国防科技著作精品译丛
网电空间安全系列

ELSEVIER
爱思唯尔

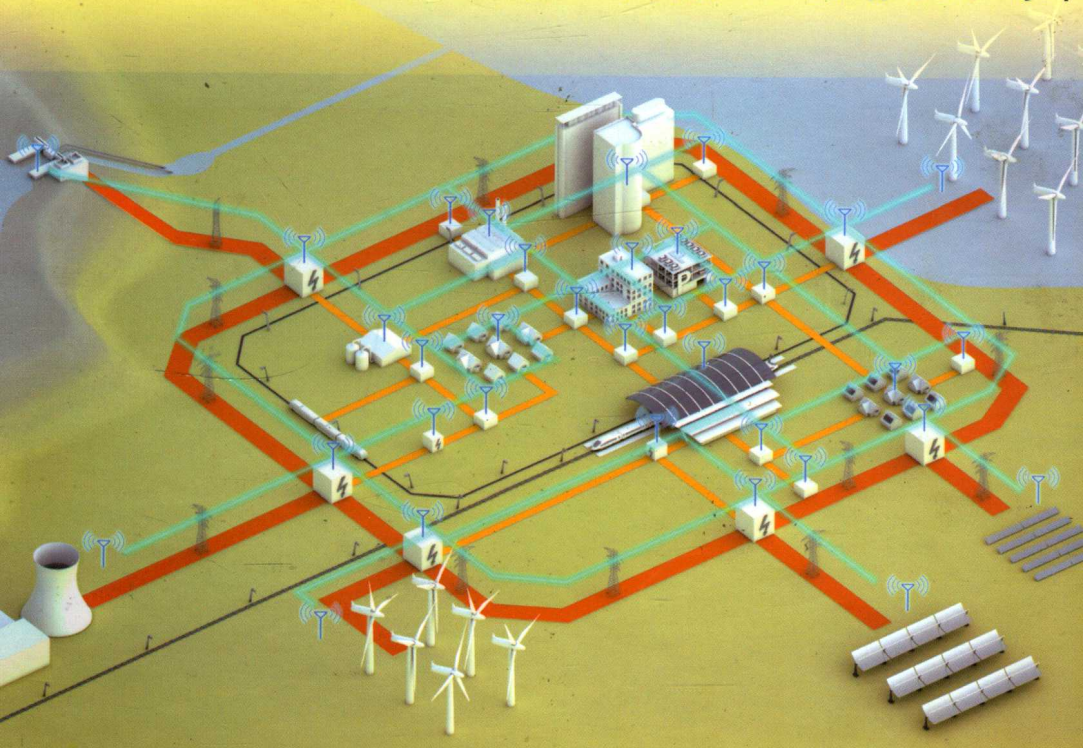
Applied Cyber Security and the Smart Grid

Implementing Security Controls into the Modern Power Infrastructure

应用网络安全与智能电网

——现代电力基础设施的安全控制

【英】Eric D.Knapp Raj.Samani 著　宁文元 王 刚 徐小天 等译



国防工业出版社
National Defense Industry Press

应用网络安全与智能电网
——现代电力基础设施的安全控制

Applied Cyber Security and the Smart Grid: Implementing Security Controls into the Modern Power Infrastructure

[英] Eric D. Knapp　Raj Samani　著
宁文元　王　刚　徐小天　等译

国防工业出版社
National Defense Industry Press

著作权合同登记　图字: 军 -2014 -039 号

图书在版编目（CIP）数据

应用网络安全与智能电网: 现代电力基础设施的安全控制/（英）克纳普（Knapp, E. D.），（英）萨玛尼（Samani, R.）著; 宁文元等译. -- 北京: 国防工业出版社, 2015.5
（国防科技著作精品译丛. 网电空间安全系列）
书名原文: Applied Cyber Security and the Smart Grid: Implementing Security Controls into the Modern Power Infrastructure
ISBN 978-7-118-10202-4

Ⅰ. ①应… Ⅱ. ①克… ②萨… ③宁… Ⅲ. ①智能控制—电网—安全 Ⅳ. ①TM76

中国版本图书馆 CIP 数据核字（2015）第 108824 号

应用网络安全与智能电网——现代电力基础设施的安全控制
[英]　Eric D. Knapp　Raj Samani　著
宁文元　王　刚　徐小天　等译

出版发行　国防工业出版社
地址邮编　北京市海淀区紫竹院南路 23 号　100048
经　　售　新华书店
印　　刷　北京嘉恒彩色印刷有限责任公司
开　　本　700 × 1000　1/16
印　　张　14¼
字　　数　223 千字
版 印 次　2015 年 5 月第 1 版第 1 次印刷
印　　数　1—2500 册
定　　价　69.00 元

