建设“实名、有序、有界”内网信息安全体系

王昊宇[1]，张国力[2]，方晓辉[3]
([1]四川大学计算机学院，四川 成都 610000；
[2]北京邮电大学经济管理学院，北京 100876；[3]首钢信息部，北京 100041)

[摘　要] 第一代互联网有三大特征，即“开放、自由、无界”，使互联网自诞生以来短短数十年时间，便迅速得到普及，也使互联网从诞生之时起就伴随着不安全的因素。结合首钢内网安全体系的建设，针对“开放、自由、无界”给内网安全带来的隐患，在保证互联网特点的前提下，从安全角度出发，提出了“实名、有序、有界”的安全理论，并收到了较好效果，使互联网的应用更上了一个新的台阶。

[关键词] 互联网；内网安全；实名；有序；有界
[中图分类号] TP393　　[文献标识码] A　　[文章编号] 1009-8054(2010) 08-0070-03

“Real_name, Orderly, Bounded” Intranet Security System

WANG Hao-yu[1], ZHANG Guo-li[2], FANG Xiao-hui[3]
([1]Computer Institute, Sichuan University, Chengdu Shichuan 610000, China;
[2]College of Economics and Management, Beijing University of Posts and Telecommunications, Beijing 100876, China;
[3]Shougang Information Department, Beijing 100041, China)

[Abstract] The 1st-generation Internet has such three features as “openness, freedom and unboundedness”, and in a short period of several decades since its emergence, these features make the Internet rapidly popular while with unsafety factors. This paper, in combination with the building of Shougang intranet security system, tells of the security risks brought about by “open, free, unbounded” intranet. And in the premise of ensuring Internet characteristics, from a viewpoint of security, the "real_name, orderly, bounded "security theory is proposed, and good result is achieved, thus making application of the Internet climb one storey higher.

[Keywords] the internet; intranet security; real-name; orderly; bounded

0　引言

第一代互联网有三大特征，即“开放、自由、无界”。也正是这个特征使互联网自诞生以来短短数十年时间，便迅速普及到全世界及各行各业。也正是这三大特征，使互联网从诞生之时起就伴随着不安全的因素，可以说在互联网上安全问题也是无处不在的，这时的“开放、自由、无界”，就成了“无序、匿名、无界”。“无界”是由网络的开放性决定的，它突破了国家和地域的界限，也突破了意识形态的概念，使互联网上充满了各种各样、真真假假、有用无用的信息；“无序”是指互联网缺乏统一的管理机制和统一的法律文书，只要有硬件设备谁都可以任意接入互联网，成为互联网的一部分；“匿名”指互联网是一个虚拟的世界，用户在网络上的身份是不能与现实的真实身份相对应的，而是一个虚拟的“匿名”身份。这“三大特征”与系统的脆弱漏洞、威胁攻击的结合，就形成了互联网系统的不安全性。

收稿日期：2010-06-03
作者简介：王昊宇，1989年生，男，大学本科，四川大学计算机学院，研究方向：计算机科学；张国力，1975年生，男，硕士研究生，北京邮电大学经管学院，研究方向：信息网络安全、信息系统安全合规管理，方晓辉，1956年生，男，大学本科，高级工程师，首钢信息部，研究方向：信息技术。

1　问题的提出

目前有一种观点认为第一代互联网的这“三大特征”，天生带有不安全性，无法彻底解决，为此要彻底推翻重来，建立“实名、有序、有界”的互联网接入才能解决互联网的安全问题。这种观点太悲观了，推翻重来也不现实，但是“改良”是可行的，使互联网相对安全是能够做到的。这种要建立“实名、有序、有界”互联网的观点对于内部的局域网是可以一试的。

局域网是指各单位、各行业为实现各自的信息化应用而广泛建立和使用的内部局域网，也是基于互联网建立起来的，也全面承载了互联网的“三大特征”，也就有不安全的问题。特别是近年来随着各局域网组建单位业务的扩大，跨行业尤其是

跨地域的经营，使内部的局域网不得不借助国际互联网进行内部业务的传递，这就引出内部局域网同国际互联网一样的安全问题，主要表现在："边界"不清，与外部互联网任意乱联且无防护，导致病毒泛滥和黑客攻击，给内部网络造成极大的安全隐患；终端设备的随意接入，使不确定的因素带进内网中；"匿名"指网内缺乏有效的身份认证机制，各种匿名访问、误操作或用他人身份访问现象的存在，也为内网安全埋下了风险；"无序"指网内无序的设备LVAN，无序的资源使用，无序的安全策略，这种规则的缺失，是内网极不安全的因素。

