It’s exemplification of the combination of Endpoint Security and Access Control, which can efficiently improve the active defense ability against security threaten of networks. However, the existing solution has shortages in authentication and security state checking that it could easily attacked by Man-in-the-Middle Attack and Session Hijack. What’s more, it also has limitation in Virtualization appliance as well. It’s considerable to consummate the mechanism of authentication and communication processes for improvement.

Keywords: active defense; endpoint security; admission control; network security; endpoint admission defense; 802.1x protocol

1 引言

当前，政府、学校及企业等构建了大量内部计算机网络，以支持自身的信息化建设。由于主要业务都运行在内部网络，一旦其受到破坏，将产生严重的后果。针对各种网络安全威胁，人们开发应用了防火墙、IDS、IPS、VPN、杀毒软件等软硬件技术。虽然耗资巨大，但各种安全威胁仍然未得到有效解决。终端作为网络的关键组成和服务对象，其安全性受到极大关注。终端准入控制技术是网络安全一个重要的研究方向，它通过身份认证和完整性检查，依据预先设定的安全策略，通过软硬件结合的方式控制终端的访问权限，能有效限制不可信、非安全终端对网络的访问，从而达到保护网络及终端安全的目的。终端准入控制技术的研究与应用对于提高网络安全性，保障机构正常运转具有重要作用；对于机构解决信息化建设中存在的安全问题具有重要意义。目前，终端准入控制技术已经得到较大的发展和应用，在安全领域起到越来越重要的作用。本文依据某校园网部署的终端准入控制系统，对其理论原理、运行机制等进行研究，分析存在的不足，提出解决方法。

2 发展现状

为了解决网络安全问题，安全专家相继提出了新的理念。上世纪 90 年代以来，国内外提出了主动防

① 收稿时间:2010-04-29;收到修改稿时间:2010-05-30

御、可信计算等概念，认为安全应该回归终端，以终端安全为核心来解决信息系统的安全问题[1]。同时，很多安全厂家相继提出了新的安全构想，如思科的自防御网络(Self-Defending Network，SDN)和华为 3COM 的安全渗透网络(Safe Pervasive Network，SPN)等，这些蓝图是上述理念的具体体现，而在 SDN、SPN 等新型安全构想中不约而同地将准入控制技术作为重要的组成部件或解决方案。

2.1 当前研究概况

终端准入控制是目前一种新型的安全防御技术，它通过对终端实施安全防护，可以有效地解决因不安全终端接入网络而引起的安全威胁，将病毒、蠕虫等各类攻击拒绝于网络之外，从而真正保障网络的安全。

目前，对终端准入控制还没有一个权威、统一的定义，甚至其本身也有各种叫法，如网络接入控制(Network Access Control，NAC)，网络准入控制(Network Admission Control)，终端安全接入，安全接入控制等等。普遍认为，网络接入控制是一套可用于定义在节点访问网络之前如何保障网络及节点安全的协议集合[2]。由于该技术的核心概念是从网络终端的安全控制入手，通过消除终端的不安全因素或将其减少到最小，从而保护网络和终端的安全，故本文中采取“终端准入控制”的称谓。

终端准入控制的主要思路是：终端接入网络之前应根据预定安全策略对其进行检查，只允许符合安全策略的终端接入网络，而将不安全的终端隔离于网络之外，自动拒绝不安全的主机接入受保护网络，直到这些主机符合网络内的安全策略为止[3]。

2.2 主要技术产品

目前，国内外有代表性的终端准入控制技术有以下几种：

思科的网络准入控制(Network Admission Control，NAC)，微软的网络接入保护(Network Access Protection，NAP)，Juniper 的统一接入控制(Uniform Access Control，UAC)，可信计算组织 TCG 的可信网络连接(Trusted Network Connect，TNC)，H3C 的端点准入防御(Endpoint Admission Defense，EAD)等。

其它如趋势科技、赛门铁克、Sophos、北信源、锐捷、启明星辰等等大大小小国内外厂商也不约而同地基于自身特色提出了准入控制的解决方案。这也从一个方面反映出终端准入控制技术的重要性以及广阔的发展前景。

