2010 23rd IEEE Computer Security Foundations Symposium

(CSF 2010)

Edinburgh, United Kingdom
17 – 19 July 2010

IEEE

IEEE Catalog Number: CFP10037-PRT
ISBN: 978-1-4244-7510-0

23rd IEEE Computer Security Foundations Symposium

CSF 2010

Table of Contents

Preface ..... **viii**
Committees ..... **ix**
Reviewers ..... **xi**

Session 1: Quantitative Security

Approximation and Randomization for Quantitative Information-Flow Analysis 3
Boris Köpf and Andrey Rybalchenko

Quantitative Information Flow - Verification Hardness and Possibilities 15
Hirotoshi Yasuoka and Tachio Terauchi

Quantification of Integrity 28
Michael R. Clarkson and Fred B. Schneider

Vulnerability Bounds and Leakage Resilience of Blinded Cryptography under Timing Attacks 44
Boris Köpf and Geoffrey Smith

Session 2: Security Protocol Verification I

Modeling and Verifying Ad Hoc Routing Protocols 59
Mathilde Arnaud, Véronique Cortier, and Stéphanie Delaune

Formal Verification of Privacy for RFID Systems 75
Mayla Brusó, Konstantinos Chatzikokolakis, and Jerry den Hartog

Session 3: Privacy and Anonymity

Robustness Guarantees for Anonymity 91
Gilles Barthe, Alejandro Hevia, Zhengqin Luo, Tamara Rezk, and Bogdan Warinschi

Analysing Unlinkability and Anonymity Using the Applied Pi Calculus 107
Myrto Arapinis, Tom Chothia, Eike Ritter, and Mark Ryan

A Game-Based Definition of Coercion-Resistance and Its Applications 122
Ralf Küsters, Tomasz Truderung, and Andreas Vogt

Session 4: Authorization

Towards Quantitative Analysis of Proofs of Authorization: Applications, Framework, and Techniques 139
Adam J. Lee and Ting Yu

Constraining Credential Usage in Logic-Based Access Control 154
Lujo Bauer, Limin Jia, and Divya Sharma

Session 5: Information Flow

Information Flow in Credential Systems 171
Moritz Y. Becker

Dynamic vs. Static Flow-Sensitive Security Analysis 186
Alejandro Russo and Andrei Sabelfeld

Information Flow Monitor Inlining 200
Andrey Chudnov and David A. Naumann

Required Information Release 215
Stephen Chong

Five-Minute Talks

Session 6: Security Protocol Verification II

Strong Invariants for the Efficient Construction of Machine-Checked Protocol Security Proofs 231
Simon Meier, Cas Cremers, and David Basin

A Machine-Checked Formalization of Sigma-Protocols 246
Gilles Barthe, Daniel Hedin, Santiago Zanella Béguelin, Benjamin Grégoire, and Sylvain Heraud

Impossibility Results for Secret Establishment 261
Benedikt Schmidt, Patrick Schaller, and David Basin

Session 7: Security Specifications

A Framework for the Sound Specification of Cryptographic Tasks 277
Juan A. Garay, Aggelos Kiayias, and Hong-Sheng Zhou

Towards a Formal Foundation of Web Security..... 290
Devdatta Akhawe, Adam Barth, Peifung E. Lam, John Mitchell, and Dawn Song

Session 8: Language-Based Security

Automating Open Bisimulation Checking for the Spi Calculus 307
Alwen Tiu and Jeremy Dawson

Protocol Composition for Arbitrary Primitives 322
Stefan Ciobâca and Véronique Cortier

On Protection by Layout Randomization 337
Martín Abadi and Gordon Plotkin

Author Index 353