1.	Record Nr.	UNINA9910869180703321
	Autore	Shepherd Carlton
	Titolo	Trusted Execution Environments / / by Carlton Shepherd, Konstantinos Markantonakis
	Pubbl/distr/stampa	Cham : , : Springer International Publishing : , : Imprint : Springer, , 2024
	ISBN	3-031-55561-9
	Edizione	[1st ed. 2024.]
	Descrizione fisica	1 online resource (211 pages)
	Collana	Computer Science Series
	Altri autori (Persone)	MarkantonakisKonstantinos
	Disciplina	005.8
	Soggetti	Data protection Computer networks - Security measures Cryptography Data encryption (Computer science) Cooperating objects (Computer systems) Data and Information Security Mobile and Network Security Cryptology Cyber-Physical Systems
	Lingua di pubblicazione	Inglese
	Formato	Materiale a stampa
	Livello bibliografico	Monografia
	Nota di contenuto	Introduction -- Background Material -- Operating System Controls -- Isolated Hardware Execution Platforms -- Building Execution Environments from the Trusted Platform Module -- Trusted World Systems -- Enclave Computing -- Deployment Issues, Attacks, and Other Challenges -- Conclusion.
	Sommario/riassunto	Trusted execution environments (TEEs) protect sensitive code and data on computing platforms, even when the primary operating system is compromised. Once a technical curiosity, TEEs have rapidly become a key component in securing numerous systems from cloud servers to constrained devices. Today, TEEs have been deployed on billions of devices for protecting financial payments, personal files, copyrighted media content, and many others. Despite this, TEEs remain poorly understood due to their complexity and diversity. This book addresses this gap, providing a comprehensive treatment of different TEE

technologies, their features, benefits, and shortcomings. A holistic view of secure and trusted execution is taken, examining smart cards and CPU protection rings before discussing modern TEEs, such as Intel SGX and ARM TrustZone. A wide range of paradigms for building secure and trusted execution environments are explored, from dedicated security chips to system-on-chip extensions and virtualisation technologies.

The relevant industry standards and specifications are covered in detail, including how TEEs are evaluated and certified in practice with respect to security. Several case studies are presented showing how TEEs are used in some common security mechanisms, such as secure boot sequences, biometric authentication, and file-based encryption. This book also discusses present challenges in the field, covering potential attack vectors against TEEs and concerns relating to fragmentation, interoperability, and transparency. Lastly, a selection of future directions are examined that may be used by the trusted execution environments of tomorrow. This book is particularly targeted at practitioners and researchers in cyber security, such as penetration testers, security engineers, and security analysts. Additionally, this book serves as a valuable resource for university students, both postgraduate and advanced undergraduates, and professors in computer science and electrical engineering.