ESORICS 2014

The number of submitted papers was 234, two papers have been withdrawn before notification time, 58 papers have been accepted for presentation. The acceptance rate of ESORICS 2014 was 24.79%.

PROGRAM OF ESORICS 2014

Venue: Building D20 (Congres Center of Wrocław University of Technology), Janiszewskiego 8
Registration desk will be open on Saturday, 6.09.2014, from 16:40 to 20:00. Welcome drink will be offered.

	7.09.2014		8.09.2014		9.09.2014	
8:30 - 9:00	Registration		Registration		Registration	
9:00 - 10:00	Invited talk 1 Room 10D		Invited talk 2 Room 10D		Invited talk 3 Room 10D	
10:00 - 11:15	Network Security Room 10B	Cryptography and Practice Room 10D	Privacy Aware Computing Room 10B	Cryptography 1 Room 10D	Code Analysis Room 10B	Password Authentication Room 10D
11:15 - 11:45	Coffee Break		Coffee Break		Coffee Break	
11:45-13:00	Cloud Computing 1 Room 10D		Attribute Based Cryptography Room 10B	Cryptography 2 Room 10D	E-voting and E-cash Room 10D	
13:00 - 14:30	Lunch Break		Lunch Break		Lunch Break	
14:30-16:10	Mobile Devices and Hardware Security Room 10B	Cloud Computing 2 Room 10D	Privacy Panel Room 10B	Secure Wireless Communication Room 10D	Attack Detection and Defence 1 Room 10D	
16:10 - 16:40	Coffee Break		Coffee Break		Coffee Break	
16:40 - 18:20	Cloud Computing 3 Room 10D		Privacy Room 10D		Attack Detection and Defence 2 Room 10D	
evening	Snack + time for a city walk SC Meeting		Conference Dinner		Industrial Reception	

ESORICS 2014

PROGRAM DETAILS

7.09.2014

Invited Talk 1

chair: Jaideep Vaidya

- Authenticating vehicles on the fly
  Shlomi Dolev

Network Security

chair: Einar Snekkenes

- Detecting Malicious Domains via Graph Inference,
  Pratyusa K. Manadhata, Sandeep Yadav, Prasad Rao, William Horne
- Empirically Measuring WHOIS Misuse
  Nektarios Leontiadis, Nicolas Christin
- EncDNS: A Lightweight Privacy-Preserving Name Resolution Service
  Dominik Herrmann, Karl-Peter Fuchs, Jens Lindemann, Hannes Federrath

Cryptography and Practice

chair: Robert Deng

- Ubic - Bridging the Gap between Digital Cryptography and the Physical World
  Mark Simkin, Dominique Schröder, Andreas Bulling, Mario Fritz
- Updaticator: Updating Billions of Devices by an Efficient, Scalable and Secure Software Update Distribution Over Untrusted Cache-enabled Networks
  Moreno Ambrosin, Christoph Busold, Mauro Conti, Ahmad-Reza Sadeghi, Matthias Schunter
- Local Password Validation using Self-Organizing Maps
  Diogo Mónica, Carlos Ribeiro

Cloud Computing 1

chair: Marek Klonowski

- Verifiable Delegation of Computations with Storage-Verification Trade-off
  Liang Feng Zhang, Reihaneh Safavi-Naini
- Who Is Touching My Cloud?
  Hua Deng, Qianhong Wu, Bo Qin, Jian Mao, Xiao Liu, Lei Zhang, Wenchang Shi
- Verifiable Computation over Large Database with Incremental Updates
  Xiaofeng Chen, Jin Li, Jian Weng, Jianfeng Ma, Wenjing Lou

Mobile Devices and Hardware Security

chair: Shlomi Dolev

- DroidMiner: Automated Mining and Characterization of Fine-grained Malicious Behaviors in Android Applications
  Chao Yang, Zhaoyan Xu, Guofei Gu, Vinod Yegneswaran, Phil Porras
- Detecting Targeted Smartphone Malware with Behavior-Triggering Stochastic Models
  Guillermo Suarez-Tangil, Mauro Conti, Juan E. Tapiador, Pedro Peris-Lopez
- TrustDump: Reliable Memory Acquisition on Smartphones
  He Sun, Kun Sun, Yuewu Wang, Jiwu Jing, Sushil Jajodia
- A Framework to Secure Peripherals at Runtime
  Fengwei Zhang, Haining Wang, Kevin Leach, Angelos Stavrou

