doi:10.3969/j.issn.1001 - 893x.2013.03.019

物联网安全测评和风险评估技术研究*

雷 璟**

(中国电子科学研究院,北京 100041)

摘 要:提出采用信息安全仿真、物联网安全测评和安全风险评估技术实现的物联网安全测评和风险评估服务平台的主要技术、平台结构和系统实现。此平台能够为物联网建设方案、安全技术手段进行测试与评估,推动我国物联网建设和物联网安全产业的发展。

关键词:物联网;安全测评;风险评估

中图分类号:TN918;TP393.08 **文献标志码**:A **文章编号**:1001 - 893X(2013)03 - 0323 - 06

Research on Security Evaluation and Risk Assessment for Internet of Things

LEI Jing

(China Academy of Electronics and Information Technology, Beijing 100041, China)

Abstract: The main technology, platform framework and system realization of Internet of Things(IOT) security test with evaluation and risk assessment service platform are presented, which is realized based on information security simulation, Internet of Things security test with evaluation, security risk assessment technology. The platform can test and evaluate the construction scheme, security technology means of Internet of Things, and can also promote China's Internet of Things construction and security industry development.

Key words: Internet of Things; security test with evaluation; risk assessment

1 引 言

物联网是继计算机、互联网发展之后,信息化发展的第三次浪潮。物联网是指通过信息传感设备,按照约定的协议,把物品与各类网络连接起来,进行信息交换和通信,以实现智能化识别、定位、跟踪、监控和管理的一种网络。物联网将实现物与物、人与物的广泛"联网",物联网时代网络与人们的日常生活将更加紧密[1]。

物联网作为一项发展中的新兴网络技术,它面临着许多新的安全挑战。目前,我们对于物联网信息安全的认识还处于探索阶段,信息安全保障措施还不够完备,加强物联网网络与信息安全相关问题的研究是十分重要而迫切的。物联网产业的健康发展,也迫切地需要安全产品、安全服务的支持。

当前,国内还没有开展针对物联网的安全测评和风险评估工作,针对国家物联网发展战略和国家信息安全产业的发展需求,我们在规划物联网总体架构的基础上,对物联网安全目标体系架构进行了研究和分析,构建了一个物联网安全测评和风险评估服务平台,采用信息安全仿真技术对物联网网络环境、应用系统和安全服务等进行模拟,对各种攻击行为进行仿真。运用物联网安全测评技术和安全风险评估技术对物联网感知层、网络层、应用层安全进行基于仿真环境的测试与评估,形成物联网安全测评和风险评估服务的能力,为我国物联网安全保障体系的建设、安全防护效能评估提供验证手段和决策支撑。

* **收稿日期**:2012 - 11 - 01;**修回日期**:2013 - 01 - 28 Received date:2012 - 11 - 01;Revised date:2013 - 01 - 28

