分布开放式的入侵检测与响应架构——IDRA

杨海松 李津生 洪佩琳

(中国科学技术大学电子工程与信息科学系信息网络实验室 合肥 230027)

摘 要 提出了一个完整的新型入侵检测与响应架构,该系统架构采用分布式的结构,符合标准化的方向,具有极强的可扩展性,能够对系统检测到的网络安全事件做出迅速的响应,及时地遏制事态发展.首先从现有的入侵检测系统出发,分析其面临的主要问题,然后提出了分布开放式的入侵检测与响应架构 IDRA,介绍其协议框架和系统架构,最后对 IDRA 的先进性以及可行性进行了分析.

关键词 入侵检测;互操作性;实时响应;安全策略

中图法分类号 TP393

IDRA: A Distributed Open Intrusion Detection and Reaction Architecture

YANG Hai-Song LI Jin-Sheng Hong Pei-Lin

(*Infonet Laboratory, Department of Electronic Engineering and Information Science, University of Science and Technology of China, Hefei* 230027)

Abstract A self-contained intrusion detection and reaction architecture (IDRA) is presented in this article. This architecture, which adopts distributed framework, is accordant with the standardizing trend and fully scalable. It can respond to network security incident rapidly, and then control the state of affairs in time. Authors first introduce the insufficiency of existing Intrusion Detection System (IDS), then present the IDRA's protocol framework and system architecture, exhibit its advantage and finally analyze the IDRA's feasibility.

Keywords intrusion detection; interoperability; real-time response; security policy

1 现有入侵检测系统的主要问题及其分析

随着计算机网络的迅速普及,网络所面临的安全威胁日渐加剧,作为网络安全系统的一个关键组成部分,入侵检测系统显示出日益增加的重要性.入侵检测是检测计算机网络中不合适的、不正确的以及不规则的活动的技术.现有的入侵检测系统在互操作能力和响应能力上存在着严重的不足.

为了全面地了解和控制网络的安全状况,同时考虑到网络攻击方式的复杂性和网络平台的多样性,必须建立大规模的分布式入侵检测系统,并对入侵检测系统进行选择组合.但是由于没有统一的业界规范可循,现有的入侵检测系统多是封闭式的,各系统间的互操作性问题严重地制约了入侵检测有效性的提高,也使系统的维护复杂度增加.

在网络技术高度发展的今天,仅仅将入侵报警提供给管理员,然后通过其它的途径对报警事件进行响应已经无法适应对响应的实时性和有效性的需求,将对报警事件的处置功能与原有的入侵检测功能结合起来是对新一代的入侵检测系统的必然要

收稿日期:2002-03-24;修改稿收到日期:2003-04-11.本课题得到国家自然科学基金重大研究计划"面向大规模网络的分布式入侵检测和预警模型"(90104030)、国家"八六三"高技术研究发展计划项目"宽带网络中的组播安全协议及应用研究"(2002AA121067)和国家自然科学基金重大研究计划"下一代网络体系结构、协议模型与机制"(90104011)资助.**杨海松**,男,1976 年生,博士研究生,主要研究方向为网络安全、策略管理、服务质量.E-mail: hsyang@mail.ustc.edu.cn.**李津生**,男,1937 年生,教授,博士生导师,主要研究方向为信息通信网和下一代 Internet.**洪佩琳**,女,1961 年生,教授,博士生导师,主要研究方向为信息通信网和网络安全.

求.已经有少数的入侵检测系统将防火墙、路由器等网络设备包括在内.这些设备可提供一些简单的措施,比如封锁端口、断开连接等,具有一定的实时响应和处置能力.但是整个系统的组成限制在特定厂家的网络设备之中,不具备扩展性和兼容性,而且提供的处置措施非常有限,其实用性也大打折扣.

2 分布开放式的入侵检测与响应架构——IDRA

为了解决现有入侵检测系统互操作能力和响应能力不足的问题,我们提出了分布开放式的入侵检测与响应架构 IDRA(Intrusion Detection and Reaction Architecture).IDRA 采用分布式的系统架构,设立两个级别的分析中心对入侵数据分析处理(核心级和分布级),每一个分析中心配有专门的监管站和安全策略服务器.我们将 IETF 策略框架工作组(policy framework)的策略系统引入到 IDRA 中,为 IDRA 提供建立在安全策略之上的响应机制.IETF 为了保证策略信息模型的兼容性,把策略区分为高层策略和底层设备相关配置策略,由普遍到具体地定义出策略信息模型的层次结构.高层策略在实施的时候被翻译为底层设备相关的配置策略.安全策略实施者就是防火墙、路由器、交换机或是网络服务器等网络节点,而目录服务器与策略服务器组合在一起提供策略服务.