Cloud Computing 2

chair: Xiaofeng Chen

- StealthGuard: Proofs of Retrievability with Hidden Watchdogs
  Monir Azraoui, Kaoutar Elkhiyaoui, Refik Molva, Melek Önen
- An Efficient Cloud-based Revocable Identity-based Proxy Re-encryption Scheme for Public Clouds Data Sharing
  Kaitai Liang, Joseph K. Liu, Duncan S. Wong, Willy Susilo
- Verifiable Computation on Outsourced Encrypted Data
  Junzuo Lai, Robert H. Deng, Hweehwa Pang, Jian Weng
- Verifiable Computation with Reduced Informational Costs and Computational Costs
  Gang Xu, George T. Amariucai, Yong Guan

Cloud Computing 3

chair: Reihaneh Safavi-Naini

- Detangling Resource Management Functions from the TCB in Privacy-Preserving Virtualization
  Min Li, Zili Zha, Wanyu Zang, Meng Yu, Peng Liu, Kun Bai
- Securely Outsourcing Exponentiations with Single Untrusted Program for Cloud Storage
  Yujue Wang, Qianhong Wu, Duncan S. Wong, Bo Qin, Sherman S. M. Chow, Zhen Liu, Xiao Tan
- Quantitative Workflow Resiliency
  John C. Mace, Charles Morisset, Aad van Moorsel
- Identity-based Encryption with Post-Challenge Auxiliary Inputs for Secure Cloud Applications and Sensor Networks
  Tsz Hon Yuen, Ye Zhang, Siu Ming Yiu, Joseph K. Liu

8.09.2014

Invited Talk 2

chair: Pierangela Samarati

- Kleptography: Old Warnings, new Threats!
  Moti Yung

Privacy Aware Computing

Chair: Aniket Kate

- A Fast Single Server Private Information Retrieval Protocol with Low Communication Cost
  Changyu Dong, Liqun Chen
- ID-Based Two-Server Password-Authenticated Key Exchange
  Xun Yi, Feng Hao, Elisa Bertino *(moved from Password Authentication session)*
- Authorized Keyword Search on Encrypted Data
  Jie Shi, Junzuo Lai, Yingjiu Li, Robert H. Deng, Jian Weng

Cryptography 1

chair: Jianying Zhou

- Double-Authentication-Preventing Signatures
  Bertram Poettering, Douglas Stebila
- Statistical Properties of Pseudo Random Sequences and Experiments with PHP and Debian OpenSSL
  Yongge Wang, Tony Nicol
- Efficient Hidden Vector Encryption with Constant-Size Ciphertext
  Tran Viet Xuan Phuong, Guomin Yang, Willy Susilo

Attribute Based Cryptography

chair: Mark Manulis

- Large Universe Ciphertext-Policy Attribute-Based Encryption with White-Box Traceability
  Jianting Ning, Zhenfu Cao, Xiaolei Dong, Lifei Wei, Xiaodong Lin
- PPDCP-ABE: Privacy-Preserving Decentralized Cipher-Policy Attribute-Based Encryption
  Jinguang Han, Willy Susilo, Yi Mu, Jianying Zhou, Man Ho Au
- Practical Direct Chosen Ciphertext Secure Key-Policy Attribute-Based Encryption with Public Ciphertext Test
  Weiran Liu, Jianwei Liu, Qianhong Wu, Bo Qin, Yunya Zhou
- Privacy-Preserving Auditing for Attribute-Based Credentials
  Jan Camenisch, Anja Lehmann, Gregory Neven, Alfredo Rial

Cryptography 2

chair: Yingjiu Li

- Public-Key Revocation and Tracing Schemes with Subset Difference Methods Revisited
  Kwangsu Lee, Woo Kwon Koo, Dong Hoon Lee, Jong Hwan Park
- NORX: Parallel and Scalable AEAD
  Jean-Philippe Aumasson, Philipp Jovanovic, Samuel Neves
- Even More Practical Secure Logging: Tree-based Seekable Sequential Key Generators
  Giorgia Azzurra Marson, Bertram Poettering

Privacy Panel

chair: Mirosław Kutyłowski

- Wojciech Wiewiórowski, Poland's Inspector General for Personal Data Protection
- Moti Yung, Google Inc. and Columbia University
- Peter Schoo, Huawei
- Joseph K. Liu, Institute for Infocomm Research, Singapore

