



智能电网 关键技术研究与应用丛书

智能电网的 安全与隐私

Security and Privacy
in Smart Grids

[美] 肖杨 (Yang Xiao) 主编 |
李祎斐 等译 |



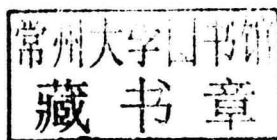
智能电网关键技术研究与应用丛书

智能电网的安全与隐私

Security and Privacy in Smart Grids

[美] 肖杨 (Yang Xiao) 主编

李祎斐 等译



机械工业出版社

Security and Privacy in Smart Grids/by Yang Xiao/ISBN: 978 - 1 - 4398 - 7783 - 8.

Copyright © 2014 by Taylor & Francis Group, LLC.

Authorized translation from English language edition published by CRC Press, part of Taylor & Francis Group LLC; All rights reserved; 本书原版由 Taylor & Francis 出版集团旗下, CRC 出版公司出版, 并经其授权翻译出版。版权所有, 侵权必究。

China Machine Press is authorized to publish and distribute exclusively the Chinese (Simplified Characters) language edition. This edition is authorized for sale throughout Mainland of China. No part of the publication may be reproduced or distributed by any means, or stored in a database or retrieval system, without the prior written permission of the publisher. 本书中文简体翻译版授权由机械工业出版社独家出版并限在中国大陆地区销售。未经出版者书面许可, 不得以任何方式复制或发行本书的任何部分。

Copies of this book sold without a Taylor & Francis sticker on the cover are unauthorized and illegal. 本书封面贴有 Taylor & Francis 公司防伪标签, 无标签者不得销售。

北京市版权局著作权合同登记 图字: 01 - 2013 - 8102 号

图书在版编目 (CIP) 数据

智能电网的安全与隐私/(美) 肖杨 (Yang Xiao) 主编; 李玮斐等译. —北京: 机械工业出版社, 2018. 5

(智能电网关键技术研究与应用丛书)

书名原文: Security and Privacy in Smart Grids

ISBN 978-7-111-59508-3

I. ①智… II. ①肖…②李… III. ①智能控制 - 电网 - 电力安全
IV. ①TM76

中国版本图书馆 CIP 数据核字 (2018) 第 059138 号

机械工业出版社 (北京市百万庄大街 22 号 邮政编码 100037)

策划编辑: 刘星宁 责任编辑: 刘星宁

责任校对: 王明欣 封面设计: 鞠 杨

责任印制: 李 飞

北京铭成印刷有限公司印刷

2018 年 5 月第 1 版第 1 次印刷

169mm × 239mm · 13.25 印张 · 253 千字

0 001 — 2 600 册

标准书号: ISBN 978 - 7 - 111 - 59508 - 3

定价: 79.00 元

凡购本书, 如有缺页、倒页、脱页, 由本社发行部调换

电话服务

网络服务

服务咨询热线: 010 - 88361066

机工官网: www.cmpbook.com

读者购书热线: 010 - 68326294

机工官博: weibo.com/cmp1952

010 - 88379203

金书网: www.golden-book.com

封面无防伪标均为盗版

教育服务网: www.cmpedu.com

译者序

智能电网是电网与现代信息通信技术融合发展形成的新型电网。随着智能电网技术和研究的不断发展，其安全与隐私问题越发凸显，直接影响到智能电网的正常运行和人们对智能电网的接受程度。因此，研究智能电网及其安全与隐私就变得非常重要。

《智能电网的安全与隐私》一书介绍了世界各地智能电网和相关领域著名研究人员的工作成果，提出了智能电网通信和安全的先进方法和创新技术。

本书介绍了电网安全开发和部署，并介绍了用于保证当今智能电网安全的创新方法。本书给出了智能电网基础设施的建议概述，描述了如何最大限度地降低数据中心的功耗和公用事业公司费用。它还包括以下内容：

- 1) 指出智能电网通信基础设施网络安全的挑战；
- 2) 涵盖与智能电网安全相关的法规和标准；
- 3) 介绍如何对变电站自动化系统进行漏洞评估；
- 4) 考虑智能电网自动化、SCADA 系统安全和“最后一英里”的智能电网安全。