** **通讯作者**:leijanet@163.com **Corresponding author**: leijanet@163.com

2 物联网安全体系分析

2.1 物联网总体架构

物联网总体架构包括“三层两体系”,即感知层、网络层、应用层,以及信息安全保障体系、标准规范体系,如图 1 所示。

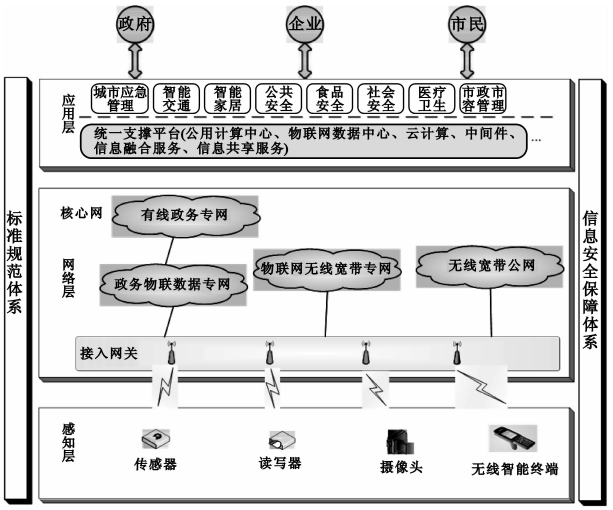


图 1 物联网总体架构图

Fig.1 The collectivity framework of Internet of Things

(1)感知层

物联网的感知层利用视频识别、红外感应、摄像头、无线智能终端、各类传感器等手段,对目标对象进行实时感知,获取基础物联数据。感知层主要包括标识感知、视频感知、位置感知、专业领域感知等。另外,感知层拥有执行控制系统,体现物联网对“物”的控制能力。

(2)网络层

物联网的网络层实现信息的传递和汇聚,其主要任务是将感知层采集到的信息,通过接入网等各种网络进行汇总和传输,将大范围内的信息进行整合,以备处理。在网络层建设物联网统一的核心网络,比如无线宽带专网、无线宽带公网、政务物联数据专网和有线政务专网等。

(3)应用层

物联网的应用层包括公用计算中心、物联网数据中心、云计算、中间件、信息融合服务、信息共享服务等统一支撑平台,以及利用这些支撑平台建立的智能化应用系统,包括城市应急管理、智能交通、智能家居、公共安全、食品安全、社会安全、医疗卫生、市政市容管理等,最终为政府、企业和市民提供精细化、智能化的服务。

(4)信息安全保障体系

建设统一的物理网网络与信息安全基础设施,包括统一的身份认证、传输网络、访问控制、安全测评、应急处置、灾难备份等;加强物联网网络与信息安全的标准制定;完善物联网网络与信息安全相关规章制度,加大对物联网安全产业的政策支持力度。

(5)标准规范体系

形成包括总体标准、感知层标准、网络层标准、应用层标准和共性标准的物联网标准体系,同时为物联网产品研发和应用开发对标准的采用提供重要支持。

2.2 安全目标体系架构

物联网安全的总体需求是物理安全、信息采集安全、信息传输安全和信息处理安全的综合,安全的最终目标是确保信息的机密性、完整性、真实性和网络的容错性,结合物联网分布式连接和管理模式,给出相应的安全目标体系架构如图 2 所示。

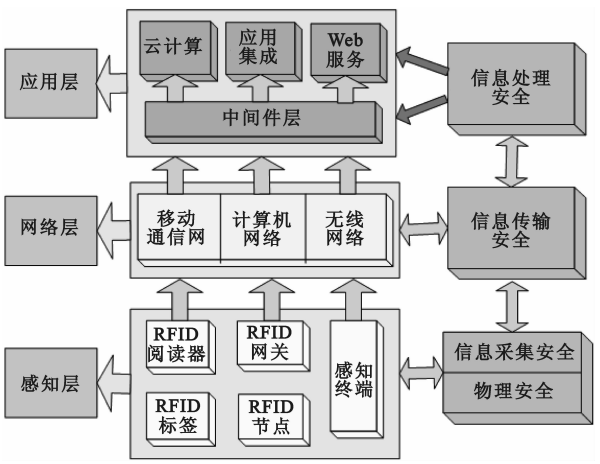


图 2 物联网安全体系架构图

Fig.2 The security framework of Internet of Things

(1)感知层安全

物联网感知层安全,主要包括物理安全和信息采集安全。物理安全是保证 RFID、摄像头等各类传感器的物理安全,防止对传感器的软、硬件进行物理攻击或破坏。信息采集安全是保证采集物理世界中发生的物理事件和数据,包括各类物理量、标识、音频、视频数据的安全。

