

2015 IEEE Security and Privacy Workshops

(SPW 2015)

**San Jose, California, USA
21-22 May 2015**



IEEE Catalog Number: CFP15SPX-POD
ISBN: 978-1-4799-9934-7

2015 IEEE CS Security and Privacy Workshops

SPW 2015

Table of Contents

Message from the Chair.....	viii
GenoPri 2015 Organizers.....	x
LangSec 2015 Organizers.....	xii
IWPE 2015 Organizers.....	xiii

2nd International Workshop on Genome Privacy and Security (GenoPri'15)

Cryptographic Approaches to Privacy

Efficient Secure Outsourcing of Genome-Wide Association Studies	3
<i>Wenjie Lu, Yoshiji Yamada, and Jun Sakuma</i>	
Privacy-Preserving Statistical Analysis by Exact Logistic Regression	7
<i>David A. Duverle, Shohei Kawasaki, Yoshiji Yamada, Jun Sakuma, and Koji Tsuda</i>	

Miscellaneous

Passing Go with DNA Sequencing: Delivering Messages in a Covert Transgenic Channel	17
<i>Ji Young Chun, Hye Lim Lee, and Ji Won Yoon</i>	
Privacy Threats and Practical Solutions for Genetic Risk Tests	27
<i>Ludovic Barman, Mohammed-Taha Elgraini, Jean Louis Raisaro, Jean-Pierre Hubaux, and Erman Ayday</i>	

Measuring Genome Privacy

Quantifying Genomic Privacy via Inference Attack with High-Order SNV Correlations	32
<i>Sahel Shariati Samani, Zhicong Huang, Erman Ayday, Mark Elliot, Jacques Fellay, Jean-Pierre Hubaux, and Zoltán Kutzlik</i>	

One Size Doesn't Fit All: Measuring Individual Privacy in Aggregate Genomic Data	41
<i>Sean Simmons and Bonnie Berger</i>	
Genomic Privacy Metrics: A Systematic Comparison	50
<i>Isabel Wagner</i>	

Policy, Law, and Genomic Privacy

Genomic Privacy and Direct-to-Consumer Genetics: Big Consumer Genetic Data – What's in that Contract?	60
<i>Andelka M. Phillips</i>	
Seeking a "Race to the Top" in Genomic Cloud Privacy?	65
<i>Mark Phillips, Bartha M. Knoppers, and Yann Joly</i>	

Second Workshop on Language-Theoretic Security (LangSec'15)

First Session: Papers

The Correctness-Security Gap in Compiler Optimization	73
<i>Vijay D'Silva, Mathias Payer, and Dawn Song</i>	
Grammatical Inference and Language Frameworks for LANGSEC	88
<i>Dr. Kerry N. Wood and Dr. Richard E. Harang</i>	
Error-Correcting Codes as Source for Decoding Ambiguity	99
<i>Adrian Dabrowski, Isao Echizen, and Edgar R. Weippl</i>	
Verification State-Space Reduction through Restricted Parsing Environments	106
<i>Jacob I. Torrey and Mark P. Bridgman</i>	

Second Session: Research Reports

On the Generality and Convenience of Etypes	117
<i>W. Michael Petullo and Joseph Suh</i>	
Protocol State Machines and Session Languages: Specification, implementation, and Security Flaws	125
<i>Erik Poll, Joeri De Ruiter, and Aleksy Schubert</i>	
Towards More Security in Data Exchange: Defining Unparsers with Context-Sensitive Encoders for Context-Free Grammars	134
<i>Lars Hermerschmidt, Stephan Kugelmann, and Bernhard Rumpe</i>	
Nom, A Byte oriented, streaming, Zero copy, Parser Combinators Library in Rust	142
<i>Geoffroy Couprie</i>	

2015 International Workshop on Privacy Engineering (IWPE'15)

Systematizing Privacy Engineering Goals

PRIPARE: Integrating Privacy Best Practices into a Privacy Engineering Methodology	151
<i>Nicolás Notario, Alberto Crespo, Yod-Samuel Martín, Jose M. Del Alamo, Daniel Le Métayer, Thibaud Antignac, Antonio Kung, Inga Kroener, and David Wright</i>	
Protection Goals for Privacy Engineering	159
<i>Marit Hansen, Meiko Jensen, and Martin Rost</i>	
Privacy by Design in Federated Identity Management	167
<i>Rainer Hörbe and Walter Hötzendorfer</i>	

Technologies for User-Management of Privacy

Extending the Power of Consent with User-Managed Access: A Standard Architecture for Asynchronous, Centralizable, Internet-Scalable Consent	175
<i>Eve Maler</i>	
Decentralizing Privacy: Using Blockchain to Protect Personal Data	180
<i>Guy Zyskind, Oz Nathan, and Alex 'Sandy' Pentland</i>	

Surveillance, Privacy and Infrastructure

Reviewing for Privacy in Internet and Web Standard-Setting	185
<i>Nick Doty</i>	
Privacy Principles for Sharing Cyber Security Data	193
<i>Gina Fisk, Calvin Ardi, Neale Pickett, John Heidemann, Mike Fisk, and Christos Papadopoulos</i>	

Evaluating Engineering Methods for PETs

Choose Wisely: A Comparison of Secure Two-Party Computation Frameworks	198
<i>Jan Henrik Ziegeldorf, Jan Metzke, Martin Henze, and Klaus Wehrle</i>	
Tor Experimentation Tools	206
<i>Fatemeh Shirazi, Matthias Goehring, and Claudia Diaz</i>	
Author Index	215