国防科技著作精品译丛
网电空间安全系列

ELSEVIER
爱思唯尔

Industrial Network Security

Securing Critical Infrastructure Networks for Smart Grid, SCADA, and Other Industrial Control Systems

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

【美】Eric D.Knapp 著　　周 秦　郭冰逸　贺惠民　等译

国防工业出版社
National Defense Industry Press

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

Industrial Network Security: Securing Critical Infrastructure Networks for Smart Grid, SCADA, and Other Industrial Control Systems

[美] Eric D. Knapp 著

技术编辑 James Broad

周 秦 郭冰逸 贺惠民

白 驹 王 刚 黄东东 译

国防工业出版社

National Defense Industry Press

著作权合同登记　图字: 军 -2013 -170 号

图书在版编目（CIP）数据

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/（美）纳普（Knapp, E. D.）著; 周秦等译. — 北京: 国防工业出版社, 2014. 6
（国防科技著作精品译丛. 网电空间安全系列）
书名原文: Industrial network security: securing critical infrastructure networks for smart grid, SCADA, and other industrial control systems
ISBN 978-7-118-09325-4

Ⅰ. ①工… Ⅱ. ①纳… ②周… Ⅲ. ①工业控制计算机—计算机网络—安全技术
Ⅳ. ①TP393. 08

中国版本图书馆 CIP 数据核字（2014）第 091022 号

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
[美] **Eric D. Knapp** 著
周　秦　郭冰逸　贺惠民　白　驹　王　刚　黄东东 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	21 ¼
字　　数	349 千字
版 印 次	2014 年 6 月第 1 版第 1 次印刷
印　　数	1—2500 册
定　　价	98.00 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

周　秦　郭冰逸　贺惠民　白　驹　王　刚　黄东东

郭雨轩　李广知　秦逸轩　毕晟煊　徐小天　石　磊

陈乐然　陈　威　王晨晨　李嘉言　杨蔚蓝　马天阳

庞浩然　张　笛　孔维绪　张卫锋　刘　石　谢　天

译者序

伴随着计算机和网络技术的发展, SCADA、DCS、PLC 等现代工业和控制系统在关键性基础设施和能源行业中日益广泛应用, 它极大地推动了工业生产, 但同时也使工业控制系统接口越来越开放, 控制系统面临的信息安全问题也日益严重。

2010 年 10 月, 肆虐伊朗的 "震网" (Stuxnet) 病毒造成伊朗布什尔核电站重大损失, 其专门针对西门子工业控制系统的明确目的性, 传播手段之高明, 造成结果之恶劣, 赢得了世界上首个网络 "超级武器" 的称号。之后, 又一恶性蠕虫 "毒区" (Duqu) 于 2011 年被发现, 其目的是收集与攻击目标有关的各种情报, 俨然一个工业间谍。2012 年 5 月, 设计更复杂、破坏力更大的超级病毒 —— "火焰" 被发现可能潜伏在目标系统中已长达 5 年。世界媒体一片惊呼: "工业病毒" 时代已经来临!

长期以来, 传统工业系统的设备专有性与天然隔离性使得人们忽视了信息安全隐患的存在, 企业管理者与工程师们往往将安全关注的焦点和资金预算都投放在设备安全和生产安全方面, 预防发生工业事故造成人员、财产、或环境损失。然而, 信息技术的发展已经打破了传统的 "物理隔离神话", 为确保国家能源和关键性基础设施行业控制系统的安全稳定运行, 研究工业网络安全的关键问题, 建立有针对性的安全防护体系已经迫在眉睫。

在这样的背景下,《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》一书尤显适应时代的需要, 该书作者 Eric Knapp 是一位长期从事 SCADA、工业控制网络、关键基础设施

等安全技术研究与公共安全策略部署的专家, 具有长达 20 年的信息安全领域工作经验。书中涵盖了从工业网络的基本概念到网络安全的具体实践建议的大量内容: 针对工业控制系统的网络攻击可能带来的潜在风险和后果; 对工业网络进行评估、保护和监控的详细方法; 工业网络的大量合规性约束, 及如何将这些特定的规则反向映射到网络安全实践中。值得注意的是本书不仅仅定位于提供一些安全建议, 更试图从机理上探求工业网络的安全防护方法, 同时兼顾通用的合规控制要求。

