ESORICS 2014

PROGRAM OF ESORICS 2014 WORKSHOPS

	10.09.2014			11.09.2014			
	Room 113	Room 114	Room 115	Room 115	Room 113	Room 114	Room 406
8:30 - 9:00	Registration			Registration			
9:00 - 10:00		SIOT Welcome	STM Welcome +Invited Talk	STM Award	QASA/SETOP Invited Talk	BADGERS Welcome +Keynote	UaESMC Welcome +Invited Talk
10:00 - 11:15	DPM Welcome and Invited Talk	SIOT Invited Talk 1	STM Session 1	STM Session 4	QASA Session 2	BADGERS Session 1	UaESMC Session 1
11:15 - 11:45	Coffee Break			Coffee Break			
11:45-13:00	DPM Session 1	SIOT Session 1	STM Session 2	STM Session 5	QASA/SETOP Session 3	BADGERS Session 2	UaESMC Session 2
13:00 - 14:30	Lunch Break			Lunch Break			
14:30 -16:10	DPM Session 2	SIOT Invited Talk2	STM Session 3	STM Session 6	QASA Invited+ Session 4 (from 14:00)	BADGERS Session 3	UaESMC Session 3 (from 14:00)
16:10 - 16:40	Coffee Break			Coffee Break			
16:40 - 18:20	DPM Session 3	SIOT Session 2	ERCIM STM Business Meeting			BADGERS Keynote + Discussion	
evening	Workshops' Dinner						

ESORICS WORKSHOPS PROGRAM DETAILS

10.09.2014

SIOT Welcome, 9:00-10:00

- Welcome

STM Welcome + Invited Talk, 9:00-10:00

- STM Welcome
- Traffic analysis countermeasures in WSN
  Javier Lopez

DPM Welcome + Invited Talk, 10:00 - 11:15

- Welcome
- Is bitcoin suitable as a research topic?
  Jordi Herrera-Joancomartí

SIOT Invited Talk, 10:00 - 11:15

- TBA

STM Session - Verification, 10:00 - 11:15

- A Formal Definition of Protocol Indistinguishability and its Verification Using Maude-NPA
  Sonia Santiago, Santiago Escobar, Catherine Meadows and Jose Meseguer
- Ensuring Secure Non-interference of Programs by Game Semantics
  Aleksandar S. Dimovski

DPM Session 1: Cryptographic Solutions for Privacy, 11:45 - 13:00

- Group Discounts Compatible with Buyer Privacy
  Josep Domingo-Ferrer, Alberto Blanco-Justicia
- Towards an Image Encryption Scheme with Content-Based Image Retrieval Properties
  Bernardo Ferreira, Joao Rodrigues, Joao Leitao and Henrique Domingos
- The crypto-democracy and the Trustworthy
  Sebastien Gambs, Samuel Ranellucci and Alain Tapp

SIOT Session 2, 11:45 - 13:00

- Access Control for Apps Running on Constrained Devices in the Internet of Things
  Andrei Mituca, Amir H. Moin and Christian Prehofer
- Federated Identity and Access Management for the Internet of Things
  Paul Fremantle, Benjamin Aziz, Jacek Kopecky and Philip Scott
- Lightweight Display Virtualization For Mobile Devices
  Mihai Carabas, Lucian Mogosanu, Razvan Deaconescu, Laura Gheorghe and Nicolae Tapus

STM Session 2 - Privacy and Implementation Security, 11:45 - 13:00

- Privacy Architectures: Reasoning About Data Minimisation and Integrity
  Thibaud Antignac and Daniel Le Métayer
- Lime: Data Lineage in the Malicious Environment
  Michael Backes, Niklas Grimm and Aniket Kate
- Efficient Java Code Generation of Security Protocols specified in AnB/AnBx
  Paolo Modesti

DPM Session 2 - Emerging challenges, 14:30 - 16:10

- Configuration Behavior of Restrictive Default Privacy Settings on Social Network Sites
  Markus Tschersich
- Toward Inherent Privacy Awareness in Workflows
  Maria Koukovini, Eugenia Papagiannakopoulou, Georgios Lioudakis, Nikolaos Dellas, Dimitra I. Kaklamani, Iakovos S. Venieris
- Index Optimization for L-Diversified Database-as-a-Service
  Jens Kohler and Hannes Hartenstein
- A-PPL: An Accountability Policy Language for Cloud Computing
  Monir Azraoui, Kaoutar Elkhiyaoui, Melek Onen , Karin Bernsmed, Anderson Santana De Oliveira and Jakub Sendor

SIOT Invited Talk 2, 14:30 - 16:10

- Key Evolution Protocols for IoT
  Marek Klonowski

STM Session 3 - Access Control 1, 14:30 - 16:10

- ALPS: An Action Language for Policy Specification and Automated Safety Analysis
  Silvio Ranise and Riccardo Traverso
- Monotonicity and Completeness in Attribute-based Access Control
  Jason Crampton and Charles Morisset
- ROMEO: ReputatiOn Model Enhancing OpenID Simulator
  Ginés Dòlera Tormo, Félix Gòmez Mármol and Gregorio Martínez Pérez
- Hybrid Enforcement of Category-Based Access Control
  Asad Ali and Maribel Fernaández

DPM Session 3, Privacy-Preserving, Protocols and Applications, 16:40 - 18:20

- Privacy-preserving Loyalty Programs
  Alberto Blanco-Justicia and Josep Domingo-Ferrer
- Secure Improved Cloud-Based RFID Authentication Protocol
  Sarah Abughazalah, Konstantinos Markantonakis, and Keith Mayes
- Privacy-Preserving Electronic Toll System with Dynamic Pricing for Low Emission Zones
  Roger Jardi-Cedo, Jordi Castella-Roca and Alexandre Viejo
- Association Rule Mining on Fragmented Database
  Amel Hamzaoui, Qutaibah Malluhi, Riley Ryan and Clifton Chris

