1.	Record Nr.	UNINA9910303454803321
	Titolo	Cyber-Physical Systems Security [[electronic resource] /] / edited by Çetin Kaya Koç
	Pubbl/distr/stampa	Cham : , : Springer International Publishing : , : Imprint : Springer, , 2018
	ISBN	3-319-98935-9
	Edizione	[1st ed. 2018.]
	Descrizione fisica	1 online resource (347 pages)
	Disciplina	006.22
	Soggetti	Data structures (Computer science)
		Data protection
		Public safety
		System safety
		Data Structures and Information Theory
		Security
		Crime Control and Security
		Security Science and Technology
	Lingua di pubblicazione	Inglese
	Formato	Materiale a stampa
	Livello bibliografico	Monografia
	Nota di contenuto	Robust Digital Computation in the Physical World -- Constraint-Based Framework for Reasoning with Differential Equations -- Approximate Computing and Its Application to Hardware Security -- Mathematical Optimizations for Deep Learning -- A Zero-Entry Cyber Range Environment for Future Learning Ecosystems -- Parallel Programming in Cyber-Physical Systems -- Automatic Application of Software Countermeasures Against Physical Attacks -- Time-Delay Attacks in Network Systems -- Attack Tree Construction and Its Application to the Connected Vehicle -- Reinforcement Learning and Trustworthy Autonomy -- Identifier Randomization: An Efficient Protection Against CAN-Bus Attacks -- Public-Key-Based Lightweight Swarm Authentication -- Physical Security Versus Masking Schemes -- Embedded Classifiers for Energy Constrained IoT Network Security -- Challenges in Cyber Security: Ransomware Phenomenon -- Applying Model-Based Situational Awareness and Augmented Reality to Next-

Generation Physical Security Systems.

Sommario/riassunto	The chapters in this book present the work of researchers, scientists, engineers, and teachers engaged with developing unified foundations, principles, and technologies for cyber-physical security. They adopt a multidisciplinary approach to solving related problems in next-generation systems, representing views from academia, government bodies, and industrial partners, and their contributions discuss current work on modeling, analyzing, and understanding cyber-physical systems.