文章编号:1001 - 9081(2005)09 - 2074 - 04

网络诱捕式入侵防御模型的设计

陈 凌[1,3],黄 皓[1,2]
(1. 南京大学 计算机科学与技术系,江苏 南京 210093;
2. 南京大学 软件新技术国家重点实验室,江苏 南京 210093;
3. 江南计算技术研究所,江苏 无锡 214083)
(chnleon@126.com)

摘 要:在研究分析 Honeypot 相关技术的基础上,提出了一个网络诱捕式入侵防御模型。入侵防御系统从主动防御的角度去解决网络安全问题,从而将黑客入侵行为引入到一个可以控制的范围,消耗其时间,了解其使用的方法和技术,跟踪其来源,记录其犯罪证据。

关键词:蜜罐;蜜网;入侵防御系统;主动防御
中图分类号:TP393.08 **文献标识码**:A

Design of a deception-based intrusion prevention model

CHEN Ling[1,3], HUANG Hao[1,2]
(1. *Department of Computer Science and Technology, Nanjing University, Nanjing Jiangsu* 210093, *China*;
2. *State Key Lab for Novel Software Technology, Nanjing University, Nanjing Jiangsu* 210093, *China*;
3. *Jiangnan Institute of Computer Technology, Wuxi Jiangsu* 214083, *China*)

Abstract: Based on the study and analysis of honeypot technology, a deception-based intrusion prevention model was proposed. According to the model, an intrusion prevention system based on proactive defense can trap and track the hacker, waste the hacker's time and record his intrusion.

Key words: Honeypot; Honeynet; IPS; proactive defense

随着网络脆弱性的变化和攻击技术的不断发展,黑客不断地开发新的攻击方法和工具用以逃避现有的安全防护体系。因此,传统的、被动防御的、静止不变的网络安全防护体系已经无法适应网络安全的需要,一个有效的防御系统将直接瞄准潜在的、新的攻击,找出延迟其破坏的方法并对其进行特定的监控分析和攻击预警处理,从而起到积极有效的主动防御目的。

当前,Honeypot[1,2] 和 Honeynet[1,2] 相关技术作为主动防御关键技术之一,逐渐为国内外众多安全机构所接受。本文正是通过研究分析 Honeypot 相关技术,并在此基础上设计和实现了一个网络诱捕式入侵防御模型的原型系统,与其他网络安全防护机制相比较,该模型创新性地提出了基于 HoneyToken[3] 组件的分布式资源监控、预警和协同响应机制,侧重于在早期检测内部、外部和未知攻击(包括未经授权的密码使用和资源访问),从而实现增强网络防御入侵的能力,并通过创建伪装的网络环境来实现对攻击的转移和牵制,从而为网络中的重要区域/资源提供保护。

1 Honeypot 和 Honeynet 技术

1.1 Honeypot 技术

根据 L. Spitzner[1-3] 的定义:Honeypot(蜜罐)是一种资源,其价值是被攻击或攻陷。Honeypot 的主要作用是模拟一个或多个易受攻击的主机,给黑客提供一个容易攻击的目标,所有与 Honeypot 进行的连接尝试都应被视为是可疑的。另外,Honeypot 还可以拖延攻击者对其真正目标的攻击,让攻击者在 Honeypot 上浪费时间。通常 Honeypot 会为我们提供额外的、有价值的信息,它可能不会直接提高计算机网络的安全,但是具有主动防御的特点,可以预测和发现新的攻击方法和安全漏洞,可以用来收集信息学习黑客活动、动机、技术和能力,是一种间接的网络安全解决方案。

1.2 Honeynet 技术

Honeynet(蜜网)也叫"陷阱网络",是由多个蜜罐构成的一个蜜罐网络,它是蜜罐概念的一种延伸,是一个包含安全缺陷的网络系统。Honeynet 的主题思想是在网络信息系统中构建一个让人攻击的平台,并通过同时使用多种操作系统平台和服务系统,使其与真实的网络环境更接近,用来模拟实际或虚构的网络运行以更加准确地了解黑客的攻击趋势和特征。

Virtual Honeynet[4](虚拟蜜网)借用了 Honeynet 技术的概念,并利用 VMM[5](Virtual Machine Monitor)相关技术将多个 Honeypot 及 Honeynet 相关部件运行在一个系统或有限的几个系统上,其优点是降低了成本而且容易部署和维护。