3 终端准入控制的基本原理

终端准入控制体现了病毒防治、补丁修复、系统维护等终端安全防护措施与接入控制、身份认证、权限控制等网络准入控制手段的结合，体现了主动防御、整体安全的理念。

3.1 终端准入控制相关理念

3.1.1 终端安全

统计结果表明，针对内网的攻击大部分是由于用户对终端使用不规范、系统安全级别不高造成的。但是很多网络的安全管理依旧将主要精力放在边界防护，大部分内网目前都还是采用边界防护模式，把安全重点放在内外网边界上。然而随着网络接入手段越来越多样，网络的边界在动态快速变化，边界防护模式存在不足，我们需要新的安全解决方法，确保我们的内网安全。在文献[1]中，作者系统地阐述了终端安全是影响信息系统安全的根源这个学术观点，同时提出以工程控制模型构建网络安全的方法，有很好的借鉴意义。

3.1.2 网络准入控制

到目前为止，有大量不同的网络准入控制方式，各自的功能和控制点不同，大致可从保护对象和开发模式划分。

按保护对象，可分为网络可信接入控制和终端可信接入控制。前者将网络视为可信主体，接入终端为不可信主体，强调终端接入网络后网络系统的安全性。主要思路是从终端着手，通过管理员制定的安全策略，对接入网络的终端进行安全性检测，自动拒绝不安全的终端接入受保护网络，直到这些终端符合网络内的安全策略为止；后者将终端视为可信主体，网络为不可信主体，强调对终端的保护，防止终端接入到不安全的网络中，其典型技术是违规外联技术。

按开发模式，可将网络接入控制分为内嵌型(in-band)、带外型(out-of-band)、基于交换机型(switch-based)、基于主机型(host-based)。

随后讨论的 EAD 系统(包括 NAC、UAC)属于网络可信型、带外型准入控制。这种方式的特点是基于代理和无代理的控制，代理模式下保证全面强制执行安全策略，而无代理模式下保证终端接收安全漏洞扫描或者策略评估扫描，根据扫描结果决定准入措施。

同时，带外型接入控制由接入设备利用 802.1x、SNMP、DHCP 和 ARP 等协议强制执行策略，对网络性能影响很小，不需要额外的设备，但其控制效果依赖于上述协议的发现和执行机制[2,4]。

3.2 终端准入控制运行机制

终端准入控制是一种主动式网络安全管理技术，体现了主动防御的理念，能有效增强网络的安全性。终端在接入网络之前，必须先接受身份认证和完整性度量，只有可信并且符合安全策略的终端才获准访问网络，拒绝不符合安全策略的设备接入，或将其放入隔离区加以修复，或仅允许其访问限定资源[3]。

终端准入控制系统的运行围绕着终端安全状态检测展开，其周期可用下图描述(见图 1)。

图 1 “检测-决策-执行”周期

检测包含准入前检测(Pre-Admission Assessment)和准入后检测(Post-Admission Assessment)，准入前检测在终端获得网络访问权限之前进行，准入后检测与其相反。准入后检测可以周期性地检测终端安全状态，保证其不会在网络访问过程中引入安全威胁。终端一旦连接到网络就要接受检测，系统之后依据检测结果和管理者制定的策略做出准入决策，最后执行该决策，整个过程周期性地循环。另外，当终端的安全状态发生改变时，将激发这个过程[4]。

3.3 终端准入控制系统框架

终端准入控制的核心概念是从网络终端的安全控制入手，结合身份认证，安全策略执行和网络设备联动，以及第三方软件系统(信息服务系统、杀毒软件和系统补丁服务器等)的应用，完成对终端的强制认证和安全策略实施，从而达到保障整个网络安全的目的。当前应用方案的框架基本相似，都由 3 个逻辑部件构成，分别为(参考 TNC 的术语)：接入请求部件(Access Requestor，AR)、策略实施部件(Policy Enforcement Point)以及策略决定部件(Policy Decision Point)。在实际应用中，往往还包含提供特定应用支持的第三方服务部件，例如第三方的防病毒软件或防病毒服务器(见图 2)。