为了保障安全策略的安全散发,我们在 IDRA 中采用了 IETF 入侵检测交换格式工作组 IDWG(Intrusion Detection exchange format Working Group)正在实现标准化的一系列协议作为入侵检测系统的标准通信协议.下面介绍在 IDRA 中所使用的各种协议以及这些协议如何有机地构成 IDRA 的协议框架.

2.1 IDRA 的协议框架

IDRA 采用的协议都已经标准化或是正在标准化.这一系列的协议包括入侵检测交换协议 IDXP[1](Intrusion Detection Exchange Protocol),为 IDXP 提供框架协议支持的可扩展块交换协议 BEEP[2,3](Blocks Extensible Exchange Protocol),规定 IDXP 传输报文格式的入侵检测报文交换格式协议 IDMEF[4](Intrusion Detection Message Exchange Format),而公共开放策略服务协议 COPS[5](Common Open Policy Service Protocol)被加载到 BEEP 框架协议之上,利用 BEEP 提供的安全传输通道传送安全策略.

2.1.1 可扩展块交换协议框架(BEEP)和入侵检测交换协议(IDXP)

IETF 的 IDWG 工作组使用可扩展块交换协议 BEEP 作为交换安全信息的应用协议框架,入侵检测交换协议(IDXP)是 BEEP 的子协议.BEEP 协议是一个基于连接的用于异步交互的应用协议框架,加载于传输协议之上(TCP),整个协议框架包括两个部分:BEEP 核心和一系列的子协议.BEEP 核心定义了在 BEEP 对等端点之间同时进行会话独立的报文交换的基本通信规程,而其它方面,诸如安全认证、加密以及具体应用相关的规范都在子协议中定义.在一个 BEEP 会话中包含了多个通道(channel),所有的报文交换都在通道中进行,每个通道都对应一个子协议,由这个子协议来定义通道中交换的报文的语法(syntax)和语义(semantics),并决定了该通道在应用中的具体用途,例如传输安全、用户认证或是数据交换.

IDXP 协议是一个基于连接的应用层的协议,定义了在入侵检测功能节点之间交换数据的通信规程,即将转为 RFC 标准.IDXP 协议使用 BEEP 框架内的其它几个专门子协议为通信双方提供安全认证、完整性校验和机密性保护.IDXP 可以传送的信息包括 IDMEF 报文、普通文本和二进制数据.在采用 IDXP 协议作为标准的通信协议之后,不同的入侵检测系统之间就可以实现安全信息的共享和交互.

除了用于交换入侵检测信息的 IDXP 子协议之外,在 BEEP 中还有几个与 IDXP 相关的子协议.

隧道子协议[6](TUNNEL profile):即将转为 RFC 标准,描述了如何将 BEEP 端点用作应用层的代理,通过此代理可以使经过认证的用户透过防火墙建立 BEEP 隧道连接.

传输安全子协议 TLS[7](Transport Security Profile):依据 RFC 2246 中定义的第一版 TLS 协议制订.TLS 协议在两个应用的通信过程中提供私密性和数据完整性保证.

简单认证和安全层 SASL[8](Simple Authentication and Security Layer):依据 RFC 2222 中定义的 SASL 协议制订,在 BEEP 会话建立过程中对用户的身份进行认证.每一个在 IANA(Internet Assigned Numbers Authority)中注册的 SASL 认证机制都对应有一个子协议.

2.1.2 入侵检测报文交换格式协议(IDMEF)

IDMEF 是用来表示入侵检测系统生成的各种安全信息的一种数据模型,定义了入侵检测的报文交

换格式,还给出了用可扩展标记语言 XML 来实现 IDMEF 的方法,包括其文档类型定义 DTD(Document Type Definition).

