# ESORICS 2012

# 17th European Symposium on Research in Computer Security

## MONDAY, SEPTEMBER 10TH

### 09:00-10:15 *plenary session*

**AUDITORIUM**

- Welcome and opening
- **Invited Talk:** Mind the Gap: Smart Phone Security and Privacy in Theory and Practice *by Ahmad-Reza Sadeghi*

### 10:45-12:45 *parallel sessions*

**AUDITORIUM**

**Session 1A:** Security and data protection in real systems (chair: Amir Herzberg)

- Modeling and Enhancing Android's Permission System *by Elli Fragkaki, Lujo Bauer, Limin Jia and David Swasey*
- Hardening Access Control and Data Protection in GFS-like File Systems *by James Kelley, Roberto Tamassia and Nikos Triandopoulos*
- Attack of the Clones: Detecting Cloned Applications on Android Markets *by Jonathan Crussell, Clint Gibler and Hao Chen*
- Boosting the Permissiveness of Dynamic Information-Flow Tracking by Testing *by Arnar Birgisson, Daniel Hedin and Andrei Sabelfeld*

**ROOM 27**

**Session 1B:** Formal models for cryptography and access control (chair: Luigi Mancini)

- Effective Symbolic Protocol Analysis via Equational Irreducibility Conditions *by Serdar Erbatur, Santiago Escobar, Deepak Kapur, Zhiqiang Liu, Christopher Lynch, Catherine Meadows, Jose Meseguer, Paliath Narendran, Sonia Santiago and Ralf Sasse*
- Deciding Epistemic and Strategic Properties of Cryptographic Protocols *by Henning Schnoor*
- Satisfiability and Feasibility in a Relationship-based Workflow Authorization Model *by Arif Khan and Philip Fong*
- Deciding Security for a Fragment of ASLan *by Sebastian A. Mödersheim*

### 14:15-15:45 *parallel sessions*

**AUDITORIUM**

**Session 2A:** Security and privacy in mobile and wireless networks (chair: Roberto Di Pietro)

- A Probabilistic Framework for Localization of Attackers in MANETs *by Massimiliano Albanese, Alessandra De Benedictis, Sushil Jajodia and Paulo Shakarian*
- Robust Probabilistic Fake Packet Injection for Receiver-Location Privacy in WSN *by Ruben Rios, Jorge Cuellar and Javier Lopez*
- Privacy-Aware Message Exchanges for Geographically Routed Human Movement Networks *by Adam Aviv, Micah Sherr, Matt Blaze and Jonathan Smith*

**ROOM 27**

**Session 2B:** Counteracting Man-in-the-Middle attacks (chair: Lujo Bauer)

- Trust No One Else: Detecting MITM Attacks Against SSL/TLS without Third-Parties *by Italo Dacosta, Mustaque Ahamad and Patrick Traynor*
- X.509 Forensics: Detecting and Localising the SSL/TLS Men-in-the-middle *by Ralph Holz, Thomas Riedmaier, Nils Kammenhuber and Georg Carle*
- A Practical Man-In-The-Middle Attack on Signal-based Key Generation Protocols *by Simon Eberz, Martin Strohmeier, Matthias Wilhelm and Ivan Martinovic*

### 16:15-17:45 *parallel sessions*

**AUDITORIUM**

**Session 3A:** Network security (chair: Ivan Martinovic)

- The Silence of the LANs: Efficient Leakage Resilience for IPsec VPNs *by Ahmad-Reza Sadeghi, Steffen Schulz and Vijay Varadharajan*
- Security of Patched DNS *by Amir Herzberg and Haya Shulman*
- Revealing Abuses of Channel Assignment Protocols in Multi-Channel Wireless Networks: An Investigation Logic Approach *by Qijun Gu, Kyle Jones, Wanyu Zang, Meng Yu and Peng Liu*

**ROOM 27**

**Session 3B:** Users privacy and anonymity (chair: Einar Snekkenes)

- Exploring Linkability of User Reviews *by Misbah Almishari and Gene Tsudik*
- Formal Analysis of Privacy in an eHealth Protocol *by Naipeng Dong, Hugo Jonker and Jun Pang*
- PRIVATUS: Wallet-Friendly Privacy Protection for Smart Meters *by Jinkyu Koo, Xiaojun Lin and Saurabh Bagchi*

## TUESDAY, SEPTEMBER 11TH

### 09:15-10:15 *plenary session*

**AUDITORIUM**

- **Invited Talk:** Computer-Aided Cryptographic Proofs and Designs *by Gilles Barthe*

### 10:45-12:45 *parallel sessions*

**AUDITORIUM**

**Session 4A:** Location privacy (chair: Keith Frikken)

- SHARP: Private Proximity Test and Secure Handshake with Cheat-Proof Location Tags *by Yao Zheng, Ming Li, Wenjing Lou and Y Thomas Hou*
- Secure Proximity Detection for NFC Devices based on Ambient Sensor Data *by Tzipora Halevi, Di Ma, Nitesh Saxena and Tuo Xiang*
- Enhancing Location Privacy for Electric Vehicles (at the Right Time) *by Joseph Liu, Man Ho Au, Willy Susilo and Jianying Zhou*
- Design and Implementation of a Terrorist Fraud Resilient Distance Bounding System *by Aanjhan Ranganathan, Nils Ole Tippenhauer, Boris Skoric, Dave Singelee and Srdjan Capkun*