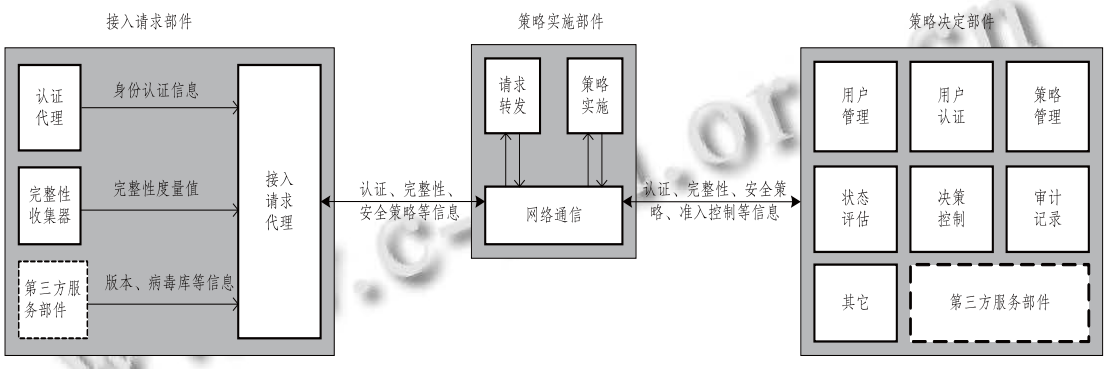

图 2 终端准入控制系统的逻辑结构

3.3.1 接入请求部件

该部件是请求访问受保护网络的实体，主要负责协商和建立网络连接、为终端或用户提供认证代理以及收集来自终端的完整性度量值，并将该值传递给网络。AR 在实际系统中往往体现为一个包含多个安全组件的客户端软件集，可以从终端收集身份认证信息(如用户名、口令、证书、智能卡信息等)和安全状态信息(防毒软件及病毒库版本、操作系统更新版本、补丁安装情况、软件列表等)，然后将这些信息传送到相连的网络，在此实现准入控制。

3.3.2 策略实施部件

PEP 是网络中的策略实施点，控制终端的访问权

限。这些设备接受终端接入请求信息，然后将信息传送到策略决定部件接受检查，由其决定采取什么样的措施。按照策略决定部件的准入控制决策，允许、拒绝、隔离或限制终端的网络访问请求。实际系统中可以是路由器、交换机、防火墙以及无线 AP 等，这些设备一般都支持 802.1x、RADIUS、DHCP 和 IPSec 等协议。负责将客户端传来的认证信息、终端安全状态信息传递给策略服务器，供其做出访问控制决策，之后从策略服务器获得访问控制决策，并执行之。

3.3.3 策略决定部件

PDP 是整个系统管理和控制的核心，作为一个软件的集合实现用户管理、用户认证、安全策略管理、安全状态评估、安全决策控制以及安全事件审计记录等功能。主要是 AAA(Authentication、Authorization、Accounting，验证、授权、记账)服务器，支持 RADIUS 协议。根据客户端认证信息、安全状态信息，决定是否允许计算机进入网络，并根据预先设定的策略，向 PEP 设备发出访问控制决策。这一过程需要依赖客户制定的访问策略。实际系统还必须提供管理服务组件，实现管理操作界面、监控工具、审计报告生成等管理服务。

3.3.4 第三方服务部件

第三方的 AV-防病毒软件、防病毒服务器和补丁服务器等，前者可与接入请求部件等捆绑处于同一软件集中也可单独部署，后两者处于隔离区中，用于终端进行自我修复或补丁升级。

4 当前系统及其不足与改进

某校当前部署的 EAD 系统是一项网络端点接入控制方案，它通过对网络接入终端的检查、隔离、修复、管理和监控，加强了终端安全，使网络变被动防御为主动防御。

4.1 EAD 系统简介

EAD 系统基本功能通过安全客户端、安全联动设备(交换机、路由器、SecPath IAG 智能业务网关)、安全策略服务器以及防病毒服务器、补丁服务器的联动实现，其系统运行过程如下图表示(见图 3)[5]。

