

普通高等教育“物联网工程专业”规划教材

物联网 安全导论

李联宁 编著

清华大学出版社



013028363

TP393.4
499

普通高等教育“物联网工程专业”规划教材

物联网安全导论

李联宁 编著



北航 C1635061

清华大学出版社
北京

013058383

内 容 简 介

本书详细介绍了物联网安全技术的基础理论和最新主流前沿技术,全书共分为6部分:物联网安全概述、物联网感知识别层安全、物联网网络构建层安全、物联网管理服务层安全、物联网综合应用层安全、物联网安全标准和安全体系规划设计。以12章的篇幅按互联网的网络结构分别讲述物联网安全需求分析、物联网安全技术架构、密码与身份认证技术、RFID系统安全与隐私、WSN无线传感器网络安全、无线通信网络安全、互联网网络安全、中间件与云计算安全、信息隐藏技术原理、位置信息与隐私保护、物联网信息安全标准以及安全体系结构规划与设计。每一章除了相关理论外,还讲解了最新前沿技术的原理。各章都附有习题以帮助读者学习理解理论知识和实际工程应用。为方便教师教学,附有全套教学PPT课件等。

本书主要作为高等院校物联网工程、信息安全、自动化、通信工程、计算机应用和电气信息类专业高年级本科生和研究生教材,也可作为物联网安全技术的专业培训教材。对物联网安全和可靠应用领域的管理决策人员、从事物联网安全领域应用和设计开发的人员以及计算机网络工程技术人员都有学习参考价值。

本书封面贴有清华大学出版社防伪标签,无标签者不得销售。

版权所有,侵权必究。侵权举报电话:010-62782989 13701121933

图书在版编目(CIP)数据

物联网安全导论/李联宁编著. —北京:清华大学出版社,2013.4

普通高等教育“物联网工程专业”规划教材

ISBN 978-7-302-30377-0

I. ①物… II. ①李… III. ①互连网络—安全技术—高等学校—教材 ②智能技术—安全技术—高等学校—教材 IV. ①TP393.4 ②TP18

中国版本图书馆CIP数据核字(2012)第242152号

责任编辑:白立军 战晓雷

封面设计:常雪影

责任校对:李建庄

责任印制:王静怡

出版发行:清华大学出版社

网 址: <http://www.tup.com.cn>, <http://www.wqbook.com>

地 址:北京清华大学学研大厦A座 邮 编:100084

社总机:010-62770175 邮 购:010-62786544

投稿与读者服务:010-62776969, c-service@tup.tsinghua.edu.cn

质量反馈:010-62772015, zhiliang@tup.tsinghua.edu.cn

课件下载: <http://www.tup.com.cn>, 010-62795954

印 装 者:北京密云胶印厂

经 销:全国新华书店

开 本:185mm×260mm 印 张:23 字 数:575千字

版 次:2013年4月第1版 印 次:2013年4月第1次印刷

印 数:1~3000

定 价:39.00元

产品编号:049180-01

前 言

随着物联网技术的飞速发展,物联网在中国受到了全社会极大的关注。与其他传统网络相比,物联网感知节点大都部署在无人监控的场景中,具有能力脆弱、资源受限等特点,这使得物联网安全问题比较突出,并且当国家重要基础行业和社会关键服务领域(如电力、金融、交通和医疗等)重要社会功能的实现即将依赖于物联网应用时,物联网安全问题已经上升到国家层面。

2010年后,全国已有近700所高等院校向教育部提交了增设物联网等相关专业的申请,首批37所院校已获准开设物联网相关专业。目前符合大学物联网安全专业教学要求的教材十分稀缺,社会上对物联网安全技术书籍的需求数量也很大。本书试图在对物联网安全技术领域做详细介绍的基础上,给出实际工程案例及行业解决方案,以达到技术全面、案例教学及工程实用的目的。

本书主要分为6个部分,分别按物联网安全的技术架构分层次详细讲述涉及物联网安全的各类相关技术。

第一部分:物联网安全概述。简单介绍物联网信息安全的基本概念和主要技术,包括3章,内容为物联网安全需求分析、物联网安全技术架构和密码与身份认证技术。

第二部分:物联网感知识别层安全。介绍涉及物联网感知层安全的理论与技术,包括2章,内容为RFID系统安全与隐私和WSN无线传感器网络安全。

第三部分:物联网网络构建层安全。介绍涉及物联网网络层安全的理论与技术,包括2章,内容为无线通信网络安全和互联网网络安全。

第四部分:物联网管理服务层安全。介绍涉及物联网管理服务层安全的理论与技术,包括1章,内容为中间件与云计算安全。

第五部分:物联网综合应用层安全。介绍涉及物联网应用层安全的理论与技术,包括2章,内容为信息隐藏技术原理和位置信息与隐私保护。

第六部分:物联网安全标准和安全体系规划设计。简单介绍物联网安全标准和安全体系规划,包括2章,内容为物联网信息安全标准和安全体系结构规划与设计。

本书主要作为普通高等院校本科生和研究生教材,教材力争紧跟物联网安全技术的最新发展,使用大量的实际工程案例辅助教学,使学生在完成学习后能够具备实际工程能力。对专业从事物联网工作的领导干部、研究人员和工程技术人员也有学习参考价值。