(2)网络层安全

物联网网络层安全,主要是保障各类感知信息安全的可靠传输。通常通过信息传输端到端或节点到节点的加密机制和各种不同网络环境之间的相互认证机制来实现。

(3)应用层安全

物联网应用层安全,主要解决信息智能处理安全,包括物联网典型应用的安全和为应用提供支撑的云计算平台的安全,主要涉及到物联网用户的隐

私保护、不同应用领域的知识产权保护等问题。基于云计算平台的物联网应用安全问题主要解决云计算平台自身的安全和安全云应用的安全。

3　主要技术

通过对物联网总体架构和安全体系架构的分析可以看出,针对物联网总体架构已经有很多安全解决方案,但是目前缺少对物联网的安全技术体制进行验证的手段。运用信息安全仿真技术,搭建物联网仿真环境,可对物联网的安全技术措施、安全保障体系实现仿真。采用物联网安全测评技术和安全风险评估技术对仿真平台进行从微观到宏观、从局部到整体、从静态到动态的安全性测评和风险评估,从而为物联网的安全性与有效性提供更加客观的依据,以便为物联网信息安全保障体系的规划、设计、建设和评价提供技术手段。

3.1　信息安全仿真技术

信息安全仿真技术重点研究物联网环境与业务模拟、信息安全技术建模与仿真等技术。物联网环境与业务模拟实现对物联网感知层、网络层、应用层环境以及多种实际业务和各种服务的模拟。信息安全技术建模与仿真通过构建安全保密设备模型、攻击行为模型、安全防护体系模型,利用半实物仿真技术、分布式仿真技术、仿真可信度验证技术等来模拟物联网真实环境的运行情况,在模拟仿真过程中为测评系统提供实时动态数据,作为安全评估的依据。

3.2　物联网安全测评技术

物联网安全测评技术通过建立完整的物联网安全评估标准体系,结合各种技术测试手段,用于对新建或已建的物联网的安全性进行全面科学评估,对保密性、完整性、可用性、可控性和不可否认性等安全指标进行系统级的评估。在得出测评结论后,提供符合要求的安全解决方案。

3.2　安全风险评估技术

安全风险评估的任务是分析系统可能遭遇的全部风险,并估计发生各种风险的可能性[2]。通过物联网安全风险评估建模技术,对评估对象进行抽象,建立能为系统风险分析提供标准或最佳建议的知识库,将安全风险数据转换为风险系数以便做出决策。通过识别被评估系统中的威胁、脆弱点,以及威胁发生后对系统造成的危害并得出结论。

4　平台组成

4.1　平台结构

针对物联网的特征和面临的安全威胁,构建一个物联网安全测评和风险评估服务平台,构造仿真数据基础库、系统安全测评知识库和风险评估专家知识库,研制信息安全仿真子系统、系统安全测评子系统、风险评估子系统,最终形成物联网安全测评和风险评估的技术与服务能力,给物联网项目建设全生命周期提供物联网建设方案的评审咨询、物联网系统安全测评与风险评估、物联网系统安全仿真与验证、物联网安全等级保护方案设计咨询等方面的服务。平台设计思路如图 3 所示。

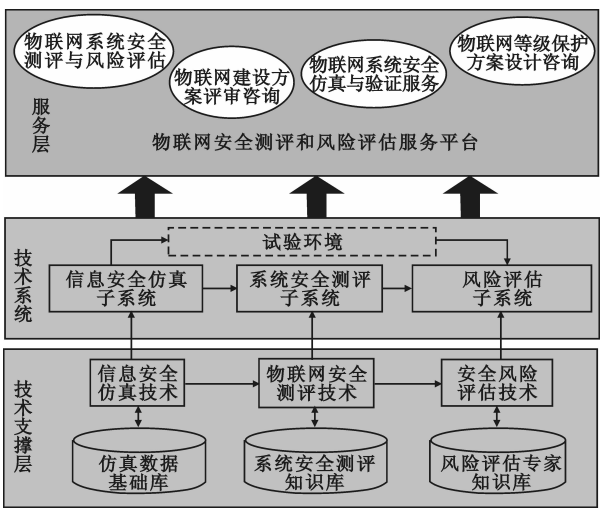


图 3　物联网安全测评和风险评估服务平台设计图

Fig.3 The design of Internet of Things security evaluation and risk assessment service platform

