1. Record Nr. UNINA9910293145603321

Autore	Lysne Olav
Titolo	The Huawei and Snowden Questions [[electronic resource]] : Can Electronic Equipment from Untrusted Vendors be Verified? Can an Untrusted Vendor Build Trust into Electronic Equipment? / / by Olav Lysne
Pubbl/distr/stampa	Cham, : Springer Nature, 2018 Cham : , : Springer International Publishing : , : Imprint : Springer, , 2018
ISBN	3-319-74950-1
Edizione	[1st ed. 2018.]
Descrizione fisica	1 online resource (XIV, 116 p. 6 illus., 5 illus. in color.)
Collana	Simula SpringerBriefs on Computing, , 2512-1677 ; ; 4
Disciplina	005.8
Soggetti	Computer security Computer engineering Management information systems Computer science Political science Economic policy Privacy Computer Engineering Management of Computing and Information Systems Governance and Government R & D/Technology Policy
Lingua di pubblicazione	Inglese
Formato	Materiale a stampa
Livello bibliografico	Monografia
Nota di contenuto	1 Introduction -- 2 Trust -- 3 What is an ICT-System? -- 4 Development of ICT Systems -- 5 Theoretical Foundation -- 6 Reverse Engineering of Code -- 7 Static Detection of Malware -- 8 Dynamic Detection Methods -- 9 Formal Methods -- 10 Software Quality and Quality Management -- 11 Containment of Untrusted Modules -- 12 Summary and Way Forward.
Sommario/riassunto	Preliminary This book is open access under a CC BY 4.0 license. This book answers two central questions: firstly, is it at all possible to verify

electronic equipment procured from untrusted vendors? Secondly, can I build trust into my products in such a way that I support verification by untrusting customers? In separate chapters the book takes readers through the state of the art in fields of computer science that can shed light on these questions. In a concluding chapter it discusses realistic ways forward. In discussions on cyber security, there is a tacit assumption that the manufacturer of equipment will collaborate with the user of the equipment to stop third-party wrongdoers. The Snowden files and recent deliberations on the use of Chinese equipment in the critical infrastructures of western countries have changed this. The discourse in both cases revolves around what malevolent manufacturers can do to harm their own customers, and the importance of the matter is on par with questions of national security. This book is of great interest to ICT and security professionals who need a clear understanding of the two questions posed in the subtitle, and to decision-makers in industry, national bodies and nation states. .