2.1.3　公共开放策略服务协议(COPS)

COPS 协议描述了一个支持策略控制的客户/服务器模型,在策略服务器(策略决定者)及其客户(策略执行者)之间协调策略信息的交换,具有可扩展性.为了将 COPS 协议加载到 BEEP 框架之上,利用 BEEP 提供的安全传输通道传送安全策略,我们提出两种引入方式:直接引入或者是 XML 结构化之后引入.

"直接引入"的方式是直接将二进制报文格式的 COPS 协议加载到 BEEP 之上.因为 BEEP 可以直接传送二进制数据,因此不需要对 COPS 协议做任何修改,但是通过 COPS 协议传送的二进制用户数据格式(就是安全策略的内容)必须明确定义并在软件的编写过程中固化在软件包内.

"XML 结构化之后引入"的方式是将 COPS 协议作为 BEEP 的子协议引入,并且将 COPS 传送的二进制用户数据格式改为用 XML 结构化的文本数据格式.

很显然,后者具有很强的可扩展性,具有更广阔的发展前景.在对一系列的协议进行了介绍之后,图 1 给出 IDRA 采用的协议框架.

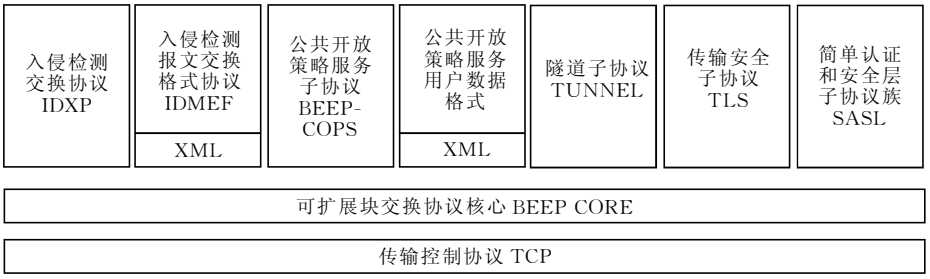

图 1　IDRA 的协议框架

2.2　IDRA 的系统架构

在介绍完 IDRA 的协议框架之后,现在给出 IDRA 的分布式系统架构.在 IDRA 的分布式系统架构中,核心级不具备对分布级的管理权限,但是具有比分布级更宽的视野.核心级的分析中心通过接收各分布级的分析中心的报告,可以对大面积的入侵行为进行检测,并将检测结果传达给分布级的监管站,同时提供建议的安全响应/处置策略对入侵报警进行处置,分布级的监管站可以直接采纳此安全策略,也可以由管理员在手工分析之后做出自己的决策.被分布级的监管站采纳的安全策略或是由分布级管理员做出的决策被下达到位于受保护网络内的检测器,这些检测器的功能在 IDRA 中进行了强化,由这些检测器将最终的响应/处置策略传达给防火墙、路由器、交换机或是网络服务器来执行.

管理员可以预先设定安全策略,在合适的时候由系统直接采用,及时地遏制事态发展.核心级管理员设定的规则一般需要经过分布级管理员允许才会被采用,当然分布级管理员也可以设定系统总是采纳核心级的安全策略.图 2 是 IDRA 的分布式系统架构示意图.

结合前面介绍过的 IDRA 协议框架,下面按照三个级别对 IDRA 中的几个关键部分的功能及其工作流程进行介绍.

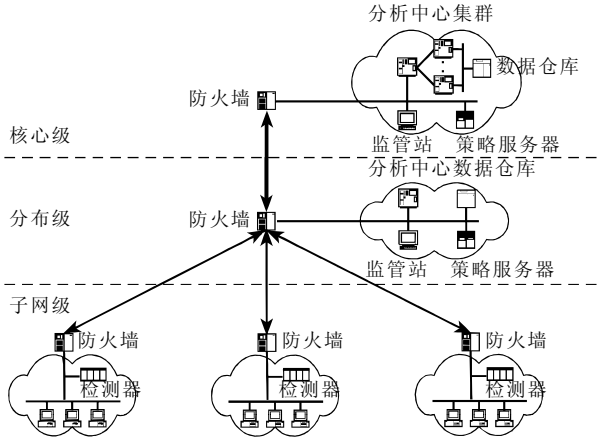

图 2　IDRA 的分布式系统架构

2.2.1　核心级

分析中心.它利用与各分布级分析中心建立的 BEEP 会话中的 IDXP 通道接收各分布级分析中心的安全数据并进行分析检测.由于核心级分析中心具有更宽的监视视野,有助于对大面积的入侵行为进行检测.经过分析处理之后的可疑事件将通过与本级的监管站相连的 IDXP 通道发往监管站.考虑到核心级分析中心在整个检测系统中所处的特殊地位,应该对分析器集群采用负载均衡技术,以保证有足够的处理能力.