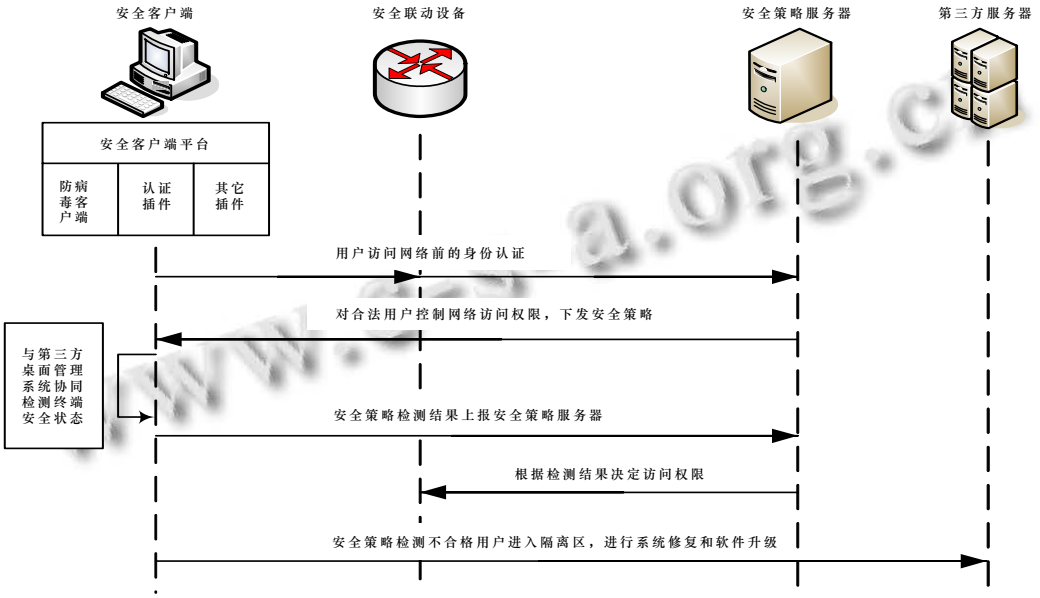

图 3 EAD 系统运行过程

4.2 当前系统的不足

当前系统在有力保障校园网安全有效运行的同时，存在一些不足之处。

4.2.1 认证过程存在安全隐患

系统中认证过程存在一定隐患，例如在系统中采用用户名加口令登录，而且信息传输安全性不高。虽

然也能应用 EAP-TLS，实现客户端与服务器强相互身份认证，但仍然能被绕过而受到中间人攻击、会话劫持攻击[6]。因此要想进一步增强端点准入防御机制的安全功能，势必要加强客户端与服务器端之间信息传输的安全性。

4.2.2 安全客户端及相关软件检查存在缺陷

目前，系统对安全客户端软件进行检测的过程比较简单，非法的兼容客户端软件通过接收版本检查请求帧，然后将合法安全客户端发出的应答帧信息封装到版本检查应答帧中发送给联动设备，能规避系统检查，躲避版本检测。现有系统无法抵御这种典型的重放攻击。同时，系统对指定软件的检查还只能简单的针对软件名称进行，安全性不够高。

4.2.3 多网卡及其使用状态识别不够准确

当前便携式计算机多存在多网卡，但是系统对多网卡识别不够细化，不能检测真实网卡的实际状态。一旦在安全策略中设置禁止使用多网卡将影响合法使用多网卡的用户。

4.2.4 无法支持虚拟化应用

虚拟化技术对终端准入控制提出了严峻的考验。准入控制能防止违反策略的终端接入网络，而对虚拟化终端就很难做到这一点。然而使用虚拟化软件构建虚拟网络以支持教学、科研的情况比较普遍，但是当前系统无法区分虚拟网卡与真实网卡，如果禁止使用了虚拟机(虚拟网卡)的终端使用网络，将影响正常用户的工作。

4.2.5 建网成本较高

构建 EAD 系统需要配备 H3C 支持 802.1x 协议的交换机，因而已有的交换设备无法充分利用，建网成本较高。同时，由于 802.1x 协议的灵活性[7]，很多厂家根据自身需要添加私有规范，开发自己的软硬件设备，导致改动标准协议现象比较普遍。各个厂家的交换机，都有对协议扩展属性的阅读和判断能力，如果交换机无法识别，很可能就丢弃报文或者修改属性，因此不同的产品无法交互。这也是当前各种网络准入控制解决方案的共同问题。

4.3 针对不足的改进

针对上述不足，目前已有研究人员提出了相应的改进方案以及测试，但是仍然存在大量工作需要完成。

4.3.1 改善认证过程消除安全隐患

目前已经使用的解决方案是四步握手认证方案，其基本思想是要求认证者(PEP)基于 RADIUS 为申请者(AR)生成会话密钥，与请求者完成双向认证。文献[8]中作者提出了一种改进方案以加强源真实性和完整性保护。

