1. Record Nr.	UNISA996466447103316
Titolo	Security Protocols XXIII [[electronic resource]] : 23rd International Workshop, Cambridge, UK, March 31 - April 2, 2015, Revised Selected Papers / / edited by Bruce Christianson, Petr Švenda, Vashek Matyas, James Malcolm, Frank Stajano, Jonathan Anderson
Pubbl/distr/stampa	Cham : , : Springer International Publishing : , : Imprint : Springer, , 2015
ISBN	3-319-26096-0
Edizione	[1st ed. 2015.]
Descrizione fisica	1 online resource (XI, 367 p. 38 illus. in color.)
Collana	Security and Cryptology ; ; 9379
Disciplina	005.8
Soggetti	Computer security Data encryption (Computer science) Management information systems Computer science Computer communication systems Systems and Data Security Cryptology Management of Computing and Information Systems Computer Communication Networks
Lingua di pubblicazione	Inglese
Formato	Materiale a stampa
Livello bibliografico	Monografia
Note generali	Includes index.
Nota di contenuto	Intro -- Preface -- Previous Proceedings in This Series -- Introduction: Information Securityin Fiction and in Fact(Transcript of Discussion) -- Contents -- The Dark Side of the Code -- 1 Introduction -- 2 Contemporary Application Development -- 3 Securing What Is Understood -- 4 The Security Gap -- 5 Verifying Expectation -- 6 Conclusion -- References -- The Dark Side of the Code (Transcript of Discussion) -- Redesigning Secure Protocols to Compel Security Checks -- 1 Overview -- 2 Example -- 3 Generalization -- 3.1 Inequality Checks -- 3.2 Combining Checks -- 3.3 Equivalent Encoding Check -- 4 Related Works -- 5 Conclusion -- 5.1 Future Work -- References -- Redesigning Secure Protocols to Compel Security Checks (Transcript of Discussion) -- References -- Derailing Attacks -- 1 Introduction -- 2

Derailing Attacks in Practice -- 3 Thwarting Derailing Attacks -- 4 Conclusion -- References -- Derailing Attacks (Transcript of Discussion) -- Establishing Software-Only Root of Trust on Embedded Systems: Facts and Fiction -- 1 Introduction -- 2 Software-Only Root of Trust -- 2.1 Architecture and Protocol -- 2.2 Known Attacks Against SWATT -- 3 New Attacks Against the SWORT Protocol -- 3.1 Future-Posted Event Attacks -- 3.2 Attacks Exploiting High Execution-Time Variance -- 3.3 Attacks Exploiting I-cache Inconsistency -- 4 Checksum and Attack Implementation -- 4.1 Checksum Function -- 4.2 WDT Reset Attack Implementation -- 4.3 Feasibility of the Time-Variance Based Attack -- 5 Challenges for Effective Countermeasures -- 6 Related Work -- 7 Conclusions -- References -- Establishing Software-Only Root of Trust on Embedded Systems: Facts and Fiction (Transcript of Discussion) -- References -- Mind Your (R,)s: Location-Based Privacy Controls for Consumer Drones -- 1 Introduction -- 2 Privacy and Security Challenges of Widespread use of Drones.

3 Policy-Based Location Access Control -- 4 Towards a Practical Realization -- 5 Enforcement? -- 6 Privacy Preserving Traffic Management for Consumer Drones -- 7 Related Work -- 8 Conclusion -- References -- Mind Your (R,)s: Location-Based Privacy Controls for Consumer Drones (Transcript of Discussion)

-- Location-Private Interstellar Communication -- 1 Introduction -- 2 To Communicate or Not to Communicate? -- 3 Adversary Model -- 3.1 Adversary Types -- 3.2 Technological Capabilities -- 4 Envisioned Controls for Location Privacy -- 4.1 Private Communication Probes -- 4.2 Random Relay Network -- 4.3 Some General Observations on Privacy Controls -- 5 Additional Security Requirements -- 6 Conclusions -- References -- Location-Private Interstellar Communication (Transcript of Discussion) -- The Lifetime of Android API Vulnerabilities: Case Study on the JavaScript-to-Java Interface -- 1 Introduction -- 2 API Vulnerabilities in Android -- 3 Case Study: The JavaScript-to-Java Interface Vulnerability -- 3.1 Threat Model -- 3.2 Sources of Vulnerability -- 3.3 Lifetime of the Vulnerability -- 3.4 Solutions -- 4 Related Work -- 5 Conclusion -- References -- The Lifetime of Android API Vulnerabilities: Case Study on the JavaScript-to-Java Interface (Transcript of Discussion) -- References -- Challenges of Fiction in Network Security -- Perspective of Virtualized Environments -- 1 Background -- 2 Our Framework -- 2.1 Workflow -- 3 Scenarios -- 3.1 HTTP Requests -- 3.2 HTTP Requests -- Lessons Learned -- 3.3 Slow Attacks -- 4 Open Questions -- 5 Summary -- References -- Challenges of Fiction in Network Security -- Perspective of Virtualised Environments (Transcript of Discussion) -- Device Attacker Models: Fact and Fiction -- 1 Introduction -- 2 Overview -- 3 Application to SSH -- 3.1 The Problem -- 3.2 The Solution.