Secure Wireless Communication

chair: Mauro Conti

- Enabling Short Fragments for Uncoordinated Spread Spectrum Communication
  Naveed Ahmed, Christina Pöpper, Srdjan Capkun
- Fingerprinting Far Proximity from Radio Emissions
  Tao Wang, Yao Liu, Jay Ligatti
- A Cross-Layer Key Establishment Scheme in Wireless Mesh Networks
  Yuexin Zhang, Yang Xiang, Xinyi Huang, Li Xu

Privacy

chair: Jaideep Vaidya

- What's the Gist? Privacy-Preserving Aggregation of User Profiles
  Igor Bilogrevic, Julien Freudiger, Emiliano De Cristofaro, Ersin Uzun
- Challenging Differential Privacy: the Case of Non-interactive Mechanisms
  Raghavendran Balu, Teddy Furon, and Sébastien Gambs
- Optimality and Complexity of Inference-proof Data Filtering and CQE
  J. Biskup, P.A. Bonatti, C. Galdi, L. Sauro
- New Insight to Preserve Online Survey Accuracy and Privacy in Big Data Era
  Joseph Liu, Man Ho Au, Xinyi Huang, Willy Susilo, Jianying Zhou, Yong Yu

---

9.09.2014

Invited Talk 3

chair: Nora Cuppens

- Protection of data access in networked computer systems
  Stefano Paraboschi

Code Analysis

chair: Frederic Cuppens

- Software Countermeasures for Control Flow Integrity of Smart Card C Codes
  Jean-François Lalande, Karine Heydemann, Pascal Berthomé
- LeakWatch: Estimating Information Leakage from Java Programs
  Tom Chothia, Yusuke Kawamoto, Chris Novakovic
- SigPath: A Memory Graph Based Approach for Program Data Introspection and Modification
  David Urbina, Yufei Gu, Juan Caballero, Zhiqiang Lin

Password Authentication

chair: Xun Yi

- Privacy-Preserving Complex Query Evaluation over Semantically Secure Encrypted Data
  Bharath K. Samanthula, Wei Jiang, Elisa Bertino *(moved from Privacy Aware Computing session)*
- Modelling Time for Authenticated Key Exchange Protocols
  Jörg Schwenk
- Zero-Knowledge Password Policy Checks and Verifier-Based PAKE
  Franziskus Kiefer, Mark Manulis

E-voting and E-cash

chair: Moti Yung

- Bitcoin Transaction Malleability and MtGox
  Christian Decker, Roger Wattenhofer
- Election Verifiability for Helios under Weaker Trust Assumptions
  Véronique Cortier, David Galindo, Stéphane Glondu, Malika Izabachène
- CoinShuffle: Practical Decentralized Coin Mixing for Bitcoin
  Tim Ruffing, Pedro Moreno-Sanchez, Aniket Kate

Attack Detection and Defence 1

chair: Elisa Bertino

- LESS is more: Host-Agent Based Simulator for Large-scale Evaluation of Security Systems
  John Sonchack, Adam J. Aviv
- Detecting Insider Information Theft Using Features from File Access Logs
  Christopher Gates, Ninghui Li, Zenglin Xu, Suresh N. Chari, Ian Molloy, Youngja Park
- SRID: State Relation based Intrusion Detection for False Data Injection Attacks in SCADA
  Yong Wang, Zhaoyan Xu, Jialong Zhang, Lei Xu, Haopei Wang, Guofei Gu
- Click Fraud Detection on the Advertiser Side
  Haitao Xu, Daiping Liu, Aaron Koehl, Haining Wang, Angelos Stavrou

Attack Detection and Defence 2

chair: Angelos Stavrou

- Botyacc: Unified P2P Botnet Detection using Behavioural Analysis and Graph Analysis
  Shishir Nagaraja
- Feature-Distributed Malware Attack: Risk and Defence
  Byungho Min, Vijay Varadharajan
- RootkitDet: Practical End-to-End Defense against Kernel Rootkits in a Cloud Environment
  Lingchen Zhang, Sachin Shetty, Peng Liu, Jiwu Jing
- Modeling Network Diversity for Evaluating the Robustness of Networks against Zero-Day Attacks
  Lingyu Wang, Mengyuan Zhang, Sushil Jajodia, Anoop Singhal, Massimiliano Albanese

Industrial Reception + Presentation

- GPU - Powerful Tool + Significant Threats. Lessons learnt from Reverse Engineering.
  Witold Waligora, REC Global