1.

Record Nr.	UNINA9910482397103321
Autore	Anon
Titolo	Belgiae pacificatorum vera delineatio. = Pourtraicture vraye des pacificateurs des Pays Bas.-d= Ware afbeeldingen vande vredemakers der Nederlanden [[electronic resource]]
Pubbl/distr/stampa	Copenhagen, : Hendrik Hondius, 1608
Descrizione fisica	Online resource (2°)
Lingua di pubblicazione	Molteplice
Formato	Materiale a stampa
Livello bibliografico	Monografia
Note generali	Reproduction of original in Koninklijke Bibliotheek, Nationale bibliotheek van Nederland.

2.

Record Nr.	UNINA9910816837003321
Titolo	Pushing the boundaries : a conversation with Freeman Dyson / / edited with an introduction by Howard Burton
Pubbl/distr/stampa	[Place of publication not identified] : , : Ideas Roadshow, , [2020] ©2014
ISBN	1-77170-043-2
Descrizione fisica	1 online resource (50 pages)
Collana	Ideas Roadshow Conversations
Disciplina	530.15
Soggetti	Mathematical physics
Lingua di pubblicazione	Inglese
Formato	Materiale a stampa
Livello bibliografico	Monografia
Nota di contenuto	Intro -- A Note on the Text -- Introduction -- The Conversation -- I. Debating Exceptionalism -- II. In Praise of Rebels -- III. Against Reductionism -- IV. Foundational Issues -- V. Current Mysteries -- VI. The Origin of Life -- VII. Space Travel -- VIII. Science and Society -- IX. Religion -- X. Final Thoughts -- Continuing the Conversation.

Sommario/riassunto

This book is based on an in-depth filmed conversation between Howard Burton and former mathematical physicist and writer Freeman Dyson, who was one of the most celebrated polymaths of our age. Freeman Dyson had his academic home for more than 60 years at the Institute for Advanced Study in Princeton. He has reshaped thinking in fields from math to astrophysics to medicine, while pondering nuclear-propelled spaceships designed to transport human colonists to distant planets. During this wide-ranging conversation Freeman looks back on his simultaneously transformative careers in theoretical physics, mathematics, biology, rocket ship design, nuclear disarmament and writing.This carefully-edited book includes an introduction, Pure and Applied, and questions for discussion at the end of each chapter. Howard Burton was the Founding Director of Canada's Perimeter Institute for Theoretical Physics. He holds a PhD in theoretical physics and an MA in philosophy. This book is part of an expanding series of 100+ Ideas Roadshow conversations, each one presenting a wealth of candid insights from a leading expert in a focused yet informal setting to provide a uniquely accessible window into frontline research and scholarship that wouldn't otherwise be encountered through standard lectures and textbooks.

