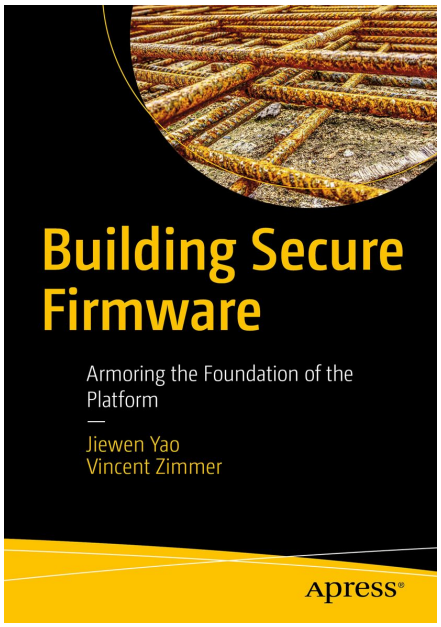

1st ed., XX, 230 p.

Printed book

Softcover

Ca. 34,99 € | Ca. £29.99 | Ca. $39.99 [1]Ca. 37,44 € (D) | Ca. 38,49 € (A) | Ca. CHF 41,50

eBook

Available from your library or springer.com/shop

MyCopy [3]

Printed eBook for just € | $ 24.99

springer.com/mycopy

Jiewen Yao, Vincent Zimmer

Building Secure Firmware

Armoring the Foundation of the Platform

- Provides insights from the inventors of many of the defenses
- Shows you how to apply the best-known methods from the authors' years of platform deployment and standards work
- Teaches you how to integrate real code mapping to theory

Use this book to build secure firmware. As operating systems and hypervisors have become successively more hardened, malware has moved further down the stack and into firmware. Firmware represents the boundary between hardware and software, and given its persistence, mutability, and opaqueness to today's antivirus scanning technology, it represents an interesting target for attackers. As platforms are universally network-connected and can contain multiple devices with firmware, and a global supply chain feeds into platform firmware, assurance is critical for consumers, IT enterprises, and governments. This importance is highlighted by emergent requirements such as NIST SP800-193 for firmware resilience and NIST SP800-155 for firmware measurement. This book covers the secure implementation of various aspects of firmware, including standards-based firmware—such as support of the Trusted Computing Group (TCG), Desktop Management Task Force (DMTF), and Unified Extensible Firmware Interface (UEFI) specifications—and also provides code samples and use cases. Beyond the standards, alternate firmware implementations such as ARM Trusted Firmware and other device firmware implementations (such as platform roots of trust), are covered. What You Will learn Get an overview of proactive security development for firmware, including firmware threat modeling Understand the details of architecture, including protection, detection, recovery, integrity measurement, and access control Be familiar with best practices for secure firmware development, including trusted execution environments, cryptography, and language-based defenses Know the techniques used for security validation and maintenance Who This Book Is For Given the complexity of modern platform boot requirements and the threat landscape, this book is relevant for readers spanning from IT decision makers to developers building firmware