4.3.2 改善设备交互机制弥补安全状态检查缺陷

文献[9]提出了一种基于 Challenge 认证的客户端软件检测方法，能够避免通过兼容客户端软件接入网络。其思想为：认证过程中，利用客户端和认证者共享的对称密钥 S 将随机数 X 加密后发送给客户端，客户端将 X 与版本信息 T 合并产生应答消息，对该消息计算 Hash 值回传，认证者通过同样方式计算并对比 Hash 值，以检测客户端版本是否合法[9]。但是，在客户端如何保存对称密钥 S 和版本信息 T，以及双方怎样同步更新密钥是值得讨论的问题。另外，版本信息 T 是公开的，如何防范选择明文攻击也是一个问题。

针对其他安全软件的检查可以考虑结合注册表信息、软件数字证书等进行。

4.3.3 改进安全客户端，识别硬件使用状态

针对多网卡终端，可以通过改进安全客户端识别不同网卡的状态以及使用情况，以更好地支持合法用户使用网络。

4.3.4 针对虚拟化应用，进行产品优化

当前的解决方案缺乏与虚拟机的兼容性，没有配置虚拟交换机的能力，无法将终端准入控制配置到虚拟环境中。当虚拟机在虚拟网络中广泛应用的时候，难以控制其与虚拟交换机的连接。因为物理安全系统无法看到虚拟 LAN 中流量的运行情况，而随着虚拟机在物理平台上运行，必然带来安全上的隐患。因而解决虚拟化中的安全问题也是当前学界和产业界的热点。国外已有 Reflex Security 和 Altor Networks 等公司提出了虚拟化安全解决方案。

4.3.5 制定行业标准，统一数据格式

制定行业标准，使不同设备实现兼容与互操作，将减少部署终端准入控制系统的投入，无疑将促进该技术的发展进步。而当前系统可考虑通过加强客户端软件及安全策略服务器，使用支持标准协议的设备等措施实现对非本厂家产品的兼容。

5 结论

终端准入控制技术以终端安全为根本，以准入控制为手段，综合运用各种网络安全技术及设备，提升了网络对于安全威胁的主动防御、整体防御、综合防御能力。然而拥有一整套的终端准入控制方案并不意味着实现了网络安全，更重要的是网络安全管理人员科学合理的安全策略和实施，以及用户的积极主动配合。可以想象，在内部网络中如果存在针对 IE 的极光病毒 Auroras，而管理员并未在安全策略中配置对微软相应补丁程序的检测规则，那么再好的准入控制也不能阻止受感染终端对内网的危害。因此，正如 Kadrich 在《终端安全》一书中不断强调的：网络安全是一个过程控制问题。

参考文献

1 Mark. Kadrich S.终端安全.北京:电子工业出版社, 2009.06.
2 李梅梅,孙德刚,朱大立. 网络接入控制技术的安全性分析. 第十八届全国信息保密学术会议(IS2008)论文集,三亚 2008:83－94.
3 戴飞军,凤琦,姚立宁,王震宇. 新型终端安全接入技术对比分析.信息工程大学学报, 2008,9(3):344－347.
4 Mike Fratto. Tutorial: Network Access Control(NAC) -GAINING CONTROL. [2010-3-25]. http://www.network computing.com/channels/security/. July 2007.
5 杭州华三通信技术有限公司(H3C Technologies Co, Limited). EAD 技术白皮书. [2010-1-12].http://www.h3c.com.cn/Service/Document_Center/. 2008.
6 周辉,谢冬青.一种对 WLAN 的 IEEE 802.1x 认证实施中间人攻击的改进方案.科学技术与工程,2006,6(20):3365－3368.
7 IEEE Std 802.1X 2004, IEEE Standard for Local and metropolitan area networks-Port-Based Network Access Control. LAN/MAN Standards Committee of the IEEE Computer Society, 2004.
8 周贤伟,刘宁,覃伯平.IEEE 802.1x 协议的认证机制及其改进.计算机应用, 2006,26(12):2894－2896.
9 肖噱,王磊,李闻天,张国营.802.1x 系统中客户端软件版本检测方法分析.昆明理工大学学报,2007,32(2):43－47.