网络端点接入控制的实现

周益军,黄本雄
(华中科技大学 电子与信息工程系,湖北 武汉 430074)

摘 要:互联网用户数目在迅速增长,对各种接入方式的需求在飞快扩大,对用户的操作水平的挑战也已经大大提高,如何让用户更方便、更安全的接入到网络中去已经是一个亟待研究解决的问题。网络端点接入控制通过对要求接入的网络端点进行自动地检测与修补,保证了每个接入端点的安全级别,进而使整个网络保持在较高的安全水平,方便了网络用户管理终端。文中提出了一种网络端点接入控制的实现方法,其较高效地解决了以上的问题,并在市场上也有了相应的产品。

关键词:网络端点;网络端点接入控制;主机完整性;自动处所切换
中图分类号:TP393.08 **文献标识码**:A **文章编号**:1673-629X(2006)09-0227-03

Approach to Network Access Control

ZHOU Yi-jun, HUANG Ben-xiong
(Electronics and Information Department, Huazhong University of Science & Technology, Wuhan 430074, China)

Abstract: As the network user number is increasing sharply, the demand to access to the internet is greater and greater, and the challenge to the network user is much bigger than before, how to make user access the network more safely and more conveniently is a problem needs urgent research and solving now. NAC (network access control) automatically checks the integrity of endpoint and remedies the deficiencies to make sure every endpoint is at a high safety level. As a result, the whole network is safer and the endpoint is easy to administer. Below, an approach to NAC is given, which resolves the issue above and has been applied to products already.

Key words: network endpoint; network access control; host integrity; auto-location

0 引 言

随着互联网的蓬勃发展,资源共享的概念已经深入人心。个人电脑要入网,手机要入网,打印机要入网,PDA,ATM等等各种各样的网络端点都越来越迫切地要求成为网络的一分子。CNNIC在2005年1月19日发布的互联网统计报告中声称中国上网用户总数为9400万,比去年同期增长8.0%,其中使用宽带上网的人数达到4280万;上网计算机达到4160万台,增长了14.6%[1]。互联网渐渐成为人们生活中必不可少的一部分。然而,伴随着网络带来的资源共享和效率提高等优点,网络安全问题却逐渐变成端点用户信息财产严重的威胁。CNCERT/CC在2005年上半年网络安全工作报告中显示2005年上半年,蠕虫、木马、间谍软件等恶意代码在网上的传播和活动仍然频繁。据统计,从2005年1月1日到2005年6月30日,全球共新增蠕虫、木马、病毒等恶意代码11851种,系去年同期增长数量的1.2倍。2005年上半年其新截获的病毒数量达到了13464个,比去年同期增加了一倍多[2]。鉴于这种严峻的形势和安全方面巨大的需求,各种网络安全解决方案层出不穷。

收稿日期:2005-11-09
作者简介:周益军(1980-),男,江苏无锡人,硕士研究生,研究方向为网络安全;黄本雄,教授,博士生导师,研究方向为网络安全、下一代网络等。

1 相关概念

1)网络端点:可以接入网络的,有能力接受、发送和处理某些网络信息的实体。比如,个人电脑、打印机等。

2)网络端点接入控制:其实质是在网络端点接入网络时,做一系列检测、控制动作,确保接入端点的安全水平级别。网络接入控制,即NAC(Network Access Control),是由思科公司倡导的业界合作计划,最早于2003年11月提出。其主旨是向授权合作伙伴公开技术信息,以便合作伙伴开发和销售支持NAC网络基础设施的第三方服务器及客户端应用。目前,包括赛门铁壳、IBM、趋势、McAfee、CA、瑞星和金山等15家安全领域主要厂商,都已成为NAC合作伙伴[3,4]。

3)主机完整性:主机在安全方面的一系列要求,比如,是否安装Windows需要的补丁;是否安装某些被管理员认可的防病毒、反间谍软件,病毒库、特征库是不是最新的等等。它可由网络管理员定义。

4)处所:虽然是个表示地点的名词(比如,公司、家里、网吧等等),但表示网络端点接入时候的环境,比如无线接入、拨号接入、有没有边界防火墙等等。原因是在某一处所,接入方式一般比较固定,所以用地点来指代接入环境。比如在公司一般都有边界防火墙的、分到的是内部地址;