1.3 HoneyToken

HoneyToken 是 Honeypot 概念的一种延伸,与 Honeypot 相比,它已不仅仅是一种计算机资源,而是一种用于捕获非授权访问的数字实体或信息系统资源。换句话说,HoneyToken 是一种预先伪装的"数字资源诱饵",在创建一个 HoneyToken 后,任何使用和访问都是非法的,即均可视作是被攻击者越权访问。用作 HoneyToken 的资源通常可以是信用卡号码,电子表格文件,幻灯片文件,数据库记录,或者一个假造的用户名和口令等。HoneyToken 的一个重要性质是守法者不会去访问它,也就

收稿日期:2005 - 03 - 11;**修订日期**:2005 - 05 - 19 **基金项目**:国家 863 计划资助项目(2003AA142010)
作者简介:陈凌(1974 -),男,浙江临海人,工程师,硕士,主要研究方向:计算机网络与安全; 黄皓(1957 -),男,教授,博士生导师,主要研究方向:安全信息系统.

是说任何 HoneyToken 的访问者都是潜在的攻击者。

2　入侵防御模型的设计

2.1　入侵防御的思想和过程描述

（1）设计思想

网络诱捕式入侵防御模型的主要设计思想是将主动诱捕相关技术引入现有的入侵检测安全机制，并通过设计实现特定的功能组件来完成分布式资源监控、预警、协同响应、入侵转移、牵制和主动诱捕等功能。当在早期检测到内部、外部和未知攻击时，需要通过与其他安全产品的协同工作来完成入侵行为的转移、牵制和实时监控等操作，以尽可能地达到有效执行企业安全策略和间接保护服务器安全的目的，同时减少了安全防护体系中的“缝隙”，更高效地处理安全问题，保护整体安全。

（2）入侵防御的过程描述

首先，需要在综合评估和分析整体网络安全的基础上，按照特定的安全策略在被保护网络中的各关键资源点设置和创建不同类型的数字诱饵，并对其进行实时监控。

同时，根据特定的安全策略在被保护网络中的各关键主机上启动入侵预警探头（Sensors）来实时检测针对被保护网络的攻击行为。

然后，当数字诱饵主动诱捕到异常访问行为或入侵预警探头（Sensors）检测到攻击行为时，模型将协同其他网络安全系统或设备进行预警响应，并将后继的相关异常网络通信或黑客入侵行为转移至预先设计和部署的虚拟蜜网环境中进行入侵牵制和监管。

而后，虚拟蜜网环境将提供一个伪装和诱捕入侵者的虚拟网络环境，用以进一步的监控和研究入侵者的行为，并可以提供对入侵过程的安全审计、离线恢复和取证分析等功能，必要时还可以提供攻击现场的自我保护和隔离功能，从而保护真正服务器的安全，提高网络的整体安全防护性能。

2.2　体系结构设计及网络部署

为了适应网络安全的积极防御需求，我们设计实现了网络诱捕式入侵防御模型的原型系统。其体系结构如图 1。

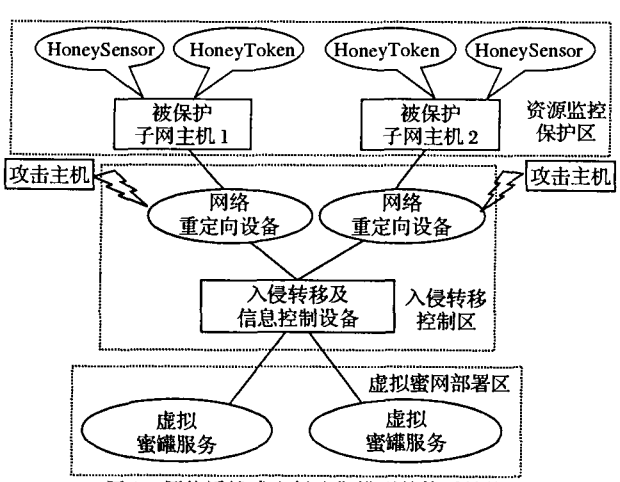

图 1　网络诱捕式入侵防御模型的体系结构

在体系结构图中，入侵防御模型采用分布式结构设计，各主要模块/组件的功能将以应用程序、软件模块、专用设备和网络系统等多种实现方式来体现，并在实际网络中按照其设计的功能特点分成资源监控保护区、入侵转移控制区和虚拟蜜网部署区三个主要功能区域进行网络部署。以下就三个功能区域的网络部署分别进行说明。