3.3 The Public Log Structure and Proofs -- 3.4 Security Discussion -- 4 Conclusion -- References -- Device Attacker Models: Fact and Fiction (Transcript of Discussion) -- Smearing Fingerprints: Changing the Game of Web Tracking with Composite Privacy -- 1 Introduction -- 2 Discussion -- 3 Related Work -- 4 Conclusion -- References -- Smearing Fingerprints: Changing the Game of Web Tracking and Differential Privacy (Transcript of Discussion) -- Pico Without Public Keys -- 1 Introduction: A Motivating Story -- 2 Objective -- 3 The Core Idea -- 3.1 A Small Leftover Problem -- 4 Web Login Without Public Keys -- 4.1 Revocation on the Web Today -- 4.2 TLS Without Public Key, but with Revocation -- 4.3 Avoiding Unnecessary Re-Registration -- 5 Pico Without Public Keys -- 5.1 Levels of Pico Compliance -- 5.2 And When the Token Is Not Available? -- 5.3 How Should Pico Evolve? -- 6 Conclusions -- References -- Pico Without Public Keys (Transcript of Discussion) -- Do You Believe in Tinker Bell? The Social Externalities of Trust -- 1 Introduction -- 2 Motivation -- 3 System Design -- 3.1 Member Registration -- 3.2 A Simple Threat Model -- 3.3 A More Realistic Threat Model -- 3.4 Payment System -- 3.5 Generating Trust and Reputation Metrics -- 4 Discussion -- 4.1 Mitigating Collusions and Malicious Members -- 4.2 Mitigating Sybil Attacks -- 4.3 Security Economics -- 5 Related Work -- 6 Conclusion -- References -- Do You Believe in Tinker Bell? The Social Externalities of Trust (Transcript of Discussion) -- Security is Beautiful -- 1 Introduction -- 2 Position -- 3 Conclusions -- References -- Security is Beautiful (Transcript of Discussion) -- On the Use of Security and Privacy Technology as a Plot Device -- 1 Introduction -- 2 Talk Summary -- References -- On the Use of Security and Privacy Technology as a Plot Device (Transcript of Discussion).

Bitcoin: Perils of an Unregulated Global P2P Currency -- 1 Introduction -- 2 Bitcoin and Crime -- 2.1 Dark Markets -- 2.2 Theft and Malware -- 3 Future Threats -- 4 Discussion -- 5 Conclusion -- References -- Bitcoin: Perils of an Unregulated Global P2P Currency (Transcript of Discussion) -- Will Technology Make Information Security Impossible? And Must Technology Be Invented Just Because We Can? -- 1 Introduction -- 2 Plots of the Works -- 2.1 The Productions of Time -- 2.2 The Dead Past -- 3 Implications of These Inventions -- What Are the Threats? -- 3.1 Threats to Secrecy -- 3.2 Threats to Integrity -- 4 Potential Solutions -- and One Problem Solved? -- 5 Wider Implications -- References -- Will Technology Make Information Security Impossible? And Must Technology Be Invented Just Because We Can? (Transcript of Discussion) -- Information Leakage Due to Revealing Randomly Selected Bits -- 1 Introduction -- 2 Problem Statement -- 2.1 Notation -- 2.2 Related Work -- 2.3 Entropy Measures -- 3 Information Leakage -- 3.1 Cardinality of the Uncertainty Set -- 3.2 Shannon Entropy -- 3.3 Minimal Shannon Entropy -- 3.4 Minimal Renyi Entropy -- 3.5 Min-Entropy -- 3.6 Maximum Entropy -- 4 Privacy Amplification and Alternative Approaches -- 4.1 Privacy Amplification -- 4.2 Kolmogorov-Chaitin Complexity -- 4.3 Estimating Expected Leakage -- 4.4 Duality: Subsequences vs. Supersequences -- 5 Simulations -- 5.1 Methodology -- 5.2 Results Discussion -- 6 Conclusions -- References -- Information Leakage Due to Revealing Randomly Selected Bits (Transcript of Discussion) -- Efficient Data Intensive Secure Computation: Fictional or Real? -- 1 Introduction -- 2 Private Set Intersection: Background -- 3 Data Structural Approach -- 3.1 From Bloom Filter to Garbled Bloom Filter -- 3.2 Performance Comparison -- 4 Fully Homomorphic Encryption Approach.

4.1 The BGV FHE Scheme -- 4.2 Polynomial Representation of a Set -- 4.3 The Private Set Intersection Protocol Based on FHE -- 4.4 Efficiency -- 5 Conclusion -- References -- Efficient Data Intensive Secure Computations: Fictional or Real? (Transcript of Discussion) -- Epilogue -- Author Index.

Sommario/riassunto

This book constitutes the thoroughly refereed post-workshop proceedings of the 23rd International Workshop on Security Protocols, held in Cambridge, UK, in March/April 2015. After an introduction the volume presents 18 revised papers each followed by a revised transcript of the presentation and ensuing discussion at the event. The theme of this year's workshop is "Information Security in Fiction and in Fact".