3.	Record Nr.	UNINA9910961414803321
	Autore	Fagbemi Damilare D
	Titolo	The IoT Architect's Guide to Attainable Security and Privacy
	Pubbl/distr/stampa	Milton, : Auerbach Publishers, Incorporated, 2019
	ISBN	1-000-76261-0 1-000-76225-4 0-367-44093-8
	Edizione	[1st ed.]
	Descrizione fisica	1 online resource (330 pages)
	Altri autori (Persone)	WheelerDavid M WheelerJ. C
	Disciplina	005.8
	Soggetti	Internet of things - Security measures
	Lingua di pubblicazione	Inglese
	Formato	Materiale a stampa
	Livello bibliografico	Monografia
	Note generali	Description based upon print version of record.
	Nota di contenuto	Cover -- Half Title -- Title Page -- Copyright Page -- Dedication -- Contents -- Foreword -- Foreword -- Preface -- Acknowledgments -- About the Authors -- Part One -- Chapter 1 How We Got Here -- 1.1 We Forgot Security When Building the Internet -- 1.2 What's This Book About and Who's It For? -- 1.3 Let's Break Down the Book -- 1.4 What's an IoT System? -- 1.4.1 Everyone Needs to Know the Location of the Nearest Pizza -- 1.4.2 Computing Everywhere -- 1.5 An IoT System's Major Components -- 1.5.1 The Human IoT System -- 1.6 Shall We Just Connect Everything? -- 1.7 Wait! We Need to Add Security! -- References -- Chapter 2 The IoT Castle and Its Many Gates -- 2.1 And the Internet Got Hacked: Analyzing the Mirai Attack -- 2.1.1 Resolution of the Mirai Attack -- 2.2 "Full Disclosure," Ethics, and "Hacking Buildings for Fun and Profit" -- 2.3 Defending IoT Castles -- 2.3.1 Know Thine Enemy -- 2.4 Attacking the IoT Castle -- 2.5 A Closer Look at IoT Attack Surfaces and Breach Consequences -- 2.6 The Road Ahead -- References -- Chapter 3 The IoT Security Economy -- 3.1 A Toy Is Not a Plaything, It's a Tool for Cybercrime -- 3.2 Understanding the IoT Economy -- 3.3 The Cybercriminal Economy -- 3.4 Cryptocurrency 01100101 -- 3.4.1 Mining, Minting, and Verifying Transactions -- 3.4.2 The Draw of Crypto Mining -- 3.4.3 The Monero Cryptocurrency -- 3.5 Where Cybercriminals Go to Hide -- 3.6

Accessing the Dark Web with Tor -- 3.7 Money Money Money . . . Making Bank on the Dark Web -- 3.8 Challenges in the Regular IoT Economy: Out of the Dark, and into Naïvety -- 3.9 Why You Should Care -- References -- Part Two -- Chapter 4 Architecting IoT Systems That Scale Securely -- 4.1 The IoT System Architecture -- 4.1.1 The Cloud Layer -- 4.1.2 The Gateway Layer -- 4.1.3 The Devices Layer -- 4.2 IoT Must Be a Low-Cost System.

4.2.1 IoT Gateway Layer: Reason 1-Client Volume -- 4.2.2 IoT Gateway Layer: Reason 2-Energy Costs -- 4.2.3 IoT Gateway Layer: Reason 3-Long-Haul Communications Costs -- 4.2.4 IoT Gateway Layer: Reason 4-Security -- 4.2.5 IoT Gateway Layer: Reason 5-Scaling -- 4.3 Details of the IoT Architecture Layers -- 4.3.1 Basic IoT Edge Device Architecture -- 4.3.2 Simple IoT Gateway Architecture -- 4.4 Fundamental IoT Cloud Architecture -- 4.5 Why Security Is Hard in IoT Systems -- References -- Chapter 5 Security Architecture for Real IoT Systems -- 5.1 Preparation for the Coming Storm -- 5.2 What Is Security Architecture? -- 5.3 The Security Architecture Process -- 5.3.1 Analyze the System Architectural Views -- 5.3.2 Perform Threat Analysis -- 5.3.3 Threat Disposition -- 5.3.4 Incorporate Threat Mitigation into the System Architecture -- 5.3.5 Rinse and Repeat -- 5.3.6 Security Architecture Review Board -- 5.3.7 After Security Architecture Approval -- 5.4 Design Principles for Security Architecture -- 5.4.1 Open Design Principle -- 5.4.2 Economy of Mechanism Principle -- 5.4.3 Fail-Safe Default Principle -- 5.4.4 Separation of Privilege Principle -- 5.4.5 Complete Mediation Principle -- 5.4.6 Least Privilege Principle -- 5.4.7 Least Common Mechanism Principle -- 5.4.8 Defense-in-Depth Principle -- 5.4.9 Trust No One Principle -- 5.4.10 Secure the Weakest Link Principle -- 5.5 Addressing the Security Concerns of an Industrial IoT System -- 5.5.1 The Autonomous Factory -- 5.5.2 Architecting for IoT Manageability -- 5.5.3 Architecting IoT Device Trust -- 5.5.4 Architecting End-to-End Encryption -- 5.5.5 Architecting for Longevity -- 5.5.6 Architecting IoT with Intelligence -- 5.5.7 Architecting for Scale -- 5.6 Summarizing IoT Security Architecture -- References -- Chapter 6 Securing the IoT Cloud -- 6.1 The History of The Cloud -- 6.2 So What Is the Cloud?.