物联网安全测评和风险评估服务平台具体网络拓扑图如图 4 所示。

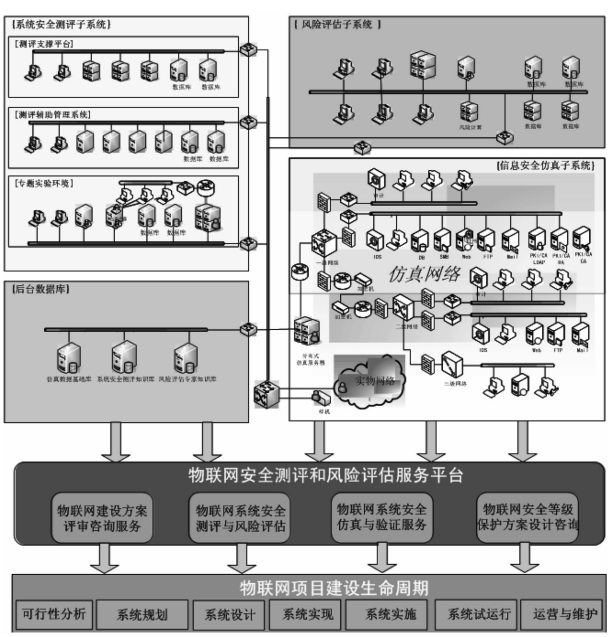


图 4　物联网安全测评和风险评估服务平台网络拓扑图

Fig.4 The network topology of Internet of Things security evaluation and risk assessment service platform

4.2 信息安全仿真子系统

信息安全仿真子系统积累各类攻击技术、安全防护设备的作用机制、特征、脆弱点、应对措施等数据,实现对物联网传感设备、网络环境、应用系统、安全服务等的可信仿真,真实再现实际物联网环境下的网络系统、安全措施、运行场景、安全行为、应用服务等,通过模拟发现物联网存在的安全隐患以及相应的应对措施。信息安全仿真子系统为系统安全测评子系统与风险评估子系统提供了数据支持,是服务的基础。

信息安全仿真子系统由安全保密设备模型、攻击行为模型、安全防护体系模型、网络环境仿真模块、信息安全行为模块、信息安全仿真验证模块等组成,其中网络环境仿真模块用于搭建物联网仿真基础平台,并集成部分安全防护功能仿真模块以及实物中的安全功能样机构建完整的安全防护体系,为仿真业务数据及导入的真实业务数据流提供运行环境。信息安全行为模块对物联网网络环境中的安全保密设备及攻击行为进行数据模型建模,形成高可信度的安全保密设备及攻击行为仿真模型。信息安全仿真验证模块用于对仿真模型的可信度进行验证。

信息安全仿真子系统能够支持设备级和系统级的仿真,为安全产品测试、网络系统安全性验证提供仿真手段。

信息安全仿真子系统的逻辑设计如图 5 所示。

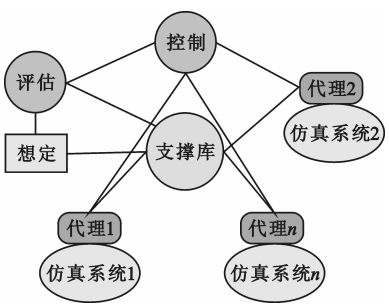


图 5 信息安全仿真子系统逻辑设计图

Fig.5 The logical design of information security simulation subsystem

信息安全仿真子系统采用基于 HLA/RTI(高层体系结构/运行支撑框架)的分布式仿真技术[3],采用协调一致的标准通信接口、标准和协议来规范各系统间的信息交换,并通过计算机网络将仿真系统连接起来,形成一个可交互的时空一致的联合仿真环境,构建物联网基于 HLA/RTI 体系多 OPNET 平台的多网系分布式、交互式联合仿真。