在家里一般分配到的是公共网络地址。每个“处所”对应一套安全策略。

5)自动处所切换:根据端点接入网络的环境,可以自动识别“处所”,并应用与“处所”对应的安全策略。

2 不安全因素

分析一下整个网络上面的各个环节。从人开始,到端点设备,到局域网,到广域网,到千千万万个其他网络节点,到不计其数的其他用户。这个中间,人们关注的是第二环节,与人接触进而与网络相连的这个端点设备,一方面它要与人,也即操作者、管理者接触;另一方面,它和网络是相连的。攻击来自于网络,而不安全因素却跟自身也密切相关。这个就是网络端点安全[5]。

威胁的引入可以分为机-机、人-机两种方式[6]。机-机威胁可以定义成,由另一个网络端点通过网络对本机造成的威胁。它是带攻击性质的,类似一支攻城大军,有绞尽脑汁要攻取城堡的主攻将领(黑客);有威力巨大的攻城工具(黑客工具);有彪悍勇猛的士兵(强悍的主机等硬件资源),甚至还有盟军(别的黑客)。如今的黑客人数越来越多,技术越来越先进,黑客工具也是越来越精妙,再加上黑客随处随时都可以接入到网络中去,可以说这种外部的威胁是日趋严重。

与之相对的人-机威胁定义为,操作网络端点的管理员由于自身的原因导致的威胁。它是带防守性质的,类似守城将领的防范意识、防守策略等等。现在网络用户急速增长,他们的计算机、网络的知识水平也是参差不齐,并且有数据显示其整体水平是不高的。CNNIC 在 2005 年 1 月 19 日发布的互联网统计报告中显示高中(中专)学历以下的网民占到了 42.3%[1]。这些人中大多数人都是没有接受过专门的网络安全培训的,在学历较高的网民中,也有不少缺乏网络安全知识的网民。就个人电脑一项的用户的统计数据就可以看出端点用户的安全意识是不够强的。要这些用户自己去解决网络的安全问题,有些勉为其难。文中称用户自身带来的问题为“人”的问题。

另外还有各类边界型的个人型的防火墙、反病毒软件、反间谍软件、入侵检测保护系统和系统安全补丁等安全软件,其他做安装、分发策略和管理等任务的控制软件,就类似于可以使用的城墙、望塔、箭楼等守城工事。

那么在这个防御过程中,各种可用软件就形成了“木桶理论”中“木桶”的板。如何避免某块木板偏短,如何减小板间缝隙,这些十分麻烦、异常复杂的,本来需要用户自己去解决的问题就是端点接入控制要解决的问题。

3 方 案

端点控制就是在端点要求接入的时候,对其某些设备或者参数作检测,然后做出一种反应动作(拒绝接入,允许接入但是需要用某套中央控制器提供的安全规则,或者让其接入到一个受限的网络,在这个受限网络中,可以拿到一些做补救措施必需的资源)。在接入的时候,检测端点的接入方式、网络地址、主机完整性等等。之后就形成一个信息集合,针对这一信息集合,再根据某种已经存在的规则进行匹配,进而得出一个结论,这个结论告诉了控制执行者正确的执行动作。可以安装一个客户端在每个被管理的端点,来搜集这些信息,然后把信息送给中央控制器,让它做出判断,最后把结果送给一个准入控制器,让这个控制器去执行允许或者阻止这个端点接入的动作(见图 1)。