本书为读者提供一个框架，用于保证这个不断发展的系统的安全性。本书涵盖直接攻击、智能电表和通过网络的攻击等内容，提供了可立即使用的可操作的建议，以防止这种攻击。

本书主要由李伟斐翻译，其他参加翻译的人员有汤奕、马辰智、边晓婕、张茹敏、韩凝、张通、张瑀彤、喻一伟、何淇彰、曹可凡、张鑫、吕晓薇、陈逍雨。本书内容所涵盖的领域非常宽广，限于译者的水平，加之时间仓促，书中难免会出现翻译不当甚至错误之处，恳请广大读者批评指正。

译者

原书前言

智能电网集成了电力传输系统与通信网络和信息技术 (IT)，以提供更好的服务。安全与隐私将在构建未来智能电网方面发挥重要作用。本书的目的是为智能电网提供最先进的方法和创新的的安全与隐私技术，并涵盖这些领域的一系列主题。

本书介绍了智能电网安全与隐私的基本原理和实际应用，涵盖世界各地智能电网和相关领域的许多著名研究人员的最新工作进展。本书包含 10 章内容，分为两个部分，第一部分为通用智能电网；第二部分为智能电网的安全与隐私。我们相信本书将为研究开发人员和与研究开发感兴趣的学生设计和部署智能电网安全与隐私提供一个很好的参考。

本书离不开参编者和出版社的巨大努力。感谢参编者，他们为了读者牺牲了白天和晚上的时间来整理这些章节。感谢出版商，没有他们的鼓励和质量的工作，这本书将无法完成。

肖杨

亚拉巴马大学计算机科学系

亚拉巴马州塔斯卡卢萨

电子邮件: yangxiao@ieee.org

致 谢

本书中的有关内容得到美国国家科学基金会 (NSF) 的授权 CCF - 0829827、CNS - 0716211、CNS - 0737325 和 CNS - 1059265 的支持。

关于主编



肖杨博士在 2002 年加入孟菲斯大学计算机科学系之前，曾担任美国电气电子工程师学会 (IEEE) 802.11 标准增强工作的 MAC (媒介访问控制) 架构师。目前是亚拉巴马大学计算机科学系教授。他是 2001 ~ 2004 年 IEEE 802.11 工作组的投票成员，也是 IEEE 高级会员。他是美国国家科学基金会 (NSF)、加拿大创新基金会 (CFI) 电信专家委员会和美国生物科学研究所 (AIBS) 的小组成员，还是许多国家和地区国际资助机构的裁判/评审员。他的研究领域是安全、通信/网络、机器人和远程医疗。他发表了 200 多篇期刊文章、200 多篇评审会议论文，并出版了一些学术

专著。他的研究得到美国 NSF、全球网络创新环境 (GENI)、圣地亚哥舰队工业供应中心 (FISCSD) 和亚拉巴马大学研究资助委员会的支持。他目前担任国际安全与网络杂志 (IJSN) 和国际传感器网络杂志 (IJSNet) 的主编，也是国际远程医疗和应用杂志 (IJTA) (2007 ~ 2009) 的创始人之一。