（1）资源监控保护区将由多个被保护子网所构成，每个被保护子网中除了可以部署防火墙系统、入侵检测系统等安全设备外，还需要根据不同的安全需求在多个主机系统和服务器上设置 HoneySensors 和 HoneyTokens。其中，HoneySensors 将以应用程序或软件模块的形式存在，而 HoneyTokens 将以不同形式的数字资源存在，每个 HoneyToken 将对应特定的 HoneyToken 组件，HoneyToken 组件将以应用程序或软件模块的形式存在。模型的资源监控、早期预警和协同响应功能正是在此区域通过 HoneySensor 和 HoneyToken 组件得到了有效的发挥。

（2）入侵转移控制区将由网络重定向设备和入侵转移及信息控制设备所构成，如图 1 所示，攻击者所在的主机通过特定的网络连接方式联入此区域，并经由此区域通向被保护子网和虚拟蜜网。模型的网络重定向、入侵转移和信息控制功能在此区域通过以上两种专用设备的形式得到了有效的发挥。

（3）虚拟蜜网部署区将由多个虚拟蜜罐服务构成，各虚拟蜜罐服务将按照特定的安全策略和伪装策略提供虚拟的网络信息系统，从而为入侵者提供实际或虚构的网络和系统运行环境，用以进一步地了解黑客的攻击意图。

2.3　主要功能模块

模型主要由 5 个功能模块所构成，其逻辑关系可如图 2 所示。

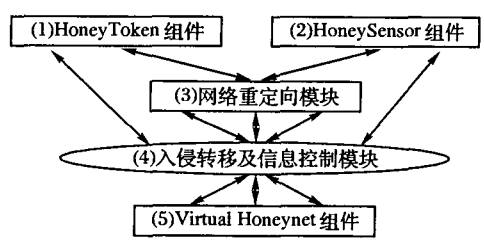

图 2　模型的主要功能模块

（1）HoneyToken 组件

HoneyToken 组件是用来创建、管理 HoneyToken 并可以监控其访问行为的软件模块，它主要包含 HoneyToken 创建模块、HoneyToken 访问行为监控模块和 HoneyToken 联动响应模块，其主要功能为：

① HoneyToken 创建模块用以为被保护网络的各关键资源点创建不同类型的 HoneyToken（如文件、数据库记录、伪造的用户 Login 等）；

② HoneyToken 访问行为监控模块用以对被保护网络的关键资源实施访问监测和异常检测；

③ HoneyToken 联动响应模块提供与其他网络安全产品和部件的协同响应功能。

（2）HoneySensor 组件

HoneySensor 组件主要负责检测针对常用网络服务应用的攻击，而后进行攻击行为的预警响应和安全审计，并将响应需求和审计日志通过专用的加密通道传送到入侵转移及信息控制模块。

HoneySensor 组件的功能模块设计按常用的网络服务类型来划分，主要包含 WebSensor 模块、FtpSensor 模块、MailSensor 模块和其他 Sensor 模块。以下我们将以 WebSensor 模块的设计为例进行简单介绍。WebSensor 模块主要是针对 Apache Web Server，并以特定的软件模块形式嵌入到 Apache 服务器代码中，用于在 Web 服务器和其他模块

处理之前对 Web 请求进行攻击检测和预警响应。WebSensor 模块的设计主要包含三个部分：

① Mod_Security 子模块。负责检测针对 HTTP 协议应用程序的攻击，并对攻击行为进行预警响应和安全审计操作；

② Mod_Evasion 子模块。负责检测针对 Web Server 的 DoS 和暴力攻击，并对攻击行为进行预警响应和安全审计操作；

③ Mod_Commun 子模块。负责将 Mod_Security 子模块和 Mod_Evasion 子模块产生的响应需求和审计日志通过专门设计的通道协议接口传送到入侵转移及信息控制设备，并由网络重定向设备联动，将其后的请求重定向到虚拟蜜网中相应的 HoneyWeb 进行处理。

(3) 网络重定向模块

网络重定向模块的主要功能是按照特定的入侵转移策略将各子网中异常网络通信转发至预先设计和部署的 Virtual Honeynet 中进行监测，并负责转发来自入侵转移及信息控制模块的外发网络通信报文。