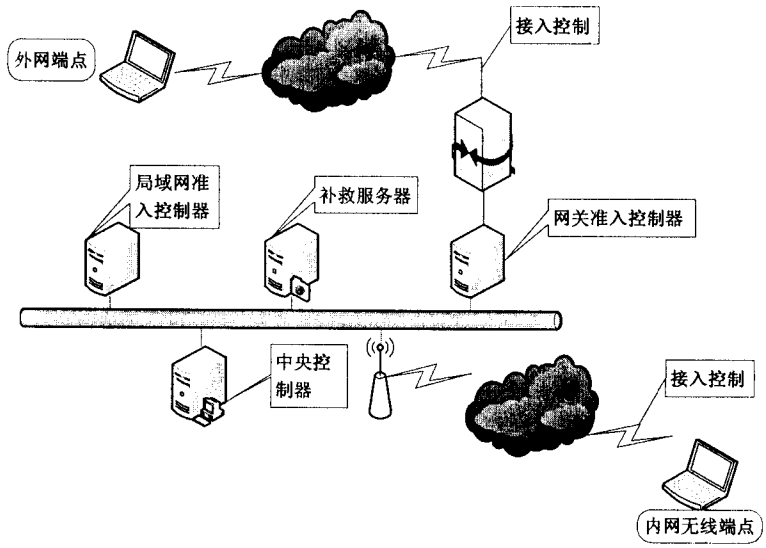

图 1 接入控制系统框图

如果被检测的端点不是非法的,但是由于主机完整性没有通过而不能接入到预期的网络,这个时候需要给机会让该客户端做一些补救措施。

接入的同时还可以对接入“处所”作判断,然后选择一套合适的安全策略来让客户端应用实施。

4 实 现

4.1 接入控制系统

接入控制系统由客户端、中央控制器和准入控制器三部分组成。

(1)客户端。

安装在每个被管理的端点上面,接受中央控制器的策略分发,在端点贯彻策略执行,配合准入控制器强制端点提高安全等级。

客户端有两种状态:

①在线状态,这种状态下,客户端与服务器按一定的心跳间隔通信,每当通信的时候客户端察看在服务器上面是否有可用更新策略,如果有的话,就下载到本地,并应用它,结束本次通信,等待下次;如果没有,则不做任何事情,等待下一个心跳重复检测。

②离线状态,这种状态下,客户端应用本地的默认策

略。

(2)中央控制器。

集中控制管理客户端和准入控制器的策略。此控制器,针对客户端有防火墙规则、入侵检测保护规则、主机完整性检测规则等,并且提供了管理客户端的两种组织方式:一种是根据计算机来管理,比较适合非域组网方式使用;另一种是根据用户名来管理,比较适合域组网方式使用。针对准入控制器,中央控制器制定一些配置性策略。比如,指定信任的外部地址;指定够强壮的内部可信服务器地址;指定受限客户端可以访问的资源等等。

(3)准入控制器。

接受中央控制器的策略,贯彻策略执行。可以是网桥式的强制网关型控制器,也可以是利用一些现有的网络控制协议来做认证的认证控制器。这些强制的形式虽然不同,但它们要检测的内容基本相同。检测的东西是主机完整性信息,在中央控制器上面注册的特性信息(用于标示客户端身份)等等。如果验证通过就给与放行;如果没有通过验证,就把这个客户端切换到受限的区域,加以隔离或者加以补救提高。这种验证也是按心跳来的,客户端在每次验证心跳到来之际就要接受新的验证,只有客户端的安全性保持在一定的高度,才能长时间地接入网络。

针对外网端点和内网端点接入位置的不同,为了对各种端点作全面的控制,准入控制器可以分为网关型准入控制器和局域网准入控制器(如图1所示)。网关型准入控制器是摆放在整个内网出口处的,一般放在防火墙,VPN服务器后方,它是网桥模式的包转发装置,通断受到中央控制策略;局域网型准入控制器就接在局域网内部,利用某些认证协议提供的认证机制来控制交换机端口。

4.2　接入控制过程

当装有客户端的外网端点想接入内网的时候,网关型准入控制器要求外网端点发送用户信息、主机完整性结果等信息,收到之后,先看这个客户端要访问的地址是不是内部可信任地址(这个可信任地址是指足够强壮的内部主机的地址),如果是则放行,接着看这个客户端的地址是不是受信的外部地址(这个受信地址是指已经被熟知的没有恶意的外部主机地址),如果是则放行,不是就进行身份认证,确认是同一中央控制器属下客户端,并且主机完整性检测结果也通过之后,就允许接入内部网路。经过一段时间,此次认证结果超时过期,则重新进行认证(见图2)。

4.3　自动地做补救措施

如果某一端点装了客户端,经过一系列的检测,发现主机完整性检测失败了。这个时候这个端点就被拒绝接入,如果用户想要接入预期网络的话,就得要根据主机完整性规则所检测的条目,逐条更改,使其满足要求。上文讲到,对于一个计算机水平偏低的用户来讲,这是很困难