但是局域网与互联网还是有很大区别的，在内网中结构比较清晰、用户相对固定、资源比较明确、应用比较简单，为此人们就能够构造一个"有序、有界、真实"的内部局域网。

2 建立稳固的内网安全有效边界

如果内网也无界，也就变成了互联网，而无界是危险的，所以必须把内网做到有界，为此就要把内网的边界建设成一个安全清晰的边界。

2.1 与互联网的联接边界

对于非绝对"保密"的内部局域网一般都与互联网相联，以便于对互联网的访问，或经过互联网访问其他内部网络、邮箱等。但是要从技术和行政手段上要求全网统一一个互联网出口，其他无线、专线、拨号等与互联网相联的出口一律关闭，并从技术上限制网内的设备经过其他出口对互联网的访问行为，设置与互联网隔离的防火墙，实现内网与互联网的逻辑隔离。

在互联网端口上设置双向访问控制策略，将网内的邮箱、网站等对外公开发布信息的设备放在DMZ区域，严格与内部应用系统隔开，将内部服务器地址端映射到为外部提供服务的公网IP地址上，外网用户可以在此访问邮箱、网站等，却无法经过此端口访问网内的其他应用系统，起到保护内网区域的作用；需要经过互联网端口访问内网应用系统的用户，采用虚拟专网(VPN)认证技术，并设置访问控制，只开启相应的应用系统端口地址和服务规则，只能访问被授权的应用服务器地址，否则不能访问任何内网的应用系统，把外网攻击降到最小的程度。

设置内网用户通过计费网关及内容审计网关访问互联网的策略，封闭病毒、黑客和假冒等高危网站，以防止过多的病毒危险进入内网，通过与计费网关设置的联动使只有被授权的用户可以访问指定的互联网站资源，而不能双向访问。为防止内网中假冒IP地址对互联网的访问行为，采取源IP地址与源设备的MCA地址的绑定办法，有效地避免了内部非授权用户对互联网的访问。

2.2 内网不同功能区和不同无线局域网(WLAN)的边界

局域网内有众多不同区域和不同的WLAN划分，重要应用的系统统一置于一个重要的区域内，用防火墙严格地与互联网和其他区域隔离，重要的WLAN之间也用防火墙隔离，并进行访问策略的设定；各个分局域网间无论是用什么"专线"相联的，都要用UTM防火墙隔离，并设置双向的访问策略，对不同的协议进行不同的控制。只有经过授权的用户才能经过"专线"访问另一个局域网的授权访问的资源，防止非法越权访问。即设置内网中不同WLAN之间的边界和不同的访问策略。

2.3 终端边界

内网的边界也要包括终端设备，而且是必须管理起来的重要边界。对于从终端设备接入内网的要从"实名"和安全两方面去管。网络的所谓"实名"是指设备的实名，从终端设备接入时，就要按照使用单位、使用人员(或使用系统)的规则为终端设备命名，即所谓的"实名制"，并将终端设备占用的IP地址与设备的MCA地址绑定，使设备无法改变也不能被其他设备冒充，用实名的办法确定接入终端的合法性和真实性。

终端设备的"安全"，指要接入的终端设备自身要符合内网的安全规定，如：要有正版的操作系统，要及时更新补丁，要有正版的杀病毒系统，并及时更新病毒代码，没有病毒等不合内网安全策略的"程序"，不得用其他方式与互联网连接(还可以设定更严格的安全策略，如不得使用UBS接口、只能运行规定的程序、检查注册表及登录密码等)。

建立认证服务器和策略服务器形成终端管理系统，其原理是：利用接入层交换机的X802.1X协议类型和终端管理系统来对要接入的终端设备进行准入管理(见图1)。通过对交换机的配置和Wlan的设定，将内网划分为3个区域：正常工作区、安全修复区和访客隔离区。工作原理是：当未安装认证客户端的终端设备在接入内网时先进入访客隔离区，经过审查后安装认证客户端；对虽然安装了认证客户端但不符合安全策略的终端设备进入安全修复区，进行安全策略的修复工作，使之符合内网的安全策略；对安装了认证客户端，又通过了安全策略检查的终端进入内网区进行工作。以此来规范内网终端的边界，对不是本局域网的终端设备又不符合安全策略的彻底进行隔离。

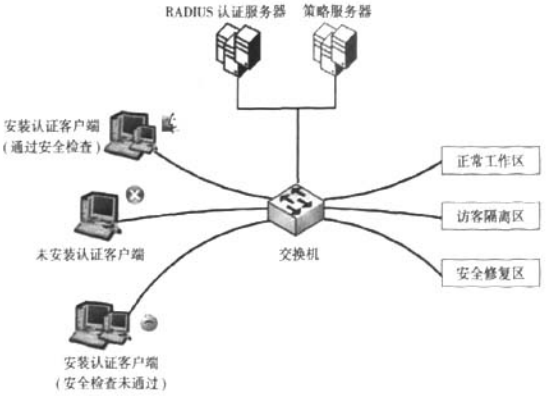

图1 终端安全准入系统架构

还有其他几种技术和方法，也可以实现对终端准入控制的管理，这里不再介绍。

3 建立身份认证的“实名”真实系统

“匿名”访问和使用互联网信息是互联网的特点之一，没有“匿名”就不可能有互联网快速发展到今天的局面，但它也是最不安全的因素之一。就内网而言，绝不能以“匿名”的方式访问各种应用信息，而必须实名访问，这里的实名是指用户的实名，即要建立统一的安全身份认证系统，进行内网的身份认证，实现“实名”访问。