4.3 物联网安全测评子系统

物联网安全测评子系统是在掌握攻防技术作用机理、各类传感设备和物联网存在的安全漏洞等知识的基础上,有针对性地改进和完善现有的测试技术手段与工具,以高效地完成踩点、扫描、检测、渗透、验证、取证及获取测试数据等安全测试的全过程,准确地发现物联网的安全漏洞,真实地展现安全目标系统的现状。该系统是提供物联网安全测评和风险评估服务的核心环节。

物联网安全测评子系统建设内容主要包括 3 个部分,即测评标准、提供底层支撑的测评支撑平台和针对物理安全、网络安全、应用安全等进行测评的专题实验室。系统组成结构如图 6 所示。

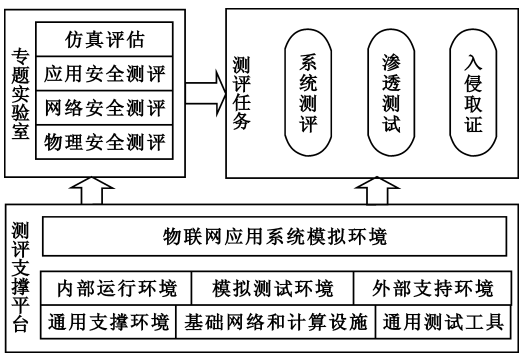


图 6 物联网安全测评子系统组成结构图

Fig.6 The composition of Internet of Things security evaluation subsystem

4.3.1 测评标准

物联网安全测评标准是在参考国内国际相关信息安全标准的基础上,结合物联网的特点,研制出可操作性强的物联网安全测评准则,并形成物联网安全测评标准体系。

物联网安全测评标准技术要求主要包括感知层安全要求、网络层安全要求和应用层安全要求。其中,感知层安全要求主要包括传感器设备安全、传感网络安全等,网络层安全要求主要包括核心网接入安全、移动通信接入安全、无线接入安全、边界安全防护等,应用层安全要求主要包括数据安全、云计算安全、中间件和服务安全等。

4.3.2 支撑平台

测评支撑平台为物联网安全测评提供硬件和软件支撑环境,由基础网络和计算设施、通用支撑环境和通用测试工具组成。

(1)基础网络和计算设施

基础网络和计算设施提供基本网络通信设施和计算资源,包括内部运行环境、模拟测试环境和外部支持环境。

(2)通用支撑环境

为支持各类测评任务提供通用的操作系统和中间件级的运行支撑环境,包括操作系统、数据库软件、中间件软件、虚拟机软件、软件开发环境、仿真软件、数据恢复检测工具等。

(3)通用测试工具

为了支撑测评任务,提供通用的测试工具,包括端口扫描工具、网络/操作系统弱点扫描软件、应用程序/数据库弱点扫描软件、密码破解软件、文件分析工具、网络分析工具、漏洞检查工具等。

4.3.3　专题实验室

专题实验室主要针对物理安全、网络安全、应用安全等进行测评,由物理安全测评实验室、网络安全测评实验室和应用安全测评实验室组成。

(1)物理安全测评实验室

物理安全主要针对传感器节点的电路和天线的安全性以及各个节点间的身份进行测试和评估。采用模拟攻击的测试方法,对测评对象施加真实的物理攻击,以检验系统的健壮性和安全性。

(2)网络安全测评实验室

重点对物联网多种异构网络间的身份认证、访问控制和边界防护措施进行测试和评估。

(3)应用安全测评实验室

针对应用系统和软件的安全性、功能、性能、稳定性、兼容性、代码合法性进行测试和评估,同时对云计算平台的安全性进行测试和评估。

4.4　风险评估子系统

4.4.1　系统组成

信息安全风险管理是一个不断降低安全风险的过程,目标是将安全风险降低到用户和决策者可以接受的程度[4]。物联网信息安全风险评估就是对物联网系统的信息安全风险程度进行分析评价,系统地分析所面临的信息安全威胁及其存在的脆弱性,评估信息安全事件发生的可能性,并结合信息安全事件所涉及的价值来判断事件一旦发生造成的影响与等级[5]。在系统的软件实现上,针对物联网的特点,通过多接口技术,实现数据采集与处理,从系统级的角度,实现风险评估的自动化。物联网风险评估子系统的组成如图 7 所示。