6.3 Cloud Architecture Overview -- 6.3.1 Object Storage Service -- 6.3.2 Block Storage Service -- 6.3.3 Compute Service -- 6.3.4 Image Service -- 6.3.5 Networking Service -- 6.3.6 Identity Service -- 6.4 How the Cloud Enables and Scales IoT Security -- 6.4.1 Secure Centralization of Data Management and Analytics -- 6.4.2 Secure IoT Device Management -- 6.4.3 Secure Multi-Presence Access to IoT Devices -- 6.5 A Summary of Security Considerations for IoT Cloud Back Ends -- 6.6 Practical IoT Cloud Security Architecture: The "Dalit" Smart City Use Case -- 6.6.1 Introducing ATASM as a Threat Modeling Tool -- 6.6.2 Dalit Cloud Architecture Overview -- 6.6.3 Data Ingestion and Processing View -- 6.6.4 Device Software (and Firmware) Updates View -- 6.6.5 Networking View -- 6.6.6 Cloud Resource Monitoring and Auditing View -- 6.6.7 Threat Analysis -- 6.7 What We Learned -- References -- Chapter 7 Securely Connecting the Unconnected -- 7.1 What Connectivity Means to IoT -- 7.2 Classifying IoT Communication Protocols -- 7.2.1 Bandwidth, Bits, Codes, and Hertz -- 7.2.2 Physical Layer Communications-Wired and Wireless -- 7.2.3 Wired Phys -- 7.2.4 Wireless Phys -- 7.2.5 Comparison of Different Phys -- 7.2.6 Upper-Layer Protocols -- 7.2.7 Application Layer Protocols for IoT -- 7.2.8 Protocols Summary -- 7.3 Network Security for IoT -- 7.3.1 Protecting the Little Ones -- 7.3.2 Additional Steps by the Bigger Devices- Self-Protection Services -- 7.3.3 System Protect and Detect Services -- 7.4 Security Analysis for Protocols -- 7.4.1 The

Preliminaries and Definitions -- 7.4.2 An Informal Analysis Model for Protocol Design -- 7.4.3 An Informal Analysis of a Digest Authentication Protocol -- 7.4.4 The Formal Security Models -- 7.5 IoT Protocol Conclusions -- References -- Chapter 8 Privacy, Pirates, and the Tale of a Smart City.

8.1 Shroud for Dark Deeds or Fortress for the Vulnerable -- 8.2 Chapter Scope -- 8.3 AI and IoT Unite-Amplifying the Engineer's Significance in Society -- 8.4 The Elephant in the Room -- 8.5 Scenario: Safe Driving App Meets Smart Fridge -- 8.5.1 IoT Saves Our Bacon, but Tattles if We Eat Cured Fatty Pork -- 8.5.2 Smart Algorithms to the Rescue -- 8.6 From Autonomous Vehicles to Smart Cities -- 8.6.1 Scenario: The Tale of a Smart City -- 8.7 The Deepfake and IoT -- 8.8 Learning from Smart Appliances, Myopia, and Deepfakes -- 8.9 Privacy Playbook -- 8.9.1 Bring in the "Great White Shark" -- 8.9.2 Know the Pirate Lineup -- 8.9.3 Believe in the Data Afterlife -- 8.9.4 Defy Fate -- 8.9.5 Obfuscate Waldo -- 8.9.6 Playbook Wrap-up -- References -- Chapter 9 Privacy Controls in an Age of Ultra-Connectedness -- 9.1 Introduction -- 9.2 Defining Privacy and Information Privacy -- 9.3 A Better Definition of Personal Information and How That Becomes Personal Knowledge -- 9.3.1 Data from a Fitness App Turns into Military Intelligence -- 9.4 Who Cares about Privacy? -- 9.5 Privacy Controls -- 9.5.1 Access Controls -- 9.5.2 Anonymization -- 9.5.3 Differential Privacy -- 9.5.4 Homomorphic Encryption -- 9.5.5 Secure Multi-Party Computation -- 9.5.6 Zero-Knowledge and Group Signatures -- 9.5.7 Data Retention and Deletion Policy -- 9.6 Privacy Legislation -- 9.6.1 European Union Data Protection Directive -- 9.6.2 General Data Protection Regulation -- 9.6.3 California Consumer Privacy Act of 2018 -- 9.6.4 California Online Privacy Protection Act -- 9.6.5 Children's Online Privacy Protection Act of 1998 -- 9.6.6 Health Insurance Portability and Accountability Act of 1996 -- 9.7 The Future of Privacy Controls -- References -- Chapter 10 Security Usability: Human, Computer, and Security Interaction -- 10.1 Poor User Experience Design Isn't Just Inconvenient, It's Painful.

