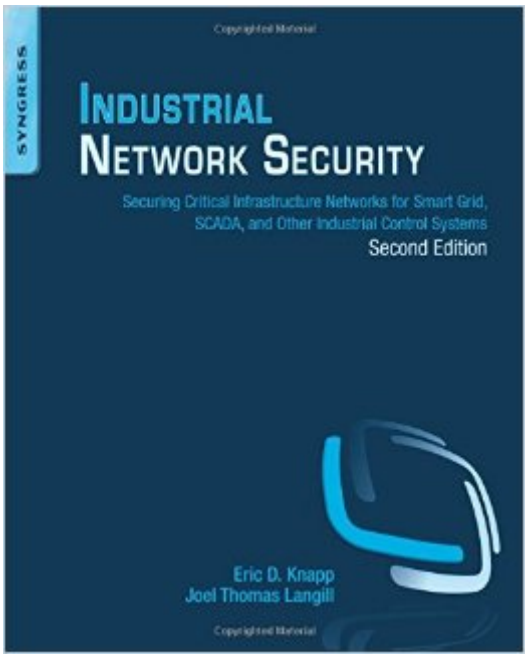
Industrial Network Security, Second Edition: Securing Critical Infrastructure Networks For Smart Grid, SCADA, And Other Industrial Control Systems



Synopsis

As the sophistication of cyber-attacks increases, understanding how to defend critical infrastructure systemsâ •energy production, water, gas, and other vital systemsâ •becomes more important, and heavily mandated. Industrial Network Security, Second Edition arms you with the knowledge you need to understand the vulnerabilities of these distributed supervisory and control systems. The book examines the unique protocols and applications that are the foundation of industrial control systems, and provides clear guidelines for their protection. This how-to guide gives you thorough understanding of the unique challenges facing critical infrastructures, new guidelines and security measures for critical infrastructure protection, knowledge of new and evolving security tools, and pointers on SCADA protocols and security implementation.All-new real-world examples of attacks against control systems, and more diagrams of systemsExpanded coverage of protocols such as 61850, Ethernet/IP, CIP, ISA-99, and the evolution to IEC62443 Expanded coverage of Smart Grid security New coverage of signature-based detection, exploit-based vs. vulnerability-based detection, and signature reverse engineering

Book Information

Paperback: 460 pages

Publisher: Syngress; 2 edition (December 29, 2014)

Language: English

ISBN-10: 0124201148

ISBN-13: 978-0124201149

Product Dimensions: 7.5 x 1 x 9.2 inches

Shipping Weight: 2.1 pounds (View shipping rates and policies)

Average Customer Review: 4.9 out of 5 starsÂ Â See all reviewsÂ (8 customer reviews)

Best Sellers Rank: #100,859 in Books (See Top 100 in Books) #3 inÂ Books > Computers & Technology > Hardware & DIY > Microprocessors & System Design > Control Systems #20 inÂ Books > Computers & Technology > Networking & Cloud Computing > Network Administration > Storage & Retrieval #93 inÂ Books > Computers & Technology > Networking & Cloud Computing > Network Security

Customer Reviews

First off a touch of background on the reviewer. I've been an automation professional for about 15 years working in industries ranging from big chemical to pharmaceuticals all the way from DCS's to tiny systems with 20 I/O and two screen HMI. I've worked for both operating companies and

integrators. I was excited when I saw the title of the book because I expected a balanced look at real world solutions for very real problems. There is a serious issue right now in our industry with a number of people spreading FUD about how we are all doomed because our protocols are insecure and vendors don't practice proper SDL. While the facts they speak of are true, I think a more balanced approach of highlighting the deficiencies and then immediately providing actionable information an end user can take away is more appropriate. This happens to be almost the exact flow of this book. You can see the table of contents for yourself but the authors do an excellent job of giving the reader some basis for understanding the material through a history lesson and also an introduction to basic concepts in ICS network design. Next they raise the stakes by describing the insecure protocols with a culmination discussing how you might hack these protocols. The information revealed is certainly not earth shattering and is probably Hacking 102 or 103 for someone once they learn the protocols. Where this text truly succeeds, however, is taking you from a fearful place in chapter 7 and walking you through real world tasks you can execute to safeguard your systems. Again, I won't repeat what you can see in the TOC but the authors do a magnificent job of taking you through the logical steps of assessing risk, compartmentalizing the risk, and then monitoring for undesirable activity on your network.

Security & Assurance) An Approach to Vulnerability Assessment for Navy Supervisory Control and Data Acquisition (SCADA) Systems An Architectural Framework for Describing Supervisory Control and Data Acquisition (SCADA) Systems Homeland Security and Private Sector Business: Corporations' Role in Critical Infrastructure Protection Extending Simple Network Management Protocol (SNMP) Beyond Network Management: A MIB Architecture for Network-Centric Services Power System SCADA and Smart Grids Design of Smart Power Grid Renewable Energy Systems Network Security Assessment: Know Your Network