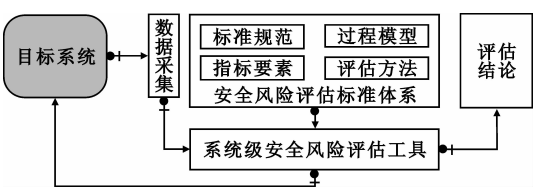


图 7　风险评估子系统组成图

Fig.7 The composition of risk assessment subsystem

4.4.2　基本要素

风险评估是围绕着基本要素进行的。物联网系统的风险主要由 4 个风险因子构成:资产、威胁、脆弱性、安全措施。风险评估基本要素的关系如图 8 所示。

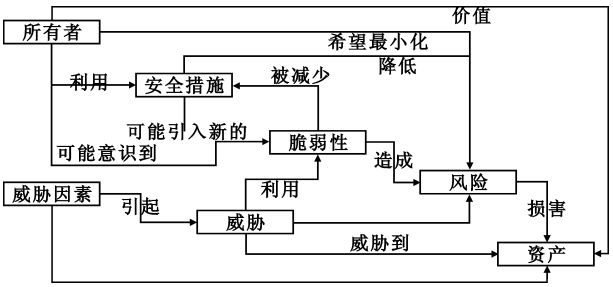


图 8　风险评估基本要素关系图

Fig.8 The relation of risk assessment basic element

资产:在物联网系统风险评估中,进行资产识别主要考虑物理事件和数据等。

威胁:指可能对资产造成不期望事件的主体,包括通过网络进入物联网系统的行为人、通过物理方式接近物联网系统的行为人、系统问题、自然灾害、病毒及恶意代码等。

脆弱性:指物联网系统中存在的可以被威胁主体利用而造成对系统不期望影响的缺陷或弱点。

安全措施:指为控制风险而采取的措施。

4.4.3　评估流程

风险评估的流程主要包括资产识别、威胁识别、脆弱性识别、安全措施分析、可能性分析、影响分析以及最后的安全性判定[6]。我们针对物联网的特点,对物联网评估过程的基本逻辑模型的设计如图 9 所示。

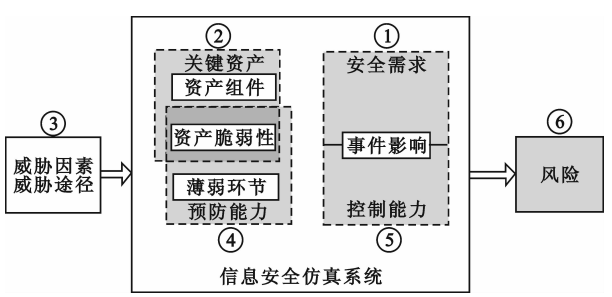


图 9　评估过程模型图

Fig.9 The model of evaluation process

在这个评估过程模型中,物联网系统风险评估的流程主要包括以下六方面的内容。

(1)系统分析:对物联网系统的安全需求进行

分析。

(2)识别关键资产:根据系统分析的结果识别出物联网系统的重要资产。

(3)识别威胁:识别出物联网系统主要的安全威胁及威胁的途径和方式。

(4)识别脆弱性:识别出物联网系统在技术上的缺陷、漏洞、薄弱环节等。

(5)分析影响:分析安全事件对物联网系统可能造成的影响。

(6)安全性判定:综合物联网关键资产、威胁因素、脆弱性及控制措施,综合安全事件影响,评估物联网系统面临的风险。

4.4.4 风险计算

风险计算是对风险基本要素进行识别、估价,再对这些要素的值进行函数计算,以得到风险值。通过以下步骤可以对风险进行计算[7]。

(1)预先价值矩阵

利用威胁发生的可能性、脆弱性被利用的难易程度以及资产价值的三维矩阵来确定风险的大小。

(2)根据风险排列威胁

首先定义威胁潜在影响的估价制度和威胁发生可能性的估价尺度;其次针对所识别的每个威胁评估其潜在影响和可能性;最后进行风险计算,排列风险等级。

(3)计算风险发生的频率和可能的影响

通过评估每项资产风险发生的频率和可能的影响,确定资产的风险。首先对资产赋值,其次评估风险发生的频次,再次根据资产和频次确定风险值,最后计算每个系统的每项资产的总得分,据此排列优先等级。