书中各章都附有习题,以帮助读者学习理解和实际工程应用。同时,可以从清华大学出版社网站(www.tup.com.cn)下载配套的教学课件(PowerPoint演示文件)以便教学使用。

本书由李联宁教授编著,在本书编写过程中,编者参考了国内外大量的物联网及计算机网络书刊及文献资料,在此对有关文献的作者表示感谢。对于本书中的错误或不妥之处,恳请广大读者不吝赐教。

编者

2012年12月

第一部分 物联网安全概述

第 1 章 物联网安全需求分析	3
1.1 物联网安全性要求	3
1.1.1 物联网安全涉及范围	3
1.1.2 物联网安全特征	4
1.2 物联网结构与层次	5
1.2.1 感知识别层	6
1.2.2 网络构建层	6
1.2.3 管理服务层	7
1.2.4 综合应用层	8
1.3 物联网的安全技术分析	9
1.3.1 物联网安全的逻辑层次	10
1.3.2 物联网面对的特殊安全问题	10
1.3.3 物联网的安全技术分析	11
1.3.4 物联网安全技术分类	12
1.4 感知识别层的安全需求和安全机制	13
1.4.1 感知识别层的安全需求	14
1.4.2 感知识别层的安全机制	15
1.5 网络构建层的安全需求和安全机制	15
1.5.1 网络构建层的安全需求	15
1.5.2 网络构建层的安全机制	16
1.6 管理服务层的安全需求和安全机制	17
1.6.1 管理服务层的安全需求	17
1.6.2 管理服务层的安全机制	18
1.7 综合应用层的安全需求和安全机制	18
1.7.1 综合应用层的安全需求	19
1.7.2 综合应用层的安全机制	20
1.8 影响信息安全的非技术因素和存在的问题	20
1.8.1 影响信息安全的非技术因素	20
1.8.2 存在的问题	20
1.9 未来的物联网安全与隐私技术	21

习题一	22
第 2 章 物联网安全技术框架	23
2.1 常用信息安全技术简介	23
2.1.1 数据加密与身份认证	23
2.1.2 访问控制和口令	23
2.1.3 数据加密算法	25
2.1.4 数字证书和电子签证机关	27
2.1.5 数字签名	28
2.2 物联网安全技术架构	29
2.2.1 物联网加密认证	29
2.2.2 密钥管理机制	31
2.2.3 数据处理与隐私性	33
2.2.4 安全路由协议	33
2.2.5 认证与访问控制	35
2.2.6 入侵检测与容错容错技术	36
2.2.7 决策与控制安全	37
2.2.8 物联网安全技术发展现状	38
习题二	38
第 3 章 密码与身份认证技术	39
3.1 密码学基本概念	39
3.1.1 密码学的定义和作用	39
3.1.2 密码学的发展历程	39
3.1.3 古典密码学	41
3.1.4 现代密码学	42
3.1.5 加密技术分类	43
3.2 现代加密算法	45
3.2.1 加密算法	45
3.2.2 加密算法的选择与应用	49
3.3 对称密码技术	51
3.3.1 对称密码技术简介	51
3.3.2 分组密码	52
3.3.3 序列密码	53
3.3.4 对称密码的算法	53
3.4 非对称密码技术	55
3.4.1 公钥密码算法概述	55
3.4.2 RSA 算法	57
3.4.3 RSA 在数字签名中的运用	60

3.5	认证与身份证明	63
3.5.1	认证与身份证明概述	63
3.5.2	身份认证系统	64
3.5.3	个人特征的身份证明	66
3.6	物联网认证与访问控制	69
3.6.1	电子 ID 身份识别技术	70
3.6.2	基于零知识证明的识别技术	72
3.7	物联网密钥管理机制	74
3.7.1	密钥管理流程	74
3.7.2	密钥管理系统	76
3.7.3	密钥管理技术	77
3.7.4	物联网密钥管理系统设计	78
3.8	物联网数据处理与隐私性	79
	习题三	80