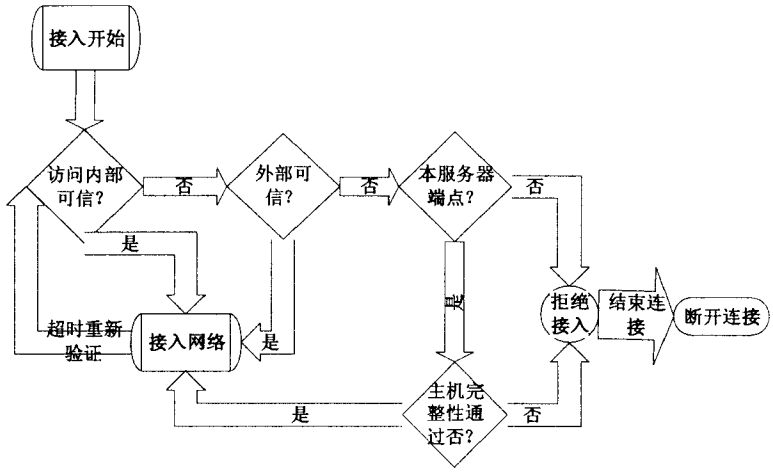

图2　接入控制流程图

的事情,即使是对于高水平的用户来说,这也是很麻烦事情。所以,形成一个安全自动地、不需要用户参与的补救措施就显得很有意义了。

如图1所示,在局域网内设置了一个补救服务器,为了让外网接入失败的主机可以访问这个服务器,可以把它设成内部可信地址,这样准入控制器在拒绝某一客户端接入网络的同时,可以给出一个补救措施,并指向这个补救服务器让客户端可以取得必要的资源。等一项补救措施完成,再对其做主机完整性检测,检测还是不通过,则继续补救其他的项目,直到主机完整性检测通过,客户端得以接入预期网络。

这种补救措施的实施方法,都是自动完成的,对用户是透明的,用户需要做的事情只是多等待一段时间。这就解决了一部分"人"的问题。

4.4　更大程度地解决"人"的问题

假如检测通过了,此端点可以接入网络了。但是,对于一个移动端点,在公司,在家里,或者在客户公司,它们的一些安全设置应该是不一样的,比如,在公司内网,被认为是在工作,为了保证公司内网的安全,就不允许去一些娱乐性质的网址浏览,下载文件。要是在家里需要把这种限制放开,在家里就应该享受一下生活了。这样一来,每天上下班用户就需要把安全设置改过来改过去,显然给用户带来了管理上的困难。

这里提出一个根据接入网络的处所自动切换安全策略的方法,称之为"自动处所切换"。就是根据对接入环境的不同的检测结果,在客户端自动地应用某套对应的安全策略。具体地讲,可以根据接入网络的客户端端点的接入方式,比如以太网接入、拨号接入、无线接入等来切换;可以根据本地使用的网络地址、网卡物理地址、域名解析服务器地址等来切换;也可以根据是否是通过VPN接入来切换;还可以根据注册表中某项值来切换等等。

这种自动切换的机制为经常更换接入处所的用户免除了很多的麻烦,也让端点及时地应用合适的安全策略,提高了端点的安全级别。

(下转第232页)

们也不能否认自己产生的签名。

(6)抗滥用性:在我们的代理签名方案中用到了证书 m_w,用证书 m_w 规定了代理的权限。因此该方案具有抗滥用性。

4 基于双线性对的代理多签名方案

代理多签名体制,它允许一组原始签名人授权给一个代理签名人来代表他们。伊丽江等人[4]于 2000 年首先提出了代理多签名体制的概念和两个代理多签名体制,此后又有几个代理多签名体制[5,6]被提出。文中基于上述方案提出一新的代理多签名方案。

假设 $A_1, A_2, \cdots, A_n$ 表示原始签名人的组,对任意 $i \in \{1,2,\cdots,n\}$,A_i 的秘密密钥为 x_i,A_i 对应的公开密钥为 $Y_i = x_iP$,$A_1, A_2, \cdots, A_n$ 想把他们的签名权力委托给某个代理签名人 B。B 的公开秘密密钥对(x_b, Y_b)满足 $Y_b = x_bP$。原始签名人的组产生委任状 m_w,在委任状 m_w 中有关于委托关系的详细描述。

