Hacking Exposed Industrial Control Systems: ICS And SCADA Security Secrets & Solutions
**Synopsis**

Secure your ICS and SCADA systems the battle-tested Hacking Exposed® way! This hands-on guide exposes the devious methods cyber threat actors use to compromise the hardware and software central to petroleum pipelines, electrical grids, and nuclear refineries. Hacking Exposed Industrial Control Systems: ICS and SCADA Security Secrets and Solutions shows, step-by-step, how to implement and maintain an ICS-focused risk mitigation framework that is targeted, efficient, and cost-effective. The book arms you with the skills necessary to defend against attacks that are debilitating and potentially deadly. See how to assess risk, perform ICS-specific threat modeling, carry out penetration tests using "ICS safe" methods, and block malware. Throughout, the authors use case studies of notorious attacks to illustrate vulnerabilities alongside actionable, ready-to-deploy countermeasures.

Learn how to:
- Assess your exposure and develop an effective risk management plan
- Adopt the latest ICS-focused threat intelligence techniques
- Use threat modeling to create realistic risk scenarios
- Implement a customized, low-impact ICS penetration-testing strategy
- See how attackers exploit industrial protocols
- Analyze and fortify ICS and SCADA devices and applications
- Discover and eliminate undisclosed "zero-day" vulnerabilities
- Detect, block, and analyze malware of all varieties

**Book Information**

Series: Hacking Exposed

Paperback: 416 pages

Publisher: McGraw-Hill Education; 1 edition (September 13, 2016)

Language: English

ISBN-10: 1259589714


Product Dimensions: 7.3 x 0.8 x 9 inches

Shipping Weight: 1.4 pounds (View shipping rates and policies)

Average Customer Review: 3.7 out of 5 stars


**Customer Reviews**
Imagine this....Congratulations! You are the new CISO of the process control environment for a major energy/oil & gas operator. After many years of rotating through the various leadership programs within your company (they even let you in the computer room a few times) you have finally received the keys to the kingdom, to perhaps the most neglected network enabled infrastructure and systems within the company. After your last major successful rotation where you were responsible for implementation of patch management program across all your Windows servers - you know you have the skills to get this process control environment secure and protected from the forces of evil (and the accidental USB malware introduction)Unfortunately, unlike the data center you used to work in, the equipment is distributed all over the place. This will make getting a good inventory tough. No worries, your buddy loaned you NESSUS and you’ll get it all figured out (that Kali and NMAP thing is too confusing). Let the NESSUS-ing begin! 12 hours later... Ops! During your NESSUS scan some of these embedded computer thingy’s stopped responding even that Windows XP box (What’s that here for?). The result was an unplanned shutdown of an off shore asset that resulted in loss of product around 150,000 barrels per day. Good thing we got the plant running again within a day or two!Being the savvy leader you are, you’ve decided to transfer some of this risk and have some consultants come in to do an assessment. 250K USD and two weeks later (how do they write these reports so fast?) you are given a report that looks pretty much like the one you saw 18 months ago when a different consultancy did an assessment on a different asset on the other side of the world.

Download to continue reading...

Dmca