The Internet Of Risky Things: Trusting The Devices That Surround Us

O'REILLY
Sean Smith
The Internet of Risky Things
Trusting the Devices That Surround Us

Synopsis

By 2020, the Internet of Things (IoT) will consist of millions of computational devices intimately connected to real-world aspects of human life. In this insightful book, Professor Sean Smith, who worked in information security long before the web appeared, explains that if we build the IoT the way we built the current internet and other information technology initiatives, weâ ™re headed for trouble.With a focus on concrete solutions, The Internet of Risky Things explains how we can avoid simple flaws that have plagued several dramatic IT advances in recent decades. Developers, engineers, industrial designers, makers, and researchers will explore "design patterns of insecurities" and learn whatâ ™s required to route around or fix them in the nascent IoT.Examine bugs that plague large-scale systems, including integer overflow, race conditions, and memory corruptionLook at successful and disastrous examples of previous quantum leaps in health IT, the smart grid, and autonomous vehiclesExplore patterns in coding, authentication, and cryptography that led to insecurityLearn how blunders that led to spectacular IT disasters could have been avoided

Book Information

Paperback: 240 pages

Publisher: O’Reilly Media; 1 edition (January 29, 2017)

Language: English

ISBN-10: 149196362X

ISBN-13: 978-1491963623

Product Dimensions: 6 x 0.5 x 9 inches

Shipping Weight: 8 ounces (View shipping rates and policies)

Average Customer Review: 5.0 out of 5 stars 1 customer review

Best Sellers Rank: #380,301 in Books (See Top 100 in Books) #42 inÂ Books > Engineering & Transportation > Engineering > Electrical & Electronics > Electronics > Sensors #77 inÂ Books > Engineering & Transportation > Engineering > Telecommunications & Sensors > Mobile & Wireless #82 inÂ Books > Engineering & Transportation > Engineering > Industrial, Manufacturing & Operational Systems > Industrial Technology

Customer Reviews

Professor Sean Smith has been working in information security--attacks and defenses, for industry and government--since before there was a Web. In graduate school, he worked with the US Postal Inspection Service on postal meter fraud; as a post-doc and staff member at Los Alamos National

Laboratory, he performed security reviews, designs, analyses, and briefings for a wide variety of public-sector clients; at IBM T.J. Watson Research Center, he designed the security architecture for (and helped code and test) the IBM 4758 secure coprocessor, and then led the formal modeling and verification work that earned it the world’s first FIPS 140-1 Level 4 security validation.In July 2000, Sean left IBM for Dartmouth, since he was convinced that the academic education and research environment is a better venue for changing the world. His current work, as PI of the Dartmouth Trust Lab and Director of Dartmouth’s Institute for Security, Technology, and Society investigates how to build trustworthy systems in the real world.At Dartmouth, many of his courses have been named "favorite classes" by graduating seniors. His book Trusted Computing Platforms: Design and Applications (Springer, 2005) provides a deeper presentation of this research journey; his book The Craft of System Security (Addison-Wesley, 2007) resulted from the educational journey.Sean has published over one hundred refereed papers; been granted over a dozen patents; and advised over three dozen Ph.D., M.S., and senior honors theses. He and his students have won several "Best Paper" awards.Sean was educated at Princeton and CMU, and is a member of Phi Beta Kappa and Sigma Xi.

A grounded look at the security issues that already plague the Internet of Things and will challenge widespread adoption. The author is an excellent teacher. I opened this book out of a sense of obligation. I advise companies on pricing and monetization of the Industrial Internet of Things and security is a relevant economic value driver and thus a value metric. I left the book intellectually stimulated, eager to read more by this author, and deeply worried.Smith grounds his work in an understanding of historical security issues and anti-patterns (Chapter 4 on Overcoming Design Patterns for Insecurity is worth committing to memory). He gives many examples, some well known other probably only followed by security experts. The treatment of the Volkswagen scandal where the emissions controls were intentionally designed to trick regulators brings an interesting perspective. The final chapter that references Ogden and Richard’s seminal work on semiology was eye opening. Understanding the interacting roles of users’ mental models, the system model and the real world and how mappings lead to security issues was thought provoking.Two points really stuck with me. The lifespan of physical objects is much longer than that of most software. The methods (only partially successful) that we have developed for security on the Internet of Computers, are not likely to scale across time. There is a real risk of having large numbers of legacy devices with compromised security. The surface for attack in the Internet of Things is orders of magnitude larger than in the Internet of Computers.There are many more insertion points and types of insertion points. Our current approaches will not scale over space either.This book should be read well beyond security geeks, or even IoT implementers. There are insights and models here that are widely applicable.

Download to continue reading...

The Internet of Risky Things: Trusting the Devices That Surround Us ESP8266: Programming NodeMCU Using Arduino IDE - Get Started With ESP8266 (Internet Of Things, IOT, Projects In Internet Of Things, Internet Of Things for Beginners, NodeMCU Programming, ESP8266) Internet Business Insights: Lessons Learned and Strategies Used by 101 Successful Internet-Based Entrepreneurs (Internet Business Books) Eargle’s The Microphone Book: From Mono to Stereo to Surround - A Guide to Microphone Design and Application (Audio Engineering Society Presents) Surround Sound: Up and running Unshakeable Trust: Find the Joy of Trusting God at All Times, in All Things Autism’s False Prophets: Bad Science, Risky Medicine, and the Search for a Cure The Risky Rescue (Key Hunters #6) Operation Chowhound: The Most Risky, Most Glorious US Bomber Mission of WWII SCENARIOS 3 & 4--Risky Business: 2 Interactive Stories in 1 (Scenarios for Girls) I’ve Got This Friend Who: Advice for Teens and Their Friends on Alcohol, Drugs, Eating Disorders, Risky Behavior and More Risky Teen Behavior (Issues That Concern You) US Army Technical Manual, ARMY DATA SHEETS FOR CARTRIDGES, CARTRIDGE ACTUATED DEVICES AND PROPELLANT ACTUATED DEVICES, FSC 1377, TM 43-0001-39, 1991 Integrated circuit devices and components (Integrated-circuit technology, analog and logic circuit design, memory and display devices) ISO 14971:2007, Medical devices - Application of risk management to medical devices ISO 14971:2000, Medical devices -- Application of risk management to medical devices Prostheses: Design, Types, and Complications (Biomedical Devices and Their Applications; Medical Devices and Equipment) Echo: Dot:The Ultimate User Guide to Echo Dot 2nd Generation with Latest Updates (the 2017 Updated User Guide,by ,Free Movie,web services,Free ... Kit) (internet,smart devices, Alexa) Echo: NEW 2017 Echo Beginnerâ ™s User Guide to Master Your Echo (with latest updates, 2017 updated user guide, Echo Manual, Alexa, ... echo app) (internet,smart devices, Alexa) Internet Empire Profits: Create an Internet Business from Absolute Scratch with Domain Flipping & Associate Marketing

FAQ & Help