(本书如有印装错误，我社负责调换)
国防书店: (010) 88540777　发行邮购: (010) 88540776
发行传真: (010) 88540755　发行业务: (010) 88540717

翻译组名单

宁文元　王　刚　杜秋平

徐小天　徐伟婷　陈乐然

陈　威　石　磊　王晨晨

李　敏

译者序

智能电网技术是当前全球电力工业发展的焦点，随着其技术水平和普及程度的不断提升，更多新兴的安全问题也逐渐浮出水面。现代智能电网基础设施中普遍采用 SCADA、DCS、PLC 等现代工业控制系统以及更多的通用网络设备，在快速推动电网智能化的同时，也使得电网工控系统呈现出开放化的趋势，面临更严峻的安全挑战。

自 2010 年 10 月首个针对工控系统的病毒在伊朗爆发以来，现代电力工业的系统和网络无时无刻不在承受着层出不穷的安全威胁。然而纵观全球电力行业，智能电网的网络安全防护措施相比于其面临的风险而言，还处于较为落后的状态。传统电力系统的设备专有性和天然的隔离性使得其安全隐患 (尤其是网络安全隐患) 被长期忽视，企业更倾向于将精力投入到设备安全和生产安全之上，以保障电力生产的正常运行。然而在智能电网的环境下，其高度的网络互联和设备智能化程度已经在一定程度上打破了原有的天然隔离，网络安全已经不可避免地成为智能电网安全的重要组成部分。

《应用网络安全与智能电网》一书即出自这样的背景之下。本书从智能电网的概念入手，建立了典型智能电网的架构模型；之后针对建立的模型，对智能电网架构中各个环节面临的网络安全风险进行介绍，并给出了相应的安全防护建议。本书结合网络安全的当前形势，讨论了隐私安全、供应链安全等新兴的网络安全话题，并对智能电网网络安全的未来进行了展望。通过借鉴本书建立的智能电网模型和工控安全模型，智能电网从业人员可以以此为基础并结合实际情况，实施相应的网络安全防护措施。

本书的作者 Eric D.Knapp 是世界工控系统网络安全领域的专家，致力于研究 SCADA、ICS 等工业自动化设备和系统的安全防护技术，以及企业和工业网络安全技术等，曾撰写《工业网络安全——智能电网、SCADA 和其他工业控制系统等关键基础设施的网络安全》等著作。另一位作者 Raj Samani 身为知名安全厂商 McAfee 的副总裁，致力于信息安全技术的研究，并热衷于进行企业信息安全理念的推广。作者旨在通过本书，对智能电网网络安全的理念进行教育和宣传，激发阅读本书的广大智能电网和相关领域从业人员的思考，建立智能电网网络安全保障相关技术的研究基础。

本书的翻译工作得到国防工业出版社的大力支持，在此表示衷心的感谢。由于翻译时间及译者水平的限制，本书可能存在错误和不当之处，敬请各位读者批评指正。

信息技术研究所
华北电力科学研究院有限责任公司
2015 年 4 月

致谢

《应用网络安全与智能电网》一书得以问世，我们要感谢所有给予我们帮助的人，尤其要感谢我们的家人，在我们长达数月的研究和写作中，包括我们深夜和清晨的越洋通话，一路来给予的理解和精神支持。同时在这里也要感谢 Syngress 出版社的 Ben Rearick、Chris Katsaropoulos 及其各位同仁，使我们得以完成另一本关于智能电网网络安全的书。还要感谢技术编辑 Joel Langill，正是由于他无私真诚的帮助，保证了本书技术内容的准确性。最后我们要感谢 Jennifer Byrne 对本书提出的宝贵意见以及给予的支持。

我们还要感谢网络安全协会 (SANS Institute) 在人们熟知 SCADA 和 ICS 之前所做的推广工作。感谢 ICS 联合工作组在工业界宣传和提高工业控制系统安全方面所做出的不懈努力。感谢美国国家标准及技术研究所 (NIST) 和欧盟智能电网协调组对错综复杂的智能电网进行的恰如其分地梳理。感谢各有关组织的辛勤工作，对智能电网网络安全的最佳做法和实施标准进行统计和记录。对大家的辛勤工作和付出，我们十分感激，谨在此表示我们最诚挚的谢意和敬意。