贡献者名单

Petra Been ken

能源部奥登堡办事处研发部门
德国奥登堡

Robert Bleiker

能源部奥登堡办事处研发部门
德国奥登堡

Sumit Kumar Bose

Unisys 公司云工程全球技术中心
德国奥登堡

Scott Brock

Unisys 公司云工程全球技术中心
德国奥登堡

Zhe Chen

田纳西理工大学
田纳西州库克维尔

Xihua Dong

Marvell 半导体公司
加利福尼亚州圣克拉拉

Steffen Fries

西门子公司技术部门
德国慕尼黑

José González

能源部奥登堡办事处研发部门
德国奥登堡

Manimaran Govindarasu

爱荷华州立大学电气与计算机工程系
爱荷华州

Nan Guo

田纳西理工大学
田纳西州库克维尔

Adam Hahn

爱荷华州立大学电气与计算机工程系
爱荷华州

Clark Hochgraf

罗切斯特理工学院
纽约州罗切斯特

Hans – Joachim Hof

慕尼黑应用科技大学计算机科学与数学系
德国慕尼黑

Shujie Hou

田纳西理工大学
田纳西州库克维尔

Rose Qingyang Hu

犹他州立大学电气与计算机工程系
犹他州

Zhen Hu

田纳西理工大学
田纳西州库克维尔

Abiodun Iwayemi

伊利诺斯理工大学电气与计算机工程系
伊利诺伊州芝加哥



Zhao Li

ABB 公司美国研究中心工业软件系统部
北卡罗来纳州罗利

Chen - Ching Liu

华盛顿州立大学电气工程与计算机科学
系, 华盛顿普尔曼
柏林大学机械与材料工程系, 爱尔兰都柏林

Sumita Mishra

罗切斯特理工学院
纽约州罗切斯特

Tae Oh

罗切斯特理工学院
纽约州罗切斯特

Yi Qian

内布拉斯加大学林肯分校计算机与电子
工程系
内华达州奥马哈

Robert Qiu

田纳西理工大学
田纳西州库克维尔

Marbin Pazos - Revilla

田纳西理工大学
田纳西州库克维尔

Raghuram Ranganathan

田纳西理工大学
田纳西州库克维尔

Sebastian Rohjans

能源部奥登堡办事处研发部门
德国奥登堡

Michael Salsburg

Unisys 公司云工程全球技术中心
德国奥登堡

Ronald Skeoch

Unisys 公司云工程全球技术中心
德国奥登堡

Michael Specht

能源部奥登堡办事处研发部门
德国奥登堡

Joern Trefke

能源部奥登堡办事处研发部门
德国奥登堡

Mathias Usler

能源部奥登堡办事处研发部门
德国奥登堡

Yongge Wang

北卡罗来纳大学夏洛特分校软件与信息
系统系
北卡罗来纳州夏洛特

Zhenyuan Wang

ABB 公司美国研究中心电网自动化部
北卡罗来纳州罗利

Fang Yang

ABB 公司美国研究中心电网自动化部
北卡罗来纳州罗利

Yanzhu Ye

田纳西大学电气工程与计算机科学系
田纳西州诺克斯维尔

Peizhong Yi

伊利诺斯理工大学电气与计算机工程系
伊利诺伊州芝加哥

Chi Zhou

伊利诺斯理工大学电气与计算机工程系
伊利诺伊州芝加哥

本书涵盖了世界各地智能电网和相关领域著名研究人员的工作成果，介绍了智能电网及其安全与隐私的基本原理和应用情况，汇集了这些领域最新的进展。

本书分为两个部分，即通用智能电网以及智能电网的安全与隐私。本书介绍了电网安全开发和部署，提出了智能电网通信和安全的先进方法和创新技术，并涵盖这些领域的一系列主题。

本书适合智能电网研究人员、从业人员和高等院校相关专业学生阅读。

目 录

译者序	
原书前言	
致谢	
关于主编	
贡献者名单	

第一部分 通用智能电网

第1章 智能电网基础设施建议概述	3
1.1 概述	3
1.2 IEC TC 57 参考架构概述	4
1.2.1 标准化简介	4
1.2.2 参考架构的主要结构	4
1.2.3 当前 TC 57 参考架构的结构	5
1.2.4 无缝集成的未来愿景	7
1.2.5 业务合作伙伴和应用的集成	7
1.2.5.1 IEC 61970: 能源管理系统应用程序接口	8
1.2.5.2 IEC 61968: 电力公用事业公司应用集成 - 配电管理 系统接口	9
1.2.5.3 IEC 62325: 能源市场通信框架	9
1.2.5.4 IEC 通用信息模型	10
1.2.5.5 组件接口规范	12
1.2.5.6 接口参考模型	13
1.2.6 能源系统的集成	14
1.2.6.1 收入电表	15
1.2.6.2 智能电子设备、继电器、电表、开关设备、电流 互感器、电压互感器	18
1.2.6.3 分布式能源和电表	23
1.2.6.4 其他控制中心	24
1.2.7 安全 和数据管理	26
1.2.7.1 通过 IEC 62351 - 3 安全通信	26
1.2.7.2 通过 IEC 62351 - 4 安全配置文件	27
1.2.7.3 IEC 62351 - 5 的认证技术	28



1.2.7.4 IEC 62351-6 的协议数据单元安全扩展	29
1.2.7.5 IEC 62351-7 的入侵检测	29
1.3 无缝集成架构的应用	30
1.4 小结与展望	33
参考文献	33
第2章 智能电网和云计算：最大限度地降低数据中心的功耗和公用事业公司支出	39
2.1 概述	39
2.2 服务级协议	40
2.3 云计算中虚拟机镜像的迁移	41
2.3.1 数据迁移	41
2.3.2 网络迁移	42
2.4 架构	43
2.4.1 应用管理器	43
2.4.2 站点代理	45
2.4.3 混合云代理	45
2.5 解决方案	45
2.5.1 应用管理器	45
2.5.2 站点代理	47
2.5.3 混合云代理	49
2.6 智能电表和智能负载	50
2.6.1 数据中心智能电网	50
2.6.2 数据中心中的智能设备	51
2.7 小结	52
参考文献	53
参考书目	54
第3章 建立负载控制的分配机会调度	55
3.1 概述	55
3.2 请求响应	56
3.2.1 电价	56
3.2.2 请求响应	57
3.2.3 DR 优点	57
3.2.4 DR 指南	57
3.3 最佳停止规则	57
3.4 问题陈述	58
3.5 模拟与结果	60
3.6 讨论	62
3.6.1 价格信号模型	62
3.6.1.1 价格信号的随机模型	62