在网络重定向模块的设计和实现过程中，如何在网络重定向操作发生后尽可能地避免引起入侵者怀疑的问题，是设计需要解决的一个关键问题，我们设计和实现了基于终端(应用层重定向器)的透明通信转发机制用来很好的解决了这个关键问题。

基于终端的网络重定向模块的设计主要包含重定向内核、数据捕获接口(PCAP Interface)和通道转发接口(Tunnel Interface)三个功能部件的内容，其中，重定向内核在深入分析 Linux 操作系统内核网桥功能模块的基础上实现了透明网桥功能。

为了提高系统的安全性能和综合网络性能，网络重定向模块需要部署在被保护网络中的各关键子网或关键服务器周围。

(4) 入侵转移及信息控制模块

入侵转移及信息控制模块的主要功能：

① 负责接收来自多个网络重定向模块的通信报文，并进行特定的封装解除操作后，按指定的要求分发给相关的 Virtual Honeynet 组件；

② 负责接收来自 HoneyTokens 和 HoneySensors 组件的响应需求及审计日志，同时将其响应需求转化为特定的入侵转移策略；

③ 负责接收来自 Virtual Honeynet 组件的响应报文，而后进行特定功能的安全监测分析，然后采取相应的措施对来自 Virtual Honeynet 组件的外发网络通信进行特定的安全限制和信息控制操作。

入侵转移及信息控制模块的设计主要包含针对网络重定向模块的通信子模块、针对 Virtual Honeynet 组件的通信子模块、入侵转移子模块和信息控制子模块四个部分的内容，其中信息控制子模块又可以根据不同的安全需求包含会话限制、带宽控制、内容过滤、会话劫持和实时通信阻断等模块的内容。由于本模块一般以网关系统的形式进行部署，而且需要处理的网络通信量较大，为了避免出现网络处理瓶颈，可以根据实际情况在被保护网络中设置和部署多个入侵转移及信息控制部件。

(5) Virtual Honeynet 组件

Virtual Honeynet 组件是基于虚拟机技术实现的由多个 Honeypot 所构成的一个虚拟网络环境，其主要功能是提供一个伪装和诱捕入侵者的虚拟网络环境。Virtual Honeynet 组件的设计主要包含 Virtual Honeypot 的运行支撑环境和网络服务伪装体系两个部分的内容。

Virtual Honeypot 运行支撑环境的设计是在 User-Mode Linux[7] project 的实现基础上，通过在其宿主操作系统和 VMM 内核模块之间设计实现安全审计及日志回放接口，用以完成对黑客攻击行为的安全审计、离线恢复和取证分析等功能，Virtual Honeypot 运行支撑环境的软件结构可如图 3 所示。

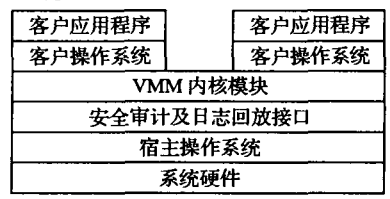

图 3 Virtual Honeypot 运行支撑环境的软件结构

网络服务伪装体系的设计主要包含伪装策略的配置管理模块、服务运行特征的伪装模块、伪装服务的远程控制模块和信息资源的伪装模块四个部分的内容。其中，服务运行特征的伪装模块和信息资源的伪装模块是网络服务伪装体系设计的核心内容。服务运行特征的伪装模块需要根据不同的伪装策略进行不同类型的服务伪装，其伪装重点将在伪装服务运行机制的基础上侧重于服务运行特征(Banner 信息、请求报文的响应、网络流量运行特征等)的虚拟仿真。信息资源的伪装模块同样需要根据不同的伪装策略进行伪装，然而，在很多场合，如何提高其欺骗质量的问题已经超出了技术实现范畴而取决于社会工程学领域的某些范畴。

3 实验分析及相关工作

在实验分析过程中，以图 1 的网络架构为主构建了一个实验测试环境，并通过特定的攻击测试案例对模型进行了功能性测试。以下就一次典型的攻击测试案例进行描述分析，案例分析过程主要侧重于模型使能前后攻击测试效果的比较分析。

攻击测试案例描述说明：

(1) 攻击测试案例可以简单概括为以下工具的攻击组合：扫描探测攻击(漏洞扫描) + Apache Web Server 的 chunk-handling 漏洞攻击(突破攻击) + Custom Backdoor 程序工具(后门植入) + 一些渗透攻击工具(子网拓展)。