在编译本书的过程中, 涉及网络安全的事件不断出现, 针对工业控制系统的新攻击方法也层出不穷。美国极力强调来自网络空间的安全威胁, 大力加强网络空间技术发展, 不断提高网络空间作战能力, 近期又曝光了一项名为 “棱镜计划” (PRISM) 的绝密电子监听计划。该项目由美国国家安全局 (NSA) 和联邦调查局于 2007 年起开始实施, 正式名号为 “US-984XN”。包括微软、雅虎、谷歌、苹果等在内的9家国际网络巨头皆参与其中, 电信巨头威瑞森公司每天为其提交数百万用户的通话记录, 项目人员可直接进入美国网际网络公司的中心服务器里挖掘数据、收集情报, 内容涵盖电子邮件、聊天记录、视频、音频、照片、文件等上网信息, 可全面监控特定目标及相关人员的一举一动。该计划再次显示了美国在网络空间控制与利用上的勃勃雄心。工业网络作为网络空间的重要组成部分, 未来必将是各个国家网络空间安全的战略要地。

本书的编译工作, 得到了国防工业出版社的大力支持, 在此一并表示衷心的感谢!

由于时间仓促, 编译人员水平有限, 难免有错误和不当之处, 敬请批评指正。

2013 年 8 月

关于本书作者

Eric D. Knapp 是 NitroSecurity 公司关键基础设施市场部 (CIM) 的主管, 专门负责针对关键基础设施、SCADA 与工业控制网络方面新安全技术的识别、评估和实现。

Eric 在信息技术领域有着 20 年的从业经历, 特别是在工业自动化技术、基础设施安全、应用以太网协议以及企业网络与工业网络两者中的 IPS 和 SIEM 系统设计与实现方面, 具有很深的造诣。除了信息安全方面的工作, Eric 也是一位获奖颇丰的人。在新汉普郡 (Hampshire) 大学和伦敦大学期间, 他对英语语言和写作进行了深入学习与研究, 并且获得了通信方面的学位。

关于本书技术编辑

James Broadc (CISSP, C —— EH, C) PTS, Securityt, MBA) 是 Cyber-Recon 公司的主席和所有者, 他和他的顾问团队专门为企业和政府提供信息安全、信息确保、认证与鉴定及其他安全咨询服务。

作为具有 20 多年 IT 从业经历的安全专业人士, 在 IT 安全的许多领域, James 是一位专家, 特别是在安全工程、渗透测试、脆弱性分析和研究等方面具有较深的造诣。他为美国许多关键部门提供安全服务, 包括国防、法律实施/执法、情报、财政和医疗保健等部门。

James 在肯恩大学布兰查德商学院 (Ken Blanchard College of Business) 获得了 MBA/IT 学位, 在西南大学 (Southwestern University) 获得了计算机编程和安全管理的硕士学位, 目前正在卡佩拉大学 (Capella University) 攻读信息安全专业的博士学位。目前, 他是 ISSA (信息系统安全协会) 和 (ISC)$^{2®}$ (CISSP 管理者) 的会员。James 和他的家庭成员 (Deanne、Micheal 和 Temara) 现在居住于弗吉尼亚州 (Virginia) 的斯塔福德 (Stafford)。

序言

工业系统安全是信息安全中最神秘的领域之一，没有任何其他信息安全领域像它这样包含如此之多的误解和谎言。虽然网上有许多可用的甚至连篇累牍的信息，但是这反而只会给那些信息安全专业人士和工业系统专业人士带来更多的困惑和误解 —— 不仅浪费金钱，而且可能会导致致命的错误。

安全性在工业领域极其重要的地位使之显得更加神秘。商业秘密信息的泄露可能只是导致一笔生意的失败，但是发电能力的丧失，毁灭的可能就不仅仅是一个人，而是数以千计的人。

随着这本关于工业系统网络安全极具研究价值的著作的出版，这个疑团终于被解开了。

该书的一些部分深深吸引了我。我赞同该书讲述的“物理隔离神话”的破灭，如今，在无线通信时代，物理隔离不再当作也不应该认为是“绝对的安全”。我也赞同书中提到的 safety 和 security 两种安全的概念，工业领域的工程师们知道更多的可能是前者，而我的信息安全同事们了解更多的却是后者，如今互联的工业系统对两者绝对都需要！最后，我也赞同该书对风险和影响的关注，而不是简单地遵循最小需求。

信息安全工程师和工业工程师都能够从本书中获益，虽然他们从属于两个不同的领域。本书有望带来这两个领域所急需的大量融合，从而有助于我们构建一个更安全的业务和工业系统。

Dr. Anton A. Chuvakin

安全卫士顾问

目录