1. Record Nr.   UNINA9910483454203321

    Titolo   Hardware supply chain security : threat modelling, emerging attacks
                            and countermeasures / / Basel Halak, editor

    Pubbl/distr/stampa   Cham, Switzerland : , : Springer, , [2021]
                            ©2021

    ISBN   3-030-62707-1

    Edizione   [1st ed. 2021.]

    Descrizione fisica   1 online resource (XV, 217 p. 2 illus.)

    Disciplina   005.8

    Soggetti   Computer security
                            Computer input-output equipment - Security measures
                            Computer viruses

    Lingua di pubblicazione Inglese

    Formato   Materiale a stampa

    Livello bibliografico   Monografia

    Nota di contenuto   Part I. Threat Modelling of Hardware Supply Chain -- Chapter 1. CIST: A
                            Threat Modelling Approach for Hardware Supply Chain Security -- Part
                            II. Emerging Hardware-based Security Attacks and Countermeasures --
                            Chapter 2. A Cube Attack on a Trojan-Compromised Hardware
                            Implementation of Ascon -- Chapter 3. Anti-counterfeiting Techniques
                            for Resources-Constrained Devices -- Part III. Anomaly Detection in
                            Embedded Systems -- Chapter 4. Anomalous Behaviour in Embedded
                            Systems -- Chapter 5. Hardware Performance Counters (HPCs) for
                            Anomaly Detection -- Chapter 6. Anomaly Detection in an Embedded
                            System.

    Sommario/riassunto   This book presents a new threat modelling approach that specifically
                            targets the hardware supply chain, covering security risks throughout
                            the lifecycle of an electronic system. The authors present a case study
                            on a new type of security attack, which combines two forms of attack
                            mechanisms from two different stages of the IC supply chain. More
                            specifically, this attack targets the newly developed, light cipher
                            (Ascon) and demonstrates how it can be broken easily, when its
                            implementation is compromised with a hardware Trojan. This book also
                            discusses emerging countermeasures, including anti-counterfeit design
                            techniques for resources constrained devices and anomaly detection