2014 IEEE 27th Computer Security Foundations Symposium

(CSF 2014)

Vienna, Austria
19 – 22 July 2014
Table of Contents

Preface........................................................................................................................................................viii
Vienna Summer of Logic Preface..............................................................................................................ix
Committees.................................................................................................................................................xii
External Reviewers...................................................................................................................................xiv

Software Security
Declarative Policies for Capability Control ...............................................................................................3
    Christos Dimoulas, Scott Moore, Aslan Askarov, and Stephen Chong
Portable Software Fault Isolation ................................................................................................................18
    Joshua A. Kroll, Gordon Stewart, and Andrew W. Appel
Certificates for Verifiable Forensics ............................................................................................................33
    Radha Jagadeesan, C.M. Lubinski, Corin Pitcher, James Riely, and Charles Winebrinner
Information Flow Monitoring as Abstract Interpretation for Relational Logic ............................................48
    Andrey Chudnov, George Kuan, and David A. Naumann

Information Flow I
On Dynamic Flow-Sensitive Floating-Label Systems ...............................................................................65
    Pablo Buiras, Deian Stefan, and Alejandro Russo
Noninterference under Weak Memory Models .........................................................................................80
    Heiko Mantel, Matthias Perner, and Jens Sauer

Usable Security
    Marian Harbach, Sascha Fahl, and Matthew Smith
How Task Familiarity and Cognitive Predispositions Impact Behavior in a Security Game of Timing
Jens Grossklags and David Reitter

Cryptography I
Attribute-Based Encryption for Access Control Using Elementary Operations
Jason Crampton and Alexandre Pinto

Automated Analysis and Synthesis of Block-Cipher Modes of Operation
Alex J. Malozemoff, Jonathan Katz, and Matthew D. Green

Certified Synthesis of Efficient Batch Verifiers
Joseph A. Akinyele, Gilles Barthe, Benjamin Grégoire, Benedikt Schmidt, and Pierre-Yves Strub

Cryptography II
A Peered Bulletin Board for Robust Use in Verifiable Voting Systems
Chris Culnane and Steve Schneider

From Input Private to Universally Composable Secure Multi-party Computation
Primitives
Dan Bogdanov, Peeter Laud, Sven Laur, and Pille Pullonen

Malleable Signatures: New Definitions and Delegatable Anonymous Credentials
Melissa Chase, Markulf Kohlweiss, Anna Lysyanskaya, and Sarah Meiklejohn

Protocol Verification
Decidability for Lightweight Diffie-Hellman Protocols
Daniel J. Dougherty and Joshua D. Guttman

Modeling Diffie-Hellman Derivability for Automated Analysis
Moses Liskov and F. Javier Thayer

Actor Key Compromise: Consequences and Countermeasures
David Basin, Cas Cremers, and Marko Horvat

A Sound Abstraction of the Parsing Problem
Sebastian Mödersheim and Georgios Katsoris

Information Flow II
Compositional Information-Flow Security for Interactive Systems
Willard Rafnsson and Andrei Sabelfeld

Stateful Declassification Policies for Event-Driven Programs
Mathy Vanhoef, Willem De Groef, Dominique Devriese, Frank Piessens, and Tamara Rezk
Additive and Multiplicative Notions of Leakage, and Their Capacities ........................................308
  Mário S. Alvim, Konstantinos Chatzikokolakis, Annabelle Mciver,
  Carroll Morgan, Catuscia Palamidessi, and Geoffrey Smith

Network Security
The Complexity of Estimating Systematic Risk in Networks ........................................................325
  Benjamin Johnson, Aron Laszka, and Jens Grossklags
Automated Generation of Attack Trees .................................................................................337
  Roberto Vigo, Flemming Nielson, and Hanne Riis Nielson
Mignis: A Semantic Based Tool for Firewall Configuration ..................................................351
  P. Adão, C. Bozzato, G. Dei Rossi, R. Focardi, and F.L. Luccio
Provably Sound Browser-Based Enforcement of Web Session Integrity ..................................366
  Michele Bugliesi, Stefano Calzavara, Riccardo Focardi, Wilayat Khan,
  and Mauro Tempesta

Privacy I
TUC: Time-Sensitive and Modular Analysis of Anonymous Communication .........................383
  Michael Backes, Praveen Manoharan, and Esfandiar Mohammadi
Differential Privacy: An Economic Method for Choosing Epsilon ........................................398
  Justin Hsu, Marco Gaboardi, Andreas Haeberlen, Sanjeev Khanna,
  Arjun Narayanan, Benjamin C. Pierce, and Aaron Roth
Proving Differential Privacy in Hoare Logic ........................................................................411
  Gilles Barthe, Marco Gaboardi, Emilio Jesús Gallego Arias, Justin Hsu,
  César Kunz, and Pierre-Yves Strub

Privacy II
Balancing Societal Security and Individual Privacy: Accountable Escrow System ..................427
  Jia Liu, Mark D. Ryan, and Liqun Chen

Author Index ..........................................................................................................................441