1. Record Nr. UNINA9910349390303321

Titolo	Security Protocols XXVI : 26th International Workshop, Cambridge, UK, March 19–21, 2018, Revised Selected Papers / / edited by Vashek Matyáš, Petr Švenda, Frank Stajano, Bruce Christianson, Jonathan Anderson
Pubbl/distr/stampa	Cham : , : Springer International Publishing : , : Imprint : Springer, , 2018
ISBN	3-030-03251-5
Edizione	[1st ed. 2018.]
Descrizione fisica	1 online resource (XI, 305 p. 30 illus., 19 illus. in color.)
Collana	Security and Cryptology ; ; 11286
Disciplina	005.8
Soggetti	Data protection Software engineering Application software Computer communication systems Artificial intelligence Security Software Engineering/Programming and Operating Systems Information Systems Applications (incl. Internet) Computer Communication Networks Artificial Intelligence
Lingua di pubblicazione	Inglese
Formato	Materiale a stampa
Livello bibliografico	Monografia
Note generali	Includes index.
Nota di contenuto	Raven Authentication Service - Attacks and Countermeasures -- Raven Authentication Service - Attacks and Countermeasures (Transcript of Discussion) -- Your code is my code: Exploiting a common weakness in OAuth 2.0 implementations -- Your code is my code: Exploiting a common weakness in OAuth 2.0 implementations (Transcript of Discussion) -- Non-Monotonic Security Protocols and Failures in Financial Intermediation -- Non-Monotonic Security Protocols and Failures in Financial Intermediation (Transcript of Discussion) -- HoneyPAKEs -- HoneyPAKEs (Transcript of Discussion) -- Entropy crowdsourcing - protocols for link key updates in wireless sensor Networks -- Entropy crowdsourcing - protocols for link key updates in

wireless sensor networks (Transcript of Discussion) -- Daemones non Operantur Nisi per Artem -- Daemones non Operantur Nisi per Artem (Transcript of Discussion) -- Intentionality and agency in security -- Intentionality and agency in security (Transcript of Discussion) -- Incentives in Security Protocols -- Incentives in Security Protocols (Transcript of Discussion) -- Too Big to FAIL: What You Need to Know Before Attacking a Machine Learning System -- Too Big to FAIL: What You Need to Know Before Attacking a Machine Learning System (Transcript of Discussion) -- How does match-fixing inform computer game security -- How does match-fixing inform computer game security? (Transcript of Discussion) -- From Secure Messaging to Secure Collaboration -- From Secure Messaging to Secure Collaboration (Transcript of Discussion) -- Requirements for Root of Trust Establishment -- Requirements for Root of Trust Establishment (Transcript of Discussion) -- User Authentication for the Internet of Things -- User Authentication for the Internet of Things (Transcript of Discussion) -- Why Preventing a Cryptocurrency Exchange Heist Isn't Good Enough -- Why Preventing a Cryptocurrency Exchange Heist Isn't Good Enough (Transcript of Discussion) -- Making Bitcoin Legal -- Making Bitcoin Legal (Transcript of Discussion) -- On the incommensurability of laws and technical mechanisms: Or, what cryptography can't do -- On the incommensurability of laws and technical mechanisms: Or, what cryptography can't do (Transcript of Discussion) -- Shatter Secrets: Using Secret Sharing to Cross Borders with Encrypted Devices -- Shatter Secrets: Using Secret Sharing to Cross Borders with Encrypted Devices (Transcript of Discussion). .

Sommario/riassunto

This book constitutes the thoroughly refereed post-workshop proceedings of the 26th International Workshop on Security Protocols, held in Cambridge, UK, in March 2018. The volume consists of 17 thoroughly revised invited papers presented together with the respective transcripts of discussions. The theme of this year's workshop was fail-safe and fail-deadly concepts in protocol design. The topics covered included failures and attacks; novel protocols; threat models and incentives; cryptomoney; and the interplay of cryptography and dissent.