10.2 Nightmare at 40: When Too Many Convenient Devices Become Too Difficult to Manage -- 10.3 Challenges of IoT Security Usability -- 10.3.1 Security Doesn't Make Sense to the Regular User -- 10.3.2 Security Is Not Interesting to the Regular User -- 10.3.3 Usable Security Is Not Demanded from Vendors -- 10.3.4 Barriers to Necessary Workflow -- 10.3.5 Different Views of Security, from Executive to Architect to Implementer, Then the User -- 10.4 Principles for Designing Usable IoT Security Controls -- 10.5 The Cause of Usable Security Belongs to All of Us -- References -- Part Three -- Chapter 11 Earth 2040-Peeking at the Future -- 11.1 Whacking at the Future of IoT -- 11.2 The Fascination of Technology Innovation -- 11.2.1 Clairvoyance or Science? -- 11.2.2 Now -- 11.2.3 The Major Types of Change Introduced by IoT -- 11.3 The Evolving Cyber Threat Landscape -- 11.3.1 Threat Agents and Cyberattackers of the Future: AI and ML -- 11.4 A Vision of 2040 -- 11.4.1 Healthcare -- 11.4.2 Agriculture -- 11.4.3 Cities and Homes, Energy, and Autonomous Transportation -- 11.5 The Emergent Future of Cloud Computing -- 11.5.1 Infrastructure as Code -- 11.5.2 Serverless Architecture -- 11.5.3 Elastic Container-Based Cloud -- 11.5.4 Autoscaling -- 11.5.5 Summarizing the Security Advantages of Emergent Trends in Cloud Computing -- 11.6 Do the Right Thing and the Future Will Take Care of Itself -- References -- Epilogue -- Index.

Sommario/riassunto

This book describes how to architect and design Internet of Things (IoT) solutions that provide end-to-end security and privacy at scale. It

is unique in its detailed coverage of threat analysis, protocol analysis, secure design principles, intelligent loT's impact on privacy, and the effect of usability on security. The book also unveils the impact of digital currency and the dark web on the loT-security economy. It's both informative and entertaining. "Filled with practical and relevant examples based on years of experience ... with lively discussions and storytelling related to loT security design flaws and architectural issues."-- Dr. James F. Ransome, Senior Director of Security Development Lifecycle (SOL) Engineering, Intel 'There is an absolute treasure trove of information within this book that will benefit anyone, not just the engineering community. This book has earned a permanent spot on my office bookshelf."-- Erv Comer, Fellow of Engineering, Office of Chief Architect Zebra Technologies 'The importance of this work goes well beyond the engineer and architect. The IoT Architect's Guide to Attainable Security & Privacy is a crucial resource for every executive who delivers connected products to the market or uses connected products to run their business."-- Kurt Lee, VP Sales and Strategic Alliances at PWNIE Express "If we collectively fail to follow the advice described here regarding loT security and Privacy, we will continue to add to our mounting pile of exploitable computing devices. The attackers are having a field day. Read this book, now."-- Brook S.E. Schoenfield, Director of Advisory Services at IOActive, previously Master Security Architect at McAfee, and author of Securing Systems