(2) 主要攻击过程及步骤：首先在攻击主机 1 上使用扫描探测工具对目标子网进行探测攻击，发现子网中的某 Apache Web Server 存在 chunk-handling 漏洞，利用 Apache Web Server 的 chunk-handling 漏洞攻击对被保护子网的 Apache Web 服务器进行攻击，成功获取该主机系统的根用户权限，然后通过此 Root 权限将自行开发的 hunter 后门程序植入该系统，并上传一些渗透攻击工具，利用上传的扫描攻击工具对子网内其他主机进行扫描和攻击尝试，最后攻击者清除当前主机上所有攻击相关日志后退出该系统。

攻击测试案例的实施和比较分析：

(1) 在不启用模型各功能组件的前提下，实施以上的攻击过程，观测到的攻击效果为：被保护子网中的 NIDS 系统发现有扫描攻击日志，主机系统无攻击相关日志。

(2) 进行模型各功能组件的部署和配置，在存在漏洞的 Apache Web Server 上部署 HoneyToken，并启动 HoneyToken 组件和 HoneySensor 组件应用程序，启动网络重定向模块和入侵转移及信息控制模块的功能，在虚拟蜜网运行支撑环境中启

动相同资源配置的 Apache Web Server。

(3) 在攻击主机 1 上再次实施攻击测试案例所描述的攻击过程,攻击过程完成后,观测到的攻击效果为:HoneySensor 组件和 NIDS 的审计日志中均发现大量针对 Web Server 的探测扫描日志,但是 HoneySensor 组件的审计日志中还发现针对 Apache Web Server 的 chunk-handling 漏洞攻击相关事件;虚拟蜜网系统的安全审计和回放日志中发现一系列的攻击事件:通过记录 hunter 后门程序的上传和运行命令检测到 hunter 后门的植入,通过记录渗透攻击工具的上传和运行命令检测到渗透攻击工具的攻击尝试;网络重定向设备和入侵转移及信息控制设备的审计日志和入侵转移策略历史日志中均发现攻击事件相关的网络重定向和入侵转移操作。

(4) 比较分析结果:模型的各功能组件成功地检测到利用 Apache Web Server 的 chunk-handling 漏洞的突破攻击事件,并及时的将进一步的黑客攻击行为(后门植入和子网渗透尝试)重定向和转移到一个可控的虚拟蜜网环境,有效地保护了被保护子网 Apache Web Server 的安全。

在整个实验和测试工作中,我们从黑客的角度出发,设计了多个典型攻击测试案例对入侵防御模型进行了功能性测试,分析与实践结果表明:本文提出的入侵防御模型能实现操作系统、应用服务级的虚拟仿真,可与网络入侵检测系统等其他安全设备协同工作,实现对入侵行为的转移防护、预警响应以及对入侵过程的审计监控和取证。

通过实践,笔者还认识到:入侵防御模型的应用和功能发挥是一个复杂的工程,不是简单部署后就可一劳永逸的,而是要持续地维护和关注,才能发挥应有的效能。为了识别和捕获到新的攻击事件,需要经常对可疑的网络事件进行深度分析。

然而,本模型仅为原型系统实现,与实际应用的目标还有一定的差距,因此,未来的工作将主要侧重于其具体功能的完善和在实际场合中的应用。

参考文献:

[1] SPITZNER L. Honeypots: Definitions and Value of Honeypots[EB/OL]. http://www.tracking-hackers.com/papers/honeypots.html, 2003.

[2] SPITZNER L. Honeypot Farms[EB/OL]. http://www.securityfocus.com/infocus/1720, 2003.

[3] SPITZNER L. Honeytokens: The Other Honeypot[EB/OL]. http://www.securityfocus.com/infocus/1713, 2003.

[4] PROVOS N. A Virtual Honeypot Framework[R/OL]. Technical Report, 03-1. Center of Information Technology Integration, University of Michigan. http://www.citi.umich.edu/techreports/reports/citi-tr-03-1.pdf, 2003.

[5] KING ST, DUNLAP GW, CHEN PM. Operating System Support for Virtual Machines[A]. Proceedings of the 2003 USENIX Annual Technical Conference(General Track)[C], 2003.71-84.

[6] DUNLAP GW, KING ST, CINAR S, *et al.* ReVirt: Enabling Intrusion Analysis Through Virtual-Machine Logging and Replay[A]. Proceedings of USENIX Symposium on Operating Systems Design and Implementation (OSDI 2002)[C], 2002.211-224.