3.6.1.2 基于用电的电价	63
3.6.2 公平	63
3.7 小结	63
致谢	63
参考文献	64
第4章 高级量测体系 (AMI) 及其与配电管理系统 (DMS) 的集成	65
4.1 概述	65
4.2 AMI	66
4.2.1 AMI 电表系统	66
4.2.2 AMI 通信网络	68
4.2.2.1 分层 AMI 通信网络	68
4.2.2.2 基于互联网协议的网状 AMI 通信网络	69
4.2.3 电表数据管理系统	70
4.3 标准化 AMI	70
4.3.1 标准 AMI 通信协议	71
4.3.1.1 ANSI C12.22	71
4.3.1.2 IEC 62056	73
4.3.2 标准 AMI 信息模型	74
4.3.2.1 ANSI C12.19-2008	75
4.3.2.2 IEC 62056-62	75
4.4 AMI 和 DMS 集成	77
4.4.1 DMS 中的电表数据模型	77
4.4.1.1 IEC 61968-9: CIM 中的电表模型	77
4.4.1.2 多重会话	78
4.4.1.3 通用电表模型与电力系统、特定领域电表模型的比较	78
4.4.2 AMI 和 DMS 集成	79
4.4.2.1 业务注意事项	79
4.4.2.2 AMI 和 DMS 集成的挑战	80
4.5 电表数据集成 (MDI) 层: AMI 和 DMS 集成的统一解决方案	80
4.5.1 MDI 层的背景	80
4.5.2 MDI 层的软件架构	80
4.5.2.1 MDI 层的组件	81
4.5.2.2 MDI 层的行为	82
4.5.3 MDI 架构评估	83
4.5.3.1 策略	83
4.5.3.2 测试结果与讨论	85
4.6 小结	85
致谢	86
参考文献	86



第5章 智能电网认知无线网络	89
5.1 概述	89
5.1.1 认知无线电	89
5.1.2 IEEE 802.22 系统	90
5.1.2.1 系统拓扑	90
5.1.2.2 服务范围	90
5.1.2.3 系统容量	90
5.2 智能电网认知无线网络	92
5.2.1 认知无线网络测试平台：认知无线电网的硬件平台	92
5.2.1.1 通用软件无线电外设2	93
5.2.1.2 小型封装软件无线电发展平台	94
5.2.1.3 无线开放访问研究平台	94
5.2.1.4 微软研究院软件无线电	95
5.3 认知无线网络和智能电网创新测试平台	96
5.3.1 新硬件平台的主板	96
5.3.2 建立网络测试平台节点的功能架构	97
5.3.3 创新网络测试平台	98
5.4 智能电网的认知算法	99
5.4.1 认知无线网络中的降维和高维数据处理	99
5.4.1.1 降维方法	99
5.4.1.2 使用具有实验认证的降维和支持向量机进行频谱监测	100
5.4.2 稳健的主成分分析	102
5.4.3 在强宽带干扰的情况下，用于恢复智能电表无线传输的 具有稳健的PCA预处理的独立分量分析	106
5.4.3.1 独立分量分析信号模型和接收机框图	106
5.4.4 使用稳健的PCA-ICA方法的模拟结果	109
5.5 智能电网中的安全通信	110
5.5.1 通信基础设施的开发	111
5.5.2 智能电网基于FPGA的模糊逻辑入侵检测	112
5.6 小结	113
参考文献	113

第二部分 智能电网的安全与隐私

第6章 智能电网通信基础设施网络安全的要求和挑战	123
6.1 概述	123
6.1.1 背景	123
6.1.2 高级要求	125
6.2 漏洞和安全要求	126
6.2.1 隐私	126