(1)代理密钥生成。每个原始签名人 $A_i(i \in \{1,2,\cdots,n\})$ 计算 $s_i = x_iH_2(m_w)$,然后 A_i 把 m_w 和 s_i 发送给代理签名人 B。B 收到后检验是否有 $e(S_i,P) = e(H_2(m_w),Y_i)$,如果这个等式成立则 B 计算 $X = s_1 + s_2 + \cdots + s_n + x_bH_2(m_w)$ 作为代理秘密密钥,而代理公开密钥为 $Y_1 + Y_2 + \cdots + Y_n + Y_b$。其中 B 的代理秘密密钥 X 只有 B 自己知道,其他人包括原始签名人 $A_i(i = 1,2,\cdots,n)$ 也无法知道。

(2)代理签名生成。对消息 M 代理签名人 B 利用基于双线性对签名机制(把 X 作为签名密钥)来获得代理签名 $S = XH_2(M)$。

代理签名验证收到消息 M 和代理签名 $S = XH_2(M)$ 后验证者利用原始签名人 $A_i(i = 1,2,\cdots,n)$ 和代理签名人 B 的公钥可以验证代理签名。他接受此代理签名当且仅当:

$$e(S,P) = e(H_2(M),H_2(m_w))(Y_1 + Y_2 + \cdots + Y_n + Y_b))$$

其方案正确性可由下述等式保证:

$$e(S,P) = e(xH_2(M),P) = e(H_2(M),XP) =$$
$$e(H_2(M),(s_1 + s_2 + \cdots + s_n + x_bH_2(m_w))P) =$$
$$e(H_2(M),(x_1 + x_2 + \cdots + x_n + x_b)H_2(m_w)P) =$$
$$e(H_2(M),H_2(m_w))(Y_1 + Y_2 + \cdots + Y_n + Y_b))$$

5 小 结

双线性配对被用来构造密码体制,包括加密体制和签名体制。文中利用双线性配对提出了一个新的代理签名体制、一个新的多代理签名体制。新体制最重要的一点是,代理签名的长度均独立于原始签名人或代理签名人的个数。

参考文献:

[1] Mambo M, Usuda K, Okamoto E. Proxy Signature for Delegating Signing[A]. In Proc 3rd ACM Conference on Computer and Communications Security[C]. New York: ACM Press, 1996.

[2] 马春波,何大可. 基于双线性映射的卡梅隆门限签名方案[J]. 计算机研究与发展, 2005,42(8):1427-1430.

[3] Bonch D, Lynn B, Shacham H. Short signatures from the Weil pairing[A]. In: Advances in Cryptology - Asiacrypt' 2001[C]. Lecture Notes in Computer Science 2248. Heidelberg: Springer,2002.514-532.

[4] Yi Lijiang,Bai Guoqiang,Xiao Guozhen. Proxy multi-signature scheme :A new type of proxy signature scheme[J]. Electronic Letters,2000,36(6):527-528.

[5] Hwang S J,Chen C C. A new proxy multi-signature scheme [A]. In: Proceedings of International Workshop on Cryptology and Network Security[C]. Taiwan: Springer - Verlag, 2001.26-28.

[6] Sun H. On proxy multi-signature schemes[A]. In: Proceedings of International Computer Symposium[C]. Taiwan: Springer-Verlag,2000.65-72.

(上接第 229 页)

5 总 结

网络端点接入控制的概念提出了怎样控制单个网络端点的安全级别,较好地解决了让用户更方便、更安全地接入网络的问题。相信在其被广泛应用之后,整个网络环境安全水平都会有大幅度的提高。

参考文献:

[1] 中国互联网络信息中心. 中国互联网络发展状况统计报告(2005/1)[EB/OL]. http://www.cnnic.net.cn/download/2005/2005011801.pdf,2005.

[2] 国家计算机网络应急技术处理协调中心. CNCERT/CC2005 年上半年网络安全工作报告[EB/OL]. http://www.cert.org.cn/upload/2005CNCERTCCAnnualReport.pdf,2005.

[3] Roberts P F. Startups Rush to Fill Network Access Control Void[EB/OL]. http://www.eweek.com/article2/0,1895,1860588,00.asp,2005-09-19.

[4] 思科网络准入控制计划首度"接触"中国厂商[EB/OL]. http://news.xinhuanet.com/it/2005-01/10/content_2439189.htm, 2005-01-10.

[5] Rasmussen M. Demand for Endpoint Security Growing, Forrester Research[EB/OL]. http://www.csoonline.com/analyst/report2170.html,2004,01-30.

[6] 李 军. 渐成热门的网络端点安全技术[J]. 计算机安全, 2005(1):14-16.