[7] DIKE J. User-Mode Linux Diary[EB/OL]. http://user-mode-linux.sourceforge.net/diary.html, 2002.

[8] JIANG XX, XU DY. Collapsar: A VM-Based Architecture for Network Attack Detention Center[EB/OL]. http://www.cs.purdue.edu/homes/jiangx/collapsar/info/content/, 2003.

[9] 刘宝旭,曹爱娟,许榕生.陷阱网络技术综述[J].网络安全技术与应用,2003(1):65-69.

(上接第 2069 页)

4.2 算法性能分析

由于 ARAN 是在基本路由协议的基础上添加一些特性设计而成的,因而它势必增加了协议的复杂性,分析如下:

(1) 由于 ARAN 协议在路由查找中不包含源路由,则在第一阶段的每个节点需存储源目的节点对对应的前趋节点的信息,以便能将路由应答信息回送至源节点,而基本的路由协议中每个节点只需维护每个目的节点对应的路由表项。ARAN 相比基本路由协议增加了对节点存储量的要求。

(2) 由于 ARAN 协议在路由查找过程中不允许由中间节点返回路由应答,且在路由查找的第一阶段后还需要最短路由的证实阶段,相比基本的路由协议交互信息更多,在一定程度上降低了路由查找效率。

(3) 由于 ARAN 协议的路由消息涉及到私钥签名、公钥验证签名、公钥加密、私钥解密等算法,而这些算法通常复杂度较高[8,9]。这一点对于资源受限的节点而言明显降低了协议的实时性与实用性。

(4) 由于 ARAN 协议采用公钥证书,则 Ad hoc 网络中需有一台证书服务器。对于规模较大的网络,可专设一个节点担当证书服务器;而规模较小的网络,则可利用一个节点来兼任。无论如何,均增加了网络铺设的成本。

虽然 ARAN 存在一些缺点,但瑕不掩瑜,它能有效地抗击大部分的恶意攻击,为路由协议提供较高的安全保障,更好地保护网络的正常运行。可以说,ARAN 协议为一种有效的按需路由安全协议,它能够较好地满足无线多跳 Ad hoc 网络在各种非军事应用领域对路由的安全需求。

参考文献:

[1] PERKINS CE, BELDING-ROYER EM, DAS S. Ad hoc On-Demand Distance Vector (AODV) Routing[EB/OL]. http://moment.cs.ucsb.edu/pub/draft-perkins-manet-aodvbis-00.txt. Mobile Ad Hoc Networking Working Group INTERNET DRAFT, 19 October 2003.

[2] JOHNSON D. The Dynamic Source Routing Protocol for Mobile Ad Hoc Networks (DSR) [EB/OL]. http://www.ietf.org/internet-drafts/draft-ietf-manet-dsr-09.txt, April 2003.

[3] Manel Guerrero . Secure Ad hoc on - demand distance vector (SAODV) routing[EB/OL]. http://moment.cs.ucsb.edu/pub/draft-guerrero-manet-saodv-00.txt, August 2001.

[4] DAHILL B, SANZGIRI K, LEVINE BN, *et al.* A Secure Routing Protocol for Ad Hoc Networks [A]. Proceeding of 10th IEEE International Conference on Network Protocols (ICNP 2002)[C], 2002.78-87.

[5] SANZGIRI K, DAHILL B, *et al.* A Secure Routing Protocol for Ad Hoc Networks [A]. Proceedings of the 10th IEEE International Conference on Network Protocols (ICNP 2002)[C], 2002.97-105.

[6] PAPADIMITRATOS P, HAAS ZJ. Secure Routing for Mobile Ad hoc Networks [A]. Proceedings of the SCS Communication Networks and Distributed Systems Modeling and Simulation Conference (CNDS 2002)[J], 2002. 43-51.

[7] IEEE Std 802.11i. Medium Access Control (MAC) Security Enhancement[S], June 2004.

[8] GB15629.11-2003.信息技术·系统间远程通信和信息交换·局域网和城域网·特定要求·第 11 部分:无线局域网媒体访问控制和物理层规范[S], 2003.

[9] 铁满霞,吴靖,唐厚俭,等.宽带无线 IP 系统移动终端的安全接入技术[J].小型微型计算机系统,2003,24(12):2075-2079.