第二部分 物联网感知知识层安全

第 4 章	RFID 系统安全与隐私	83
4.1	RFID 安全与隐私概述	83
4.1.1	RFID 基本组成架构	83
4.1.2	RFID 的安全和攻击模式	85
4.1.3	RFID 系统通信模型	87
4.1.4	安全 RFID 系统的基本特征	89
4.2	RFID 技术中的隐私问题及保护措施	91
4.2.1	位置隐私	91
4.2.2	信息隐私	91
4.2.3	隐私保护	92
4.3	产品电子代码的密码机制与安全协议	92
4.3.1	基于 RFID 技术的 EPC 系统安全问题	93
4.3.2	EPC global 系统安全分析	94
4.3.3	实现 RFID 安全性机制与安全协议	96
4.4	RFID 标签安全设置	99
4.4.1	RFID 电子标签的安全属性	99
4.4.2	RFID 电子标签在应用中的安全设计	100
4.4.3	第二代的 RFID 标准强化的安全功能	101
4.5	RFID 系统面临的攻击手段、技术及其防范	102
4.5.1	RFID 系统面临的攻击手段	102
4.5.2	RFID 芯片攻击技术	103

4.5.3	破坏性攻击及防范	103
4.5.4	非破坏性攻击及其防范	103
习题四	104
第5章	无线传感器网络安全	105
5.1	无线传感器网络安全概述	105
5.1.1	无线传感器网络安全问题	105
5.1.2	无线传感器网络的安全机制	107
5.1.3	无线传感器网络的安全分析	108
5.2	无线传感器网络的基本安全技术	111
5.2.1	安全框架与密钥分配	111
5.2.2	安全路由	112
5.2.3	入侵检测技术	112
5.3	无线传感器网络安全研究重点	113
5.3.1	无线传感器网络安全技术	113
5.3.2	密钥确立和管理	114
5.3.3	无线传感器网络的路由安全	116
5.3.4	数据融合安全	116
5.4	基于 ZigBee 技术的无线传感器网络的安全	117
5.4.1	ZigBee 技术分析	117
5.4.2	ZigBee 协议栈体系结构安全	119
5.4.3	安全密钥	121
5.4.4	ZigBee 网络结构	121
5.4.5	信任中心	122
5.4.6	存在问题及未来展望	124
习题五	124

第三部分 物联网网络构建层安全

第6章	无线通信网络安全	127
6.1	物联网信息传输	127
6.1.1	无线和有线的区别	127
6.1.2	安全连接的组成	127
6.1.3	设备局限性	128
6.2	无线网络的结构	128
6.3	无线网络的安全隐患	129
6.4	无线应用协议应用安全	131
6.4.1	WAP 协议	131

6.4.2	WAP 应用面临的安全威胁	132
6.4.3	WAP 的安全体系构架	132
6.4.4	WAP 应用模型存在的安全漏洞	133
6.4.5	端到端的安全模型	134
6.4.6	基于应用层的安全模型	135
6.5	无线网络的安全措施	135
6.6	无线局域网安全技术	136
6.6.1	无线局域网的开放性	136
6.6.2	无线局域网所面临的危险	137
6.6.3	无线局域网的安全技术	138
6.6.4	无线网络主流技术安全解决方案	141
6.7	蓝牙技术安全机制	143
6.7.1	蓝牙的安全结构	143
6.7.2	蓝牙的安全等级	144
6.7.3	蓝牙的密钥管理	145
6.7.4	蓝牙的鉴权方案	146
6.7.5	蓝牙的加密体系	146
6.7.6	蓝牙的安全局限	147
6.8	超宽带物联网信息安全策略	148
6.8.1	UWB 超宽带的优势	148
6.8.2	UWB 超宽带面临的信息安全威胁	149
6.8.3	超宽带安全性规范	150
6.8.4	超宽带拒绝服务攻击防御策略	152
6.9	物联网终端安全	153
6.9.1	物联网终端	153
6.9.2	物联网终端安全	156
	习题六	162
第 7 章	互联网网络安全	163
7.1	网络安全概述	163
7.1.1	网络安全威胁分析	164
7.1.2	网络安全服务的主要内容	165
7.1.3	Internet 安全隐患的主要体现	166
7.1.4	网络安全攻击的形式	166
7.1.5	网络安全案例	167
7.2	防火墙技术	168
7.2.1	防火墙的基本概念	168
7.2.2	防火墙的技术类别	169
7.2.3	防火墙的结构	170

