

2014 IEEE 27th Computer Security Foundations Symposium

(CSF 2014)

**Vienna, Austria
19 – 22 July 2014**



IEEE Catalog Number: CFP14037-POD
ISBN: 978-1-4799-4289-3

2014 IEEE 27th Computer Security Foundations Symposium

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

Information Flow I

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

Usable Security

Who's Afraid of Which Bad Wolf? A Survey of IT Security Risk Awareness	97
<i>Marian Harbach, Sascha Fahl, and Matthew Smith</i>	

How Task Familiarity and Cognitive Predispositions Impact Behavior in a Security Game of Timing	111
<i>Jens Grossklags and David Reitter</i>	

Cryptography I

Attribute-Based Encryption for Access Control Using Elementary Operations	125
<i>Jason Crampton and Alexandre Pinto</i>	
Automated Analysis and Synthesis of Block-Cipher Modes of Operation	140
<i>Alex J. Malozemoff, Jonathan Katz, and Matthew D. Green</i>	
Certified Synthesis of Efficient Batch Verifiers	153
<i>Joseph A. Akinyele, Gilles Barthe, Benjamin Grégoire, Benedikt Schmidt, and Pierre-Yves Strub</i>	

Cryptography II

A Peered Bulletin Board for Robust Use in Verifiable Voting Systems	169
<i>Chris Culnane and Steve Schneider</i>	
From Input Private to Universally Composable Secure Multi-party Computation Primitives	184
<i>Dan Bogdanov, Peeter Laud, Sven Laur, and Pille Pullonen</i>	
Malleable Signatures: New Definitions and Delegatable Anonymous Credentials	199
<i>Melissa Chase, Markulf Kohlweiss, Anna Lysyanskaya, and Sarah Meiklejohn</i>	

Protocol Verification

Decidability for Lightweight Diffie-Hellman Protocols	217
<i>Daniel J. Dougherty and Joshua D. Guttman</i>	
Modeling Diffie-Hellman Derivability for Automated Analysis	232
<i>Moses Liskov and F. Javier Thayer</i>	
Actor Key Compromise: Consequences and Countermeasures	244
<i>David Basin, Cas Cremers, and Marko Horvat</i>	
A Sound Abstraction of the Parsing Problem	259
<i>Sebastian Mödersheim and Georgios Katsoris</i>	

Information Flow II

Compositional Information-Flow Security for Interactive Systems	277
<i>Willard Rafnsson and Andrei Sabelfeld</i>	
Stateful Declassification Policies for Event-Driven Programs	293
<i>Mathy Vanhoef, Willem De Groef, Dominique Devriese, Frank Piessens, and Tamara Rezk</i>	

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 Narayan, 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
---------------------------	-----