作者简介

Eric D. Knapp 是全球公认的工业控制系统网络安全专家, 一贯致力于推动和引进新型安全技术, 确保自动化基础设施更安全可靠。他最初在安全技术公司 Nitro Security 供职, 负责工业控制网络安全, 侧重 SCADA 和 ICS 数据收集和关联性, 监测在这些环境中存在的高级威胁。此后, 他供职 McAfee 公司, 是关键基础设施市场的全球总监, 负责端到端 ICS 网络安全解决方案的开发和实施。目前, 他任职于 Wurldtech 安全技术公司, 担任战略联盟部主任, 继续推动嵌入式安全技术的发展, 为 SCADA、ICS 及其相关的实时设备提供更好的服务。

他长期致力于倡导改善工业控制系统网络安全, 参与许多重要的基础设施行业组织, 拥有丰富的专业技术知识, 有 20 多年的信息技术从业经验, 专攻工业自动化技术、基础设施安全、应用以太网协议、企业和工业网络入侵防御系统, 以及安全信息和事件管理系统的设计与实施。除从事信息安全工作外, 他还获得过小说作家奖。他就读的学校是新罕布什尔州大学和伦敦大学。

他在社交网络推特的地址是: Twitter @ericdknapp

Raj Samani 是信息安全界的活跃份子。他参与了很多旨在提高企业和社会对安全应用认知度的活动。目前他是 McAfee 副总裁, 欧洲、中东和非洲局 (EMEA) 首席技术总监。之前他曾在一家英国的大型公共部门担任首席信息安全官, 最近他的名字进入了 2012 年欧洲信息安全名人堂。

此前, 他曾供职于欧洲的多家公共部门, 以及许多网络安全和研究工作组。其中包括 MiData 互操作性董事会; 他在欧盟成立的负责智能电网

标准的智能电网参考组织中担任数字欧洲 (DIGITALEUROPE) 的代表。

目前, 他在 McAfee 公司的欧洲、中东和非洲局担任云安全联盟战略顾问, 之前是信息系统安全联合会 (ISSA) 英国分会主管通信的副总裁, 主持了 2008 年和 2009 年年度分会通信奖活动。他还是欧洲信息安全、信息安全杂志顾问委员会成员, 是 searchsecurity.co.uk 和信息安全门户网站的专家和电脑周刊专栏作家。他发表了多篇关于安全的论文, 还应邀参加 ITV 和 More 4 电视节目, 发表关于计算机安全方面的意见。他对 2006 年的 RSA 无线安全调查提供了帮助, 是 RIPA 议案 (第 3 部分) 咨询委员会成员之一。

除了日常工作, 他取得的其他成绩或荣誉如下:

CESG 认证咨询项目 (CLAS), 认证信息系统安全专家 (CISSP), 认证道德黑客 (CEH), 微软认证系统工程师 (MCSE-NT4, Win2K, Win2003), CCSA 管理员 (CCSA 的 NG 和 4.1), CCSE 专家 (CCSE–NG), Citrix 认证管理员 (CCA), QualysGuard 认证, RSA 认证系统工程师 (SecurID), 思科认证网络管理员 (CCNA)。他拥有 (荣誉) 文学学士和理学硕士双学位。

他在社交网络推特的地址是: Twitter @ Raj_Samani

技术编辑介绍

Joel Langill 在工业自动化和控制行业工作了 30 多年, 通过深入全面的架构设计以及产品开发、实施、系统迁移等多个岗位的工作, 积累了丰富的经验, 熟知大多数的工业领域。他在国际上从事过工业控制系统的新建和扩建工作, 对工业控制系统部署和维护面临的相关网络威胁和风险有着自己独特和不可多得的见解。

他现在是一名独立咨询专家, 主要帮助客户进行自动化系统评估和维护, 避免来自企业内部和外部的网络威胁。他创立并负责维护著名的安全网站 SCADAhacker.com, 为访问网站的客户提供丰富的信息资源, 帮助他们了解、评估和掌控安全控制系统。他还开发了结合安全意识、标准化实践、工业领先技术和针对控制系统架构的定制化方法在内的专业化培训课程, 旨在理解控制系统并使其免受网络风险的威胁。

