1. Record Nr. UNINA9910427047903321

Autore	Yao Jiewen
Titolo	Building secure firmware : armoring the foundation of the platform / / Jiewen Yao, Vincent Zimmer
Pubbl/distr/stampa	Berkeley, California : , : APress, , [2020] ©2020
ISBN	1-4842-6106-2
Edizione	[1st ed. 2020.]
Descrizione fisica	1 online resource (941 pages)
Disciplina	005.8
Soggetti	Security
Lingua di pubblicazione	Inglese
Formato	Materiale a stampa
Livello bibliografico	Monografia
Note generali	Includes index.
Nota di contenuto	Part I: Overview -- Chapter 1: Introduction to Firmware -- Chapter 2: Proactive Firmware Security Development -- Part II: Security Architecture -- Chapter 3: Firmware Resilience - Protection -- Chapter 4: Firmware Resilience - Detection -- Chapter 5: Firmware Resilience – Recovery -- Chapter 6: OS Resilience -- Chapter 7: Trusted Boot -- Chapter 8: Device Security -- Chapter 9: S3 Resume -- Chapter 10: Access Control -- Chapter 11: Configuration -- Chapter 12: Security Model -- Chapter 13: Virtual Firmware -- Part III: Security Development -- Chapter 14: General Coding Practice -- Chapter 15: Compiler Defensive Technology -- Chapter 16: The Kernel -- Chapter 17: Trusted Execution Environment -- Chapter 18: Silicon Security Configuration -- Chapter 19: Cryptography -- Chapter 20: Programming Language -- Part IV: Security Test and Maintenance -- Chapter 21: Security Unit Test -- Chapter 22: Security Validation and Penetration -- Chapter 23: Maintenance.
Sommario/riassunto	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. You will: 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.