5 结束语

通过信息安全仿真、物联网安全测评和安全风险评估技术而构建的物联网安全测评和风险评估服务平台,已经在智慧北京顶层设计和北京物联网体系顶层设计中提供了技术支撑。同时,能够为物联网网络和重要系统的安全运行提供测试评估的仿真环境和平台,可为我国物联网建设项目提供信息安全专业化服务,带动我国物联网安全测评和风险评估技术的发展,提升我国物联网信息安全技术的研发水平,最终为实现物联网信息安全跨越式发展提供有效的保障手段。该平台还可以在测评标准和测试手段上进一步完善,提高平台的服务能力和服务流程,对于推动我国物联网建设和物联网安全产业发展具有重要意义。

参考文献:

[1] 雷吉成.物联网安全技术[M].北京:电子工业出版社,2012:34-35.
LEI Ji-cheng. Internet of Things security technology[M]. Beijing: Publishing House of Electronics Industry,2012:34-35.(in Chinese)

[2] 曾庆凯,许峰,张有东.信息安全体系结构[M].北京:电子工业出版社,2010:222-225.
ZENG Qing-cai, XU Feng, ZHANG You-dong. Information security framework[M]. Beijing: Publishing House of Electronics Industry,2010:222-225.(in Chinese)

[3] GUAN Li, ZOU Ru-ping, ZHU Bin, et al. An HLA/RTI Architecture Based on Multi-thread Processing[J]. Journal of China Ordnance,2010(3):182-188.

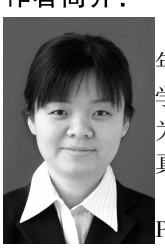
[4] 王凯.信息安全风险评估分析方法浅析[C]//国防科技工业网络信息安全技术发展研讨会论文集.北京:国防科学技术工业委员会科技与质量司,2004:110-112.
WANG Kai. Information security risk assessment analysis method shallow analysis[C]//Proceedings of National Defence Technology Industry Network Information Security Technology Development Proseminar. Beijing: Technology and Quality Department of National Defence Technology Industry Committee,2004:110-112.(in Chinese)

[5] 徐小涛,杨志红.物联网信息安全[M].北京:人民邮电出版社,2012:223-224.
XU Xiao-tao, YANG Zhi-hong. Internet of Things information security[M]. Beijing: People's Posts and Telecommunications Press,2012:223-224.(in Chinese)

[6] 向宏,傅鹂,詹榜华.信息安全测评与风险评估[M].北京:电子工业出版社,2009:313-314.
XIANG Hong, FU Li, ZHAN Bang-hua. Information security test with evaluation and risk assessment[M]. Beijing: Publishing House of Electronics Industry,2009:313-314.(in Chinese)

[7] Wang Chengqun, Chen Jiming, Hu Chonghai, et al. Kernel matrix learning with a general regularized risk functional criterion[J]. Journal of Systems Engineering and Electronics, 2010,21(1):72-80.

作者简介:



雷 瑾(1977—),女,湖北武汉人,2003年于华中科技大学获计算机应用技术专业工学硕士学位,现为高级工程师,主要研究方向为信息安全、信息网络安全建设、网络安全仿真评估。

LEI Jing was born in Wuhan, Hubei Province, in 1977. She received the M.S. degree from Huazhong University of Science and Technology in 2003. She is now a senior engineer. Her research interests include information security, information network security construction, network security simulation and evaluation.

Email:leijanet@163.com