他独特的经验和公认的工作能力, 使其与几大工业企业建立了紧密的业务联系, 如 Gartner、卡巴斯基实验室、McAfee、西门子、多芬诺安全以及 Waterfall 安全解决方案公司。他还抽出时间, 从事控制系统安全自主研发, 并在博客中经常发表控制系统评估与安全的文章。

他是在工业安全控制系统 ISA99 委员会中有投票权的成员, 是 ISA99 Stuxnet 恶意软件技术报告的主要成员。同时是关键基础设施公司的主任, 也是 SCADA 网络安全论坛活动的代表。他获得的认证包括: 道德黑客认证 (CEH), 入侵测试员认证 (CPT), 注册 SCADA 安全体系认证 (CSSA) 和 TÜV 功能安全工程师 (FSEng)。他还在美国国土安全部联邦紧急措施

署应急管理学院接受了全面的培训，完成了 ICS-400 关于意外事件指挥和危机管理培训。他毕业于伊利诺伊大学，拥有电气工程本科学位。

他在社交网络推特的地址是：Twitter @SCADAhacker

前言一

作为新近成立的欧洲网络犯罪中心 (EC3) 的负责人, 我很荣幸向大家推荐这本书, 一本具有重要意义的书。我在国际网络安全保护联盟董事会任职期间, 就结识了 Raj Samani 和许多资深的网络保护和网络安全领域专家以及利益相关者。Raj 长期以来凭借其超人的业绩, 对网络安全的辩论和工作产生了深刻的影响。他是一个有前瞻眼光的专家, 对网络安全这一复杂课题有令人敬佩的洞察力。

在过去的这些年中, 由于各种各样的原因, 包括好的和坏的, 导致网络保护被过度夸大。重要的是, 我们不能因此失去重点, 不能迷失方向。发展我们共享的网络空间会对人类做出巨大贡献, 如经济快速增长、透明性、共享、创新、发展和繁荣。这种贡献不会只造福世界的某个特定国家和地区, 而是可以惠及全世界。但像所有东西一样, 没有一样东西全是优点。金牌的背面也有人性黑暗的一面, 即罪犯、恐怖分子和独裁者。他们在网络新世界的发展过程中, 利用了网络世界的弱点。像现实世界那样, 在网络世界我们需要制定相应的法规、规章、准则并实施。

目前网络犯罪高发, 新网络威胁发展迅速, 因此需要我们相互分享现有的良好的相关知识和已实施的一些好的应对方法。为此, Samani 和 Eric Knapp 先生, 作为这一充满挑战的领域的专业人士, 共同撰写了本书。

我很坦然地推荐这样一本具前瞻性的好书, 并真诚地期望这两位优秀的专业人士能取得更大的成绩。他们两位间接地支持了我的工作, 帮助欧盟成员国实现安全、自由、开放和透明的互联网!

欧洲网络犯罪中心 (EC3) 主任

Troels Oerting

前言二

“公用事业单位的网络安全正处于混乱边缘”。

我这句话发表于 2011 年 11 月，带给了我非常不情愿接受的 15 分钟的名气。世界各国新闻媒体引用了我的这句话，并被翻译成了几种语言，经常被错误地引述为：“公用事业单位正处于混乱边缘”。这寥寥十几个字在谷歌上显示的警示作用，远远大于它们在我电脑上的效果。但这种表述方式非常精确。

从我上段话的发表到现在，公用事业单位网络安全的唯一变化，就是情况比以前还要糟糕。在对专家的采访中，他们告诉我，在过去的这些年中，网络安全领域几乎没有创新。有一家供应商坦白地说，“过去三年中，在每一次智能电网的安全会议上，我看到的是同一家供应商重复使用着相同的演讲稿子”。也有几家创新公司逆势而上，根据已有的专业知识，提出了一些新方法。但大多数的智能电网网络安全的产品只不过是用了一些华丽的辞藻，全套照搬了财务和医疗行业的安保做法。

同时，智能电网安全标准建设工作进展，也极其缓慢。一位业内人士甚至将那些标准化建设的各种会议比作毒药。原来只有少数的几个网络安全专家，到后来发展到数百个标准工作组会员。供应商参加这些会议的目的，是为了保护自己的地盘，公用事业单位则派遣律师参会，旨在对他们的承诺范围进行限制。因此，最后的唯一的成果是 NERC CIP 第 4 版的出台，大家对此就无需感到震惊。这个产品无非是在关键网络资产定义中添加了 16 个条款，而且从其概念设计到具体实施还将需要近 5 年的时间。尽管行业标准建设饱受诟病，但却是非常重要的。供应商告诉我说，如果没有标准，他们不知道该生产什么样的产品。同样，如果没有行业标准，公用事业单位也不知道该购买什么。但是，很多公用事业单位将自己企业的