监管站.它在图形用户界面上为管理员提供整个系统的工作状态显示,同时为了辅助管理员对安全事件进行有效的手工分析,还应当具备一些实用的功能,例如对误报警的管理、对已分析事件的标记、层层探究和关联分析的能力等.在我们的 IDRA 架构中,监管站还被赋予了对安全策略的管理能力.所谓的安全策略,不仅仅包括对安全事件的响应/处置策略,还包括对整个检测与响应系统的功能设置策略等,可以通过对安全策略的设置来实现整个系统的功能剪裁和配置.监管站在接收到分析中心的可疑事件报警之后,会在提示管理员的同时自动地向策略服务器发出安全策略查询请求,这一策略查询/决定下达的过程通过与策略服务器建立的 BEEP 会话中的 COPS 通道完成.查询结果将为管理员提供参考,如果查询到的响应/处置策略被认可,就作为核心级监管站的建议策略下达给相关的分布级监管站;如果没有相关策略或是没有合适的策略可用,管理员可以手动设置合适的策略并下达,同时这一策略也被加入策略服务器作为下一次同类事件的处置参考.如果管理员经过手工分析判定可疑事件没有足够的安全威胁,也可以选择忽略.对于一些检测准确率比较高的攻击或是一些"温和"的预防措施(例如压制调速 Throttling 技术),可以在策略中规定无须管理员参与就直接将包含了响应/处置措施的策略规则传达给相关的分布级监管站.

策略服务器.在 IDRA 架构中,每一个策略服务器都有自己的目录服务器,这两者被组合在一起提供策略服务.策略服务器提供方便的用户界面,帮助管理员对目录数据库进行维护.存储在目录数据库中的安全策略使检测工作具有了继承性和可积累性,为以后的检测分析提供了参考.策略服务器接收到监管站策略查询请求之后,对目录数据库进行检索,并将检索到的包含了响应/处置措施的策略规则返回给监管站.

数据仓库.它是一个作为决策支持系统 DSS(Decision-making Support System)和联机分析处理 OLAP(On-Line Analytical Processing)数据源的结构化数据环境.采用关系数据库实现的联机分析应用称为 ROLAP,采用多维数据库实现的联机分析应用称为 MOLAP.数据仓库在分析中心的检测过程中发挥着重要的作用:在入侵检测过程中有大量的分组数据信息需要存储,这些分组数据信息就是做出分析检测决策的数据源,根据时效的不同,一些被完整地保存在数据仓库中,而另一些则被缩减后再存储在数据仓库中.

2.2.2 分布级

分布级分析中心.功能等同于核心级的分析中心,但是待分析的数据来自于下辖网络的检测器,在对这些数据进行检测分析之后,还必须将其中一些核心级可能感兴趣的数据上传给核心级的分析中心.

分布级监管站.它具有和核心级的监管站同样的功能,但是分布级的监管站能够从核心级获得建议策略.需要注意的是,只有当此建议策略被本级的管理员采纳之后才会真正施加到本级所辖的网络中,就是说每一个分布级的管理员对下辖的网络具有绝对的管理权,并不受核心级的约束.通过这样的设计,使得网络的管理权仍然掌握在实际的网络所有者手中,但是同时又提供了大面积的入侵检测与响应能力.

分布级策略服务器.功能等同于核心级的同类设备,但是被存入策略信息库中的安全策略不仅仅来自于本级的管理员,还可能是被本级管理员所采纳的核心级的建议策略.

分布级数据仓库.功能等同于核心级的数据仓库,存储的数据来源于本级所辖的网络内部.

2.2.3 子网级

检测器.其监视所在网络内的分组数据,并利用与分布级分析中心建立的 BEEP 会话中的 IDXP 通道将分布级分析中心可能感兴趣的分组数据上传.同时检测器被赋予了策略代理的功能,负责通过与分布级监管站建立的 BEEP 会话中的 COPS 通道接收安全策略,并将这些策略传达给所有可控制的网络设备,这些设备就是真正的安全策略实施者,策略分发的通信协议同样采用加载在 BEEP 之上的 COPS 协议.

