Embedded Systems Security: Practical Methods For Safe And Secure Software And Systems Development

EMBEDDED SYSTEMS SECURITY
Practical Methods for Safe and Secure Software and Systems Development

David Kleidermacher and Mike Kleidermacher

DOWNLOAD EBOOK
Synopsis

The ultimate resource for making embedded systems reliable, safe, and secure. Embedded Systems Security provides:

- A broad understanding of security principles, concerns, and technologies
- Proven techniques for the efficient development of safe and secure embedded software
- A study of the system architectures, operating systems and hypervisors, networking, storage, and cryptographic issues that must be considered when designing secure embedded systems
- Nuggets of practical advice and numerous case studies throughout

Written by leading authorities in the field with 65 years of embedded security experience: one of the original developers of the world’s only Common Criteria EAL 6+ security certified software product and a lead designer of NSA certified cryptographic systems. This book is indispensable for embedded systems and security professionals, new and experienced. An important contribution to the understanding of the security of embedded systems. The Kleidermachers are experts in their field. As the Internet of things becomes reality, this book helps business and technology management as well as engineers understand the importance of "security from scratch." This book, with its examples and key points, can help bring more secure, robust systems to the market. Dr. Joerg Borchert, Vice President, Chip Card & Security, Infineon Technologies North America Corp.; President and Chairman, Trusted Computing Group

Embedded Systems Security provides real-world examples of risk and exploitation; most importantly the book offers clear insight into methods used to counter vulnerabilities to build true, native security into technology. Adriel Desautels, President and CTO, Netragard, LLC.

Security of embedded systems is more important than ever. The growth in networking is just one reason. However, many embedded systems developers have insufficient knowledge of how to achieve security in their systems. David Kleidermacher, a world-renowned expert in this field, shares in this book his knowledge and long experience with other engineers. A very important book at the right time. Prof. Dr.-Ing. Matthias Sturm, Leipzig University of Applied Sciences; Chairman, Embedded World Conference steering board

Gain an understanding of the operating systems, microprocessors, and network security critical issues that must be considered when designing secure embedded systems.

Contains nuggets of practical and simple advice on critical issues highlighted throughout the text. Short and to the point real case studies included to demonstrate embedded systems security in practice.

Book Information

Paperback: 416 pages
Publisher: Newnes; 1 edition (March 30, 2012)
I have been designing and implementing security products for about 7+ years now (embedded systems for 12yrs) to "high assurance" standards and I have to say these authors have done a great job with this book. I usually don't like to buy books that have not been heavily rated yet, but with security books you don't want a 10 year old book (unless maybe it is cryptography!) if you want something that is relevant. That is why I am taking the time to rate this book. I encourage anyone considering this book to buy it right now. The issues and technologies are relevant and the authors have done a great job putting this together. I am very experienced in this area, but I think it is a pretty easy read... that being said I have only got through the first three chapters so far so I will update this if I change my mind!UPDATE: I finished this book about a week ago and I still recommend it. However I will say it is a bit slanted toward Green Hills... probably has to do with the author's close relationship with them! (I'll let you look it up). So read with that in mind. You see a similar slant/sales job in the model driven design (MDD) section that was written by another person with a company that sells a tool for MDD. I would say read the content and get out the security concepts without taking too much stock in how it may reflect on a competing vendor products. I also want to add that as far as the "Embedded Cryptography" section of the book... it is nice to have in the book but if you want to learn about cryptography there are much better sources out there. This book isn't meant to just be a source for crypto so it makes sense but just want to make the readers aware. Some suggestions for a starter book that is "Applied Cryptography" by Schenier.

Download to continue reading...

Development Home Security: Top 10 Home Security Strategies to Protect Your House and Family