安全定义为实施最低限度的行业标准，这离企业实现安全保护的目标还有很大差距。

总而言之，现阶段创新处于一种停滞状态，行业标准建设犹如在冰川上行走。我们必须让那些攻击电网安全的人不再相信他们的运气。当我们在争论不休、对技术进行投票决策之时，网络攻击者既不会遵守行业标准也不会遵守法律，相反他们开足马力在攻击的道路上前行。NERC CIP 第 5 版本主要针对当前的网络威胁而设计，预计可以在 Stuxnet 创建之后的 7 年之内进行实施。坐等标准的出台，来保护智能电网的策略，绝非上乘之策。

但是希望犹存。尽管前面的说法有些令人沮丧，但多数同行一致认为如今拥有足够的安全功能，保护智能电网。问题不在于产品缺失，缺失的是方法。由于从投资到安全保护，整个流程缺乏清晰的设计路线，因此用于安全保护的预算仍然无法敲定。尽管我从来没有见过一家公用事业单位反对安全保护，但我确实遇到了一些公用事业单位并不知道如何实现安全保护。决策者可能不知道一个安全架构到底该由哪些因素构成，但能感觉出别人呈现给他们的很多安全方案缺失了一些东西。

我们缺少的是如何利用现有的东西，来创建一个安全的智能电网。作为一名研究分析师，我的一部分工作职责是参加行业会议，并且是很多很多的行业会议。从规则的角度看，供应商赞助的会议是最有意义的，因为会议上的讨论几乎都是“应用”型的，可解决现实中存在的问题。从事实际操作的人对行业会议上那些理论性的东西是不感兴趣的。现实中的问题，需要使用现实的方法进行解决。印刷精美的小册子，就如同科幻故事，每件事每个人的故事都是完美无缺的。而在现实世界中，往往意味着“只要不是最坏的选择”便等于最好的选择。这也是网络安全的核心和保证电网安全的希望，这种希望不是来源于理论，而是采取真实可用的安全措施，解决现实世界中存在的问题。

企业的首要任务是把握重点。对于智能电表的长篇累牍的讨论，包括电表易于受到攻击，电表如何收集个人信息，以及电表对健康的潜在威胁(已被证明不对) 等，这些都不是网络攻击的主要目标。相反，最让人担心的攻击目标是输配电的管理控制系统。敌对国家和有组织的犯罪一直将目标锁定在能源供应，而不是能源需求。至于网络攻击者为什么将能源供应锁定为他们的攻击目标，原因可能有很多，但没有必要了解为什么，因为没有太大意义。与其了解攻击方的心理，莫不如充满信心，找出今后网络攻击的目标所在。

在各种网络攻击的记录中，智能电表始终是智能电网安全中最经常讨论到的话题，这其中的原因，可能是智能电表更易于理解和探讨。从定义上来说，智能电表就是现代 IT 设备，有众人皆知的计算和联网能力。相比之下，控制网络通常包括成千上万的设备，我们通常会善意地形容这类设备为珍贵的财产，实际上就是些陈旧且尚有很长的剩余服务寿命的东西。如何保护陈旧与现代设备并存的这样一种控制网络，其实就是现实社会中所说的智能电网安全工作。

综上所述，公用事业单位还得靠自己。在本书中，Raj 和 Eric 的直接受众是那些能保护电网安全的人们。在与电网安全相关的诸多事宜中，网络安全是可想象到的最平淡无奇的一个话题。网络安全存在于日常生活的每时每刻，是一场永不休止的资金大战，需要应对艰巨的技术挑战，需要制订精细的实施计划，计划的精细程度都超出了人们的想象能力。而所有这一切努力就是为了寻求一个安全保护解决方案。世上本就不存在绝对安全这种事情。真实世界中的安全，其实是在没有理想方案的情况下，不停地选择相对最适合的解决方案的一个过程。这是一项艰苦的工作，而且往往成功到来的时候，都是悄无声息。但过程却至关重要。

掌控电网者，掌控经济。每个公用事业单位都要发挥自己的作用，牢牢掌控网络安全。现在是行动的时候了。

Navigant Research 高级研究分析师

Robert P. Lockhart

目录