策略分发的任务交给检测器实现而非分布级的监管站出于两个原因.首先,本着分级管理的原则,每个子网级的网络内可以受安全策略控制的设备只有检测器掌握了它们的具体情况;其次,分布级监管站的负载能力有限,无法再承担直接将安全策略分发到安全策略实施者的繁重任务.

安全策略受控设备.例如防火墙、路由器、交换机及网络服务器等,这些设备是安全策略的实施者.具体的响应/处置策略可能会要求这些设备切断某个连接、封锁某个端口,甚至断电以保护网络不受更为严重的破坏.对合理而且有效的处置措施进行研究并且把它们用合适的安全策略表述清楚是 IDRA 的一项重要任务.在 IDRA 中,对防火墙还有特殊的

要求,就是能够提供 BEEP 隧道的建立服务.

2.3 IDRA 的功能连接关系

图 3 给出了 IDRA 协议框架和系统架构的功能连接关系.需要再次说明的是,加载在 BEEP 之上的 IDXP 通道和 COPS 通道的传输安全、身份认证以及应用层隧道支持是通过 TLS 子协议、SASL 子协议和 TUNNEL 子协议得到的.

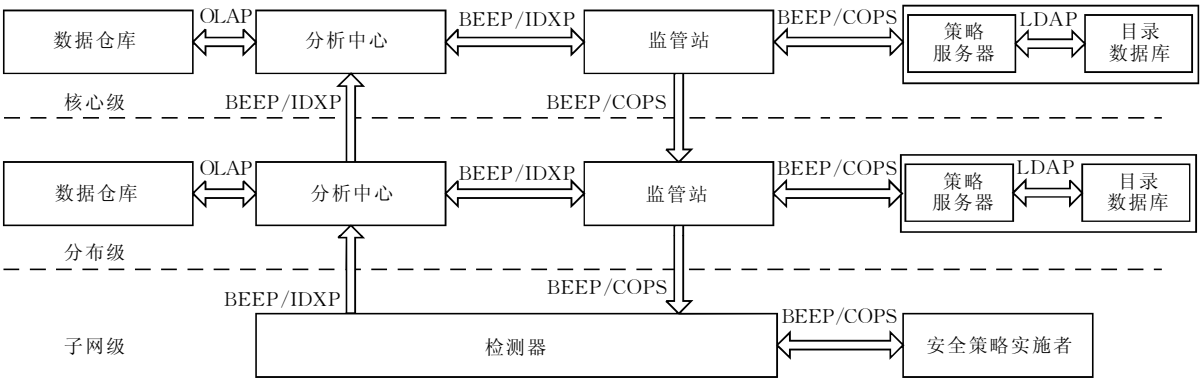

图 3　IDRA 节点之间的功能连接图

3　IDRA 的先进性

我们提出的 IDRA 很好地解决了入侵检测系统架构中的互操作问题以及"实时"响应和处置问题,为下一代入侵检测与响应系统提供了由目前的主流协议构成的完备的协议框架和系统架构.IDRA 的先进性体现在以下几个方面.

(1) 所有协议均为标准协议或是即将标准化,并采用扩展性极强的 XML 语言作为核心描述语言;

(2) 采用分布式的系统架构,分工明确,视野宽阔,响应/处置过程迅速、准确 ;

(3) 采用规范的策略系统架构,以安全策略为响应/处置过程的核心,易于对系统进行剪裁配置,有利于表述复杂规则,同时处置措施可以以策略形式保存,使检测工作具有继承性和可积累性;

(4) 将 COPS 协议加载于 BEEP 框架之上,利用 BEEP 框架提供的用户认证、加密等功能来保障策略服务,同时采用 XML 来实现 COPS 协议,更增加了其扩展性;

4　IDRA 的可行性分析

长期以来,对入侵检测系统的响应/处置能力的研究进展缓慢,除了缺少统一的标准协议导致各厂家的系统不具备互操作性之外,可能还有管理权限和自动响应处置的准确度问题.