**ROOM 27**

**Session 4B:** Voting protocols and anonymous communication (chair: Mirek Kutylowski)

- Applying Diverifiability to Blind Ballot Copying in the Helios Internet Voting System *by Yvo Desmedt and Pyrmos Chaidos*
- Defining Privacy for Weighted Votes, Single and Multi-Voter Coercion *by Jannik Dreier, Pascal Lafourcade and Yassine Lakhnech*
- TorScan: Tracing Long-lived Connections and Differential Scanning Attacks *by Alex Biryukov, Ivan Pustogarov and Ralf Philipp Weinmann*
- Introducing the qMix Open Source Framework for Mix Implementations *by Karl-Peter Fuchs, Dominik Herrmann and Hannes Federrath*

### 14:15-15:45 *parallel sessions*

**AUDITORIUM**

**Session 5A:** Private computation in cloud systems (chair: Emiliano De Cristofaro)

- Secure and Efficient Outsourcing of Sequence Comparisons *by Marina Blanton, Mikhail J. Atallah, Keith B. Frikken and Qutaibah Malluhi*
- Third-Party Private DFA Evaluation on Encrypted Files in the Cloud *by Lei Wei and Michael Reiter*
- New Algorithms for Secure Outsourcing of Modular Exponentiations *by Xiaofeng Chen, Jin Li, Jianfeng Ma, Qiang Tang and Wenjing Lou*

**ROOM 27**

**Session 5B:** Formal security models (chair: Gilles Barthe)

- Towards Symbolic Encryption Schemes *by Naveed Ahmed, Christian Damsgaard Jensen and Erik Zenner*
- Decision Procedures for Simulatability *by Charanjit Jutla and Arnab Roy*
- Model-Checking Bisimulation-based Information Flow Properties for Infinite State Systems *by Deepak D'Souza and K. R. Raghavendra*

### 16:15-17:45 *parallel sessions*

**AUDITORIUM**

**Session 6A:** Identity based encryption and group signature (chair: Joachim Posegga)

- Identity-Based Traitor Tracing with Short Private Key and Short Ciphertext *by Fuchun Guo, Yi Mu and Willy Susilo*
- Identity-Based Encryption with Master Key-Dependent Message Security and Leakage-Resilience *by David Galindo, Javier Herranz and Jorge Villar*
- Unique Group Signatures *by Matthew Franklin and Haibin Zhang*

**ROOM 27**

**Session 6B:** Authentication (chair: Nora Cuppens)

- Relations among Notions of Privacy for RFID Authentication Protocols *by Daisuke Moriyama, Shin'ichiro Matsuo and Miyako Ohkubo*
- PEARY2: Privacy-Enhanced Anonymous Authentication with Reputation and Revocation *by Kin Ying Yu, Tsz Hon Yuen, Sherman S.M. Chow, S.M. Yiu and Lucas C.K. Hui*
- Dismantling iClass and iClass Elite *by Flavio D. Garcia, Gerhard de Koning Gans, Roel Verdult and Milosch Meriac*

## WEDNESDAY, SEPTEMBER 12TH

### 09:00-10:15 *plenary session*

**AUDITORIUM**

- **Invited Talk:** Integrity of Storage and Computations in the Cloud *by Christian Cachin*

### 10:45-12:45 *plenary session*

**AUDITORIUM**

**Session 7:** Encryption key and password security (chair: Joaquin Garcia-Alfaro)

- Evaluation of Standardized Password-based Key Derivation against Parallel Processing Platforms *by Markus Dürmuth, Tim Güneysu, Markus Kasper, Christof Paar, Tolga Yalcin and Ralf Zimmermann*
- Beyond eCK: Perfect Forward Secrecy under Actor Compromise and Ephemeral-Key Reveal *by Cas Cremers and Michele Feltz*
- Bleichenbacher's Attack Strikes Again: Breaking PKCS#1 v1.5 in XML Encryption *by Tibor Jager, Sebastian Schinzel and Juraj Somorovsky*
- On The Security of Password Manager Database Formats *by Paolo Gasti and Kasper Rasmussen*

### 14:15-15:45 *plenary session*

**AUDITORIUM**

**Session 8:** Malware and phishing (chair: Frédéric Cuppens)

- Scalable Telemetry Classification for Automated Malware Detection *by Jack Stokes, John Platt, Helen Wang, Joe Faulhaber, Jonathan Keller, Mady Marinescu, Anil Thomas and Marius Gheorghescu*
- Abstraction-based Malware Analysis Using Rewriting and Model Checking *by Philippe Beaucamps, Isabelle Gnaedig and Jean-Yves Marion*
- Detecting Phishing Emails the Natural Language Way *by Rakesh Verma, Narasimha Shashidhar and Nabil Hossain*

### 16:15-17:45 *plenary session*

**AUDITORIUM**

**Session 9:** Software security (chair: Dieter Gollmann)

- JVM-Portable Sandboxing of Java's Native Libraries *by Mengtao Sun and Gang Tan*
- Codejail: Application-transparent Isolation of Libraries with Tight Program Interactions *by Yongzheng Wu, Sai Sathyanarayan Venkatraman, Roland Yap and Zhenkai Liang*
- SocialImpact: Systematic Analysis of Underground Social Dynamics *by Ziming Zhao, Gail-Joon Ahn, Hongxin Hu and Deepinder Mahi*

GRAPHIC DESIGN: Patrizia Andreoni - IIT - CNR, Italy

Istituto di Informatica e Telematica
NESSoS
technicolor

**10-14 September 2012 - CNR Research Area of Pisa, Italy**