(1) 身份认证

即验证消息的收发者是否有正确的身份符号，如口令或密钥。最原始的认证方式，即人们熟悉的“用户 + 口令”，这是在解决“what you know 你知道什么”的问题，它是建立在“只有你一个人知道”的假设上，但是这种认证方式有一个致命的缺陷，即认证的“通行字”无论是直存还是单向函数值，都存在于计算机本机的硬件上，抵挡不住字典式攻击而使身份“失密”；第二种身份认证技术依赖的依据是“who you are 你是谁”，即一个人独一无二的身体特征，如指纹、脸谱等，这种技术可靠性很强，但是成本很高且不易对信息进行加密；第三种技术解决“what you have 你有什么”，它是假设某一个东西只有你本人拥有，如 IC 卡、USBKey 个人数字证书或动态口令卡等，通过出示这个东西也可以确认你的身份。要在被认证方没有泄密自己身份的前提下能够以电子的方式来证明自己的身份，其本质是被认证方拥有一些私密信息，任何第三方都无法伪造，被认证方能够使认证方相信他拥有那些私密，则他的身份就得到了认证，这就是 PKI 身份认证技术。

(2) PKI 身份认证体系（见图 2）

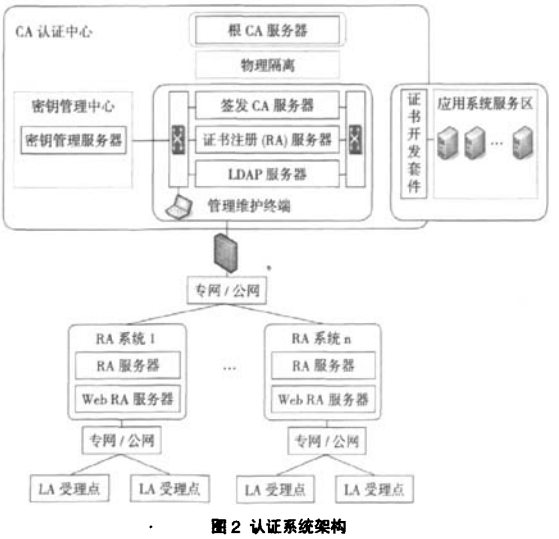

图 2 认证系统架构

这是一套典型的多级安全认证系统，被广泛应用于大型跨地区内网系统的身份认证识别中。它由认证中心 (CA) 和密钥管理中心 (KMC) 及证书注册分中心 (RA) 组成，利用统一的身份标识和信息安全传输加密技术，对信息的交互双方进行身份的验证和签名验证，只有当用户的身份得到确认后，才允许用户对系统进行访问，而系统也为用户提供了真实性的“身份认证、信息加密、信息完整和不可抵赖”的网络信息安全 4 大要素的服务。

如果为了进一步加强安全性，对于数字证书可以采取双因子认证的方式，将数字证书存于 USBKey 介质中，USBKey 内置智能芯片，可以存放 CA 和私钥的各种信息，完成认证、数据加密所需的工作。非法用户无法获取私钥信息，也就防止了假冒身份的登录和访问行为。

(3) 工作原理

统一建立一个 CA 中心，负责实现证书签发、吊销、恢复及证书生命周期的管理，同时结合密钥，用于传输的加密管理。证书可以分为双因子、动态等多种模式；多级 RA(含子级 RA) 对每次要使用应用系统的用户进行身份认证的核实工作；经过身份核实的进入应用区访问工作；系统或用户可以选择对传输信息的加密与否。

4 建立安全的内网规则

“无规则就不安全”，这句话用在互联网的信息安全方面非常贴切，为此，内网需要建立一套运行规则来保证内网的信息安全。其实上面谈到的建立边界和身份认证就是一种规则，同时还要加强以下规则：

① 安全策略规则：统一安装部署网络防病毒系统，及时升级保证时时监控有效；正版操作系统，及时升级打补丁；

② 主动防御规则：部署入侵检测防护、漏洞扫描系统；经常对系统进行安全审计；

③ 员工行为规则：终端设备安装运行软件管理、访问互联网内容管理和终端流量管理。

总之，在内网安全的落实方面，认真协调了子网安全控制和通向外网的网关控制的关系，收到了较好效果。在内网安全管理方面，也采取了随需应变的策略。通过建立内网管理规则，以及技术和行政的结合来规范内网的管理。

5 结语

内网是简化了的互联网，所以它的管理程度远远低于互联网的管理，只要按“实名、有界、规则”就一定能够管好内网。但是黑客、病毒的技术也在不断的发展，所以内网的安全也是相对的，这就要求人们要经常不断地加强内网的安全建设，把安全问题作为信息建设的永恒话题来抓。