4.1　管理权限的问题

在大规模的入侵检测系统中,被监管的网络通常不属于同一组织,这些组织有各自的网管人员对网络进行管理,虽然分析中心可以对入侵行为进行检测,但是对入侵行为如何响应和处置的决定权不属于分析中心.于是多数的入侵检测系统通常只是在发现入侵行为之后在控制台向管理员发出警告,然后由管理员和现场的网管人员联系,商量采取何种措施.这样的响应速度和响应方式显然无法令人满意,再考虑到现场网管人员安全意识和技术水平的限制,更加使得正确的安全决策执行起来困难重重.

在 IDRA 的系统架构中,核心级管理员设定的规则一般需要经过分布级管理员允许才会在子网级网络使用,除非分布级管理员设定系统总是采纳核心级的安全策略.就是说对网络的管理权限仍属于网络的所有者,核心级的分析中心只能够提供建议的处置策略,但是此机制为分布级管理员提供了选择机会,使得此级别的管理员不需要具备很强的分析能力.

通过赋予分布级管理员最终执行权,解决了大规模的入侵检测系统面临的管理权限问题,并且从核心级管理员做出决策,到此决策被下达到分布级监管站,直至最终被位于子网级的检测器传达给防火墙、路由器等安全策略实施者,全部的操作都在本系统内高效准确地完成.

4.2　自动响应/处置的准确度问题

入侵检测系统的误警率是不得不考虑的另一个问题.如果赋予了安全策略过于强大的功能,在没有人工分析参与的情况下,可能很多的正常网络应用都会被入侵检测系统视为恶意的攻击行为加以阻

断.尽可能地降低入侵检测系统的误警率是一项长期而且艰苦的工作,但是在误警率降到足够低的程度之前,我们依然有足够的理由为入侵检测系统添加自动响应/处置的能力.

首先,被管理员预先添加到安全策略信息库中的策略是有限而且可控的,只要安全策略得到明智小心的设计,也是比较安全的,而采用安全策略系统所带来的好处却是显而易见的,例如入侵检测系统因此具备了用户定制、剪裁的能力,并且一些成功的安全策略可以被反复使用,大大减小了管理员的工作量等.其次,可以采用的处置手段有很多种,其中有一些很精巧的响应方式来对疑为攻击的分组进行处理,在不完全切断的情况下监视可疑业务的变化,最终可以做出比较准确的判断.最后,网络上流传着越来越多的攻击工具,这些已经"通俗"的攻击手段被众多的好奇者反复使用,类似的攻击已经可以比较准确的识别,完全可以交给安全策略系统自动处置,而不必通过管理员.

5 总 结

经过以上的讨论,我们已经对分布开放式的入侵检测与响应架构 IDRA 做出了描述.首先我们分析了入侵检测与响应架构 IDRA 的产生背景,对 IDRA 中所采用的一系列关键协议以及 IDRA 的系统架构进行了介绍,然后分析了其必要性和先进性,讨论了一些曾经阻碍入侵检测与响应系统发展的问题并逐一分析解决.现在我们可以得出结论:这是一个完整的新型入侵检测与响应架构,该系统架构采用分布式的结构,符合标准化的方向,具有极强的可扩展性,能够对系统检测到的网络安全事件做出迅速的响应,及时地遏制事态发展.

参 考 文 献

1 Feinstein B *et al*. The Intrusion Detection Exchange Protocol (IDXP), draft-ietf-idwg-beep-idxp-07, 2002

2 Rose M. The Blocks Extensible Exchange Protocol Core. RFC3080, 2001

3 Rose M. Mapping the BEEP Core onto TCP. RFC3081, 2001

4 Curry D *et al*. Intrusion Detection Message Exchange Format Data Model and Extensible Markup Language (XML) Document Type Definition. draft-ietf-idwg-idmef-xml-10.txt, 2003

5 Cohen R *et al*. The COPS (Common Open Policy Service) Protocol. RFC2748, 2000

6 New D *et al*. The TUNNEL Profile. draft-ietf-idwg-beep-tunnel-05, 2002

7 Dierks T *et al*. The TLS Protocol Version 1.0. RFC2246, 1999

8 Myers J. Simple Authentication and Security Layer (SASL). RFC2222, 1997

YANG Hai-Song, born in 1976, Ph.D. candidate. His research interests include network security, policy based management and QoS.

LI Jin-Sheng, born in 1937, professor and Ph.D. supervisor. His research interests include information communication network and the next generation Internet.

HONG Pei-Lin, born in 1961, professor and Ph.D. supervisor. Her research interests include information communication network and network security.