7.2.4	防火墙产品选购策略和使用	173
7.3	入侵检测	174
7.3.1	入侵检测技术	174
7.3.2	入侵检测系统	175
7.3.3	入侵检测系统的工作步骤	176
7.3.4	入侵检测系统的典型代表	178
7.4	身份验证	178
7.4.1	身份验证的基本概念	178
7.4.2	访问控制和口令	179
7.5	IPSec 安全协议	181
7.5.1	IPSec 安全协议简介	181
7.5.2	IPSec 的协议组成和实现	181
7.5.3	IPSec 封装模式与算法	182
7.5.4	IPSec 虚拟隧道接口	184
7.5.5	因特网密钥交换协议	187
7.6	虚拟专网	189
7.6.1	虚拟专网技术基础	189
7.6.2	IPSec VPN	191
7.6.3	MPLS VPN 和 IPSec VPN 技术比较	195
7.6.4	虚拟专网需求及解决方案	197
7.7	黑客	200
7.7.1	网络黑客攻击方法	200
7.7.2	黑客常用的信息收集工具	202
7.7.3	黑客防范措施	203
7.8	互联网安全协议和机制	204
	习题七	207

第四部分 物联网管理服务层安全

第 8 章	中间件与云计算安全	211
8.1	中间件技术安全	211
8.1.1	中间件概述	211
8.1.2	中间件的体系框架与核心模块	212
8.1.3	中间件的分类	212
8.1.4	物联网中间件的设计	214
8.1.5	安全中间件	214
8.2	云计算安全概述	216
8.2.1	云计算简介	216

8.2.2	云计算系统的体系结构	218
8.2.3	云计算服务层次	220
8.2.4	云计算技术层次	224
8.2.5	云计算与云安全	225
8.2.6	云计算安全概述	226
8.2.7	物联网云计算安全	227
8.3	云计算核心技术及应用	228
8.3.1	云计算的核心技术	228
8.3.2	典型云计算平台	229
8.3.3	典型的云计算系统及应用	231
8.4	云计算应用安全体系与关键技术	232
8.4.1	云计算应用安全体系	232
8.4.2	云计算安全关键技术	235
8.5	云计算应用安全防护	236
8.5.1	云计算核心架构安全	237
8.5.2	云计算网络与系统安全	252
8.5.3	云计算数据与信息安全防护	256
8.5.4	云计算身份管理与安全审计	259
8.5.5	云计算应用安全策略部署	262
8.6	云安全技术解决方案	263
	习题八	266

第五部分 物联网综合应用层安全

第9章	信息隐藏技术原理	269
9.1	信息隐藏技术概述	269
9.1.1	信息隐藏概述	269
9.1.2	信息隐藏技术和传统的密码技术的区别	272
9.1.3	信息加密和隐藏的3种模式	273
9.1.4	信息隐藏的分类	274
9.2	信息隐藏技术原理	275
9.2.1	信息隐藏技术的组成	275
9.2.2	信息隐藏技术的分类、基本模型和关键技术	277
9.3	匿名通信技术	279
9.4	数据隐写术	280
9.4.1	替换系统	281
9.4.2	变换域技术	283

9.4.3	对隐写术的攻击	284
9.5	隐蔽信道	284
9.6	版权标志和数字水印	288
9.6.1	数字水印的特点	288
9.6.2	数字水印的主要应用领域	290
9.6.3	数字水印的分类	295
9.6.4	数字水印系统组成及其模型	296
9.6.5	数字水印系统的基本原理	297
9.6.6	数字水印算法	298
9.6.7	数字水印攻击分析	299
9.7	信息隐藏技术的研究	300
	习题九	301
第 10 章	位置信息与隐私保护	302
10.1	位置服务	302
10.1.1	位置服务的定义	302
10.1.2	位置服务的发展历史	303
10.1.3	位置服务的应用类型	303
10.1.4	位置服务在我国的应用情况	306
10.2	位置服务技术原理	307
10.2.1	LBS 系统组成	307
10.2.2	LBS 系统工作的主要流程	308
10.3	地理信息系统	308
10.3.1	移动 GIS	309
10.3.2	定位技术	310
10.4	隐私保护	312
10.4.1	隐私的定义	312
10.4.2	网络隐私权	313
10.4.3	侵犯网络隐私权的主要现象	314
10.4.4	侵犯网络隐私权的主要技术手段	314
10.4.5	网络隐私权的相关法律保护	316
10.4.6	隐私保护技术	316
10.5	基于位置服务的隐私保护	318
10.5.1	隐私保护问题	318
10.5.2	隐私保护方法	319
10.5.3	隐私保护系统结构	321
10.5.4	隐私保护研究内容	322
10.5.5	隐私保护技术面临的挑战	325