6.2.2 可用性	127
6.2.3 完整性	127
6.2.4 认证	128
6.2.5 授权	128
6.2.6 可审计性	128
6.2.7 不可否认性	128
6.2.8 第三方保护	128
6.2.9 信任	128
6.3 网络安全挑战	129
6.3.1 网络互联	129
6.3.2 安全策略和运营	129
6.3.3 安全服务	130
6.4 小结	130
参考文献	131
第7章 有关智能电网安全的规定和标准	134
7.1 概述	134
7.2 标准化	134
7.2.1 国际标准化组织 (ISO) / 国际电工委员会 (IEC)	134
7.2.2 ISO/IEC 27000 系列	134
7.2.3 IEC 智能电网战略组	135
7.2.4 ISO/IEC 62351-1 ~ 11	135
7.2.5 ISO/IEC 62443	138
7.2.6 国际自动化学会	138
7.2.7 电气与电子工程师学会	138
7.2.8 国际大型电子系统理事会	138
7.2.9 电力系统信息系统和内联网安全	138
7.2.10 电力公用事业公司信息安全治理	139
7.2.11 北美电力可靠性公司	139
7.2.12 互联网工程工作组	140
7.3 国家规定	140
7.3.1 美国国家标准与技术研究所 (NIST)	140
7.3.2 特刊 800-53	141
7.3.3 特刊 800-82	141
7.3.4 特刊 1108	141
7.3.5 NIST IR 7628	141
7.3.6 美国国土安全部	141
7.3.7 德国能源供应商联合会	141
7.3.8 欧盟工作组智能电网	141
7.3.9 欧洲智能电网协调组的结果	142



7.4 小结	143
参考文献	144
第8章 变电站自动化系统漏洞评估	147
8.1 概述	147
8.2 评估方法	148
8.2.1 规划	149
8.2.1.1 控制中心	149
8.2.1.2 变电站	149
8.2.1.3 网络协议概述	150
8.2.1.4 支持协议	151
8.2.2 检查技术	151
8.2.2.1 系统配置检查	151
8.2.2.2 网络配置/规则集	151
8.2.2.3 网络传播评估	152
8.2.3 目标识别与分析	152
8.2.3.1 网络发现	153
8.2.3.2 漏洞扫描	153
8.2.4 目标漏洞验证	153
8.2.5 后期处理	154
8.3 实践状态检查	154
8.4 小结	155
参考文献	156
第9章 智能电网、自动化和 SCADA 系统安全	158
9.1 能源网络、SCADA：高级介绍	158
9.2 能源系统和自动化系统的最新攻击和事故	159
9.3 SCADA 安全	161
9.3.1 对 SCADA 系统的威胁	163
9.3.2 安全的 SCADA 远程连接	164
9.3.3 sSCADA 协议套件	165
9.3.4 计数器同步	168
9.4 小结	168
参考文献	169
第10章 智能电网安全最后一英里	172
10.1 概述	172
10.2 最后一英里智能电网系统架构	172
10.3 控制系统：智能电网对电力系统稳定性的影响	173
10.4 安全和隐私规划	173
10.5 现场网络/邻域网络中的安全威胁	174
10.5.1 物理层攻击	174



10.5.2	链路层攻击	174
10.5.3	网络层攻击	175
10.5.4	互联网协议寻址特定攻击	175
10.5.5	传输层攻击	175
10.5.6	应用层攻击	175
10.5.7	其他突出的安全威胁	176
10.5.7.1	后台管理系统威胁	176
10.5.7.2	电网不稳定性	176
10.5.7.3	安全性差异	176
10.6	AMI 系统的安全性: AMI 问题和当前的缺陷	176
10.6.1	AMI 组件	176
10.6.2	AMI 组件中的安全问题	176
10.6.2.1	AMI 系统的保密性	176
10.6.2.2	AMI 系统的完整性	177
10.6.2.3	AMI 系统的可用性	177
10.6.2.4	AMI 系统的不可否认性	177
10.6.2.5	AMI 系统授权	177
10.6.3	当前 AMI 系统的主要漏洞	177
10.6.3.1	明文 NAN 流量	177
10.6.3.2	总线监听	178
10.6.3.3	错误的加密	178
10.6.3.4	直接篡改	178
10.6.3.5	电表认证缺陷	178
10.6.3.6	拒绝服务威胁	178
10.6.3.7	存储的密钥和密码	178
10.6.3.8	加密密钥分配	179
10.7	采用传感器网络技术解决智能电网的加密和密钥管理需求	179
10.7.1	数据加密	179
10.7.2	密钥建立和管理	180
10.7.3	链路层安全框架	181
10.8	小结与展望	181
	参考文献	181
	推荐阅读	184
	附录 缩略语表	186