习题十 326

第六部分 物联网安全标准和安全体系规划设计

第 11 章 物联网信息安全标准	329
11.1 国际信息技术标准化组织.....	329
11.1.1 国际信息安全标准化组织	329
11.1.2 国际信息安全管理体​​系	330
11.2 中国信息安全标准	332
11.2.1 中国信息安全标准化的现状	332
11.2.2 中国安全标准组织机构	332
11.2.3 中国信息安全标准体系研究特点	333
11.2.4 中国在信息安全管理标准方面采取的措施	333
11.3 中国国家物联网标准组织.....	334
11.3.1 电子标签国家标准工作组	335
11.3.2 传感器网络标准工作组	336
11.3.3 中国物联网标准联合工作组	337
11.3.4 泛在网技术工作委员会	338
11.4 信息安全管理体​​系	338
11.4.1 信息安全管理简介	338
11.4.2 信息安全管理体​​系标准发展历史	339
11.4.3 信息安全管理体​​系标准主要内容	340
11.4.4 信息安全管理体​​系认证	341
习题十一	342
第 12 章 安全体系结构规划与设计	343
12.1 物联网系统的安全	343
12.1.1 物联网安全尺度	343
12.1.2 物联网应用安全问题	343
12.1.3 物联网特有的信息安全挑战	343
12.2 物联网系统安全性分析	344
12.2.1 传统网络安全问题分析	344
12.2.2 物联网特有安全问题分析	344
12.3 物联网安全体系的目标与防护原则	346
12.3.1 安全目标	346
12.3.2 防护原则	346
12.4 物联网信息安全整体防护技术	347
12.4.1 安全体系结构	347

12.4.2 纵深防御体系	348
12.5 物联网整体防护实现技术	348
12.5.1 物联网安全技术框架	348
12.5.2 关键技术实现研究	350
习题十二	351
参考文献	353

第一部分 物联网安全概述

第 1 章 物联网安全需求分析

第 2 章 物联网安全技术框架

第 3 章 密码与身份认证技术

第 1 章 物联网安全需求分析

根据国际电信联盟的定义,物联网(Internet of Things, IOT)主要解决物品到物品(Thing to Thing, T2T)、人到物品(Human to Thing, H2T)、人到人(Human to Human, H2H)之间的互联。核心共性技术、网络与信息安全以及关键应用是当前的物联网研究的重点。

与其他传统网络相比,物联网感知节点大都部署在无人监控的场景中,具有能力脆弱、资源受限等特点,这些都导致很难直接将传统计算机网络的安全算法和协议应用于物联网。这使得物联网安全问题相对比较突出,并且将来当国家重要基础行业和社会关键服务领域(如电力、金融、交通和医疗等)重要社会功能的实现都依赖于物联网及感知型业务应用时,物联网安全问题必然上升到国家层面。

考虑到当前的物联网安全研究尚未形成体系,主要研究集中在单个技术,如感知前端技术(如 RFID、传感技术)和个体隐私保护等方面,下面首先给出物联网安全安全性与层次结构分析;随后对层次结构涉及的物联网关键技术以及安全问题进行分析和论述。

1.1 物联网安全性要求

1.1.1 物联网安全涉及范围

在未来的物联网之中,每一个物品都会被连接到一个全球统一的网络平台之上,并且这些物品又时刻地与其他物品之间进行着各式各样的交互行为,这无疑会给未来的物联网带来形式各异的安全性和保密性挑战。比如,物品之间可视性和相互交换数据过程中所带来的数据保密性、真实性以及完整性问题等。

要想让消费者全面地投入未来的物联网的怀抱,要想让用户充分体验未来的物联网所带来的巨大潜在优势,要想让未来物联网的参与者尽可能避免通用性网络基础平台所带来的各种安全性与隐私性风险,物联网就必须实现这样一种特殊的工作方式,可以简便而安全地完成各种用户控制行为,也就是要求未来的物联网的技术研究工作充分考虑安全性和隐私性等内容。

传统意义上的隐私是针对于“人”而言的。但是在物联网的环境中,人与物的隐私需要得到同等级位的保护,以防止未经授权的识别行为以及追踪行为的干扰。而且随着“物品”自动化能力以及自主智慧的不断增加,像物品的识别问题、物品的身份问题、物品的隐私问题以及物品在扮演的角色中的责任问题将成为我们重点考虑的内容。

同时,通过将海量的具有数据处理能力的“物品”置于一个全球统一的信息平台和全球通用的数据空间之中,未来的物联网将会给传统的分布式数据库技术带来翻天覆地的变化。在这样的背景下,现实世界中对于信息的兴趣将分布并且覆盖数以亿万计的“物品”,其中将