SIOT Session 2, 16:40 - 18:20

- A Novel Key Generating Architecture for Wireless Low-resource Devices
  Christian T. Zenger, Markus-Julian Chur, Gerhard Wunder and Christof Paar
- Threat-based Security Analyses for the Internet of Things
  Ahmad Atamli and Andrew Martin
- UNCHAIN - Ubiquitous Wireless Network Communication Architecture for Ambient Intelligence and Health scenarios
  Daniel Rosner, Laura Gheorghe, Razvan Tataroiu and Razvan Tilimpea

ERCIM STM Business Meeting, 16:40 - 18:20

11.09.2014

STM Award, 9:00 - 10:00

- STM award ceremony
- Presentation by award winner

QASA/SETOP Invited Talk, 9:00 - 10:00

- Assessing Data Trustworthiness - Concepts and Research Challenges,
  Elisa Bertino

BADGERS Welcome and Keynote, 9:00 - 10:15

- Welcome
- Behind the NICTER: Challenges for Cybersecurity Big Data,
  Daisuke Inoue

UaESMC Welcome and Invited Talk, 9:00 - 10:00

- Welcome
- Efficient Two-Party Computations from Oblivious Transfer
  Thomas Schneider

STM Session 4 - Access Control 2, 10:00 - 11:15

- Caching and Auditing in the RPPM Model
  Jason Crampton and James Sellwood
- Stateful Usage Control for Android Mobile Devices
  Aliaksandr Lazouski, Fabio Martinelli, Paolo Mori and Andrea Saracino

QASA Session 2, 10:00 - 11:15

- Calculating adversarial risk from attack trees: Control strength and probabilistic attackers
  Wolter Pieters and Mohsen Davarynejad
- Analysis of Social Engineering Threats with Attack Graphs
  Kristian Beckers, Leanid Krautsevich and Artsiom Yautsiukhin
- Probabilistic Modeling of Humans in Security Ceremonies (Short paper)
  Cristian Prisacariu and Audun Jøsang

BADGERS Session 1, 10:15 - 11:15

- ANDRUBIS - 1,000,000 Apps Later: A View on Current Android Malware Behaviors
  Martina Lindorfer, Matthias Neugschwandtner, Lukas Weichselbaum, Yanick Fratantonio, Victor van der Veen and Christian Platzer
- The Vulnerability Dataset of a Large Software Ecosystem
  Dimitris Mitropoulos, Georgios Gousios, Panagiotis Papadopoulos, Vassilios Karakoidas, Panos Louridas and Diomidis Spinellis

UaESMC Session 1, 10:00 - 11:15

- Privacy-preserving Data Aggregation with Optimal Utility Using Arithmetic SMC
  Fabienne Eigner, Aniket Kate, Matteo Maffei, Francesca Pampaloni, Ivan Pryvalov
- Is it possible to perform statistical analysis in a cryptographically secure manner?
  Dan Bogdanov, Liina Kamm, Sven Laur, Ville Sokk

STM Session 5 - Education and Evaluation, 11:45 - 13:00

- A Formal Model for Soft Enforcement: Influencing the Decision-Maker
  Charles Morisset, Iryna Yevseyeva, Thomas Gross and Aad Van Moorsel
- NoPhish - An Anti-Phishing Education App
  Gamze Canova, Melanie Volkamer, Clemens Bergmann and Roland Borza
- Evaluation of key management schemes in wireless sensor networks
  Filip Jurnecka, Martin Stehlík and Vashek Matyas

SETOP Session 3, 11:45 - 13:00

- Metric for Security Activities assisted by Argumentative Logic
  Tarek Bouyahia, Muhammad Sabir Idrees, Nora Cuppens-Boulahia, Frederic Cuppens and Fabien Autrel
- Environment-Reactive Malware Behavior: Detection and Categorization
  Smita Naval, Vijay Laxmi, Manoj Gaur, Sachin Raja, Muttukrishnan Rajarajan and Mauro Conti
- High-Level Simulation for Multiple Fault Injection Evaluation (QASA Short paper)
  Maxime Puys, Lionel Rivière, Thanh-Ha Le and Julien Bringer

BADGERS Session 2, 11:45 - 13:15

- Security and Privacy Measurements in Social Networks: Experiences and Lessons Learned
  Iasonas Polakis, Federico Maggi, Stefano Zanero and Angelos D. Keromytis
- Classification of SSL Servers based on their SSL Handshake for Automated Security Assessment
  Sirikarn Pukkawanna, Youki Kadoyabashi, Gregory Blanc, Joaquin Garcia-Alfaro and Herve Debar
- Are We Missing Labels? A Study of the Availability of Ground-Truth in Network Security Research
  Sebastian Abt and Harald Baier

UaESMC Session 2, 11:45 - 13:00

- Minimizing Information Leakage Against Selective Failures in Consistent Multi-party Computation
  Aggelos Kiayias, Yiannis Tselekounis, Bingsheng Zhang
- Privacy Preserving Business Process Fusion
  Roberto Guanciale, Dilian Gurov

STM Session 6 - Economic Domain, 14:30 - 16:10

- Using Prediction Markets to Hedge Information Security Risks
  Pankaj Pandey and Einar Snekkenes
- Integrating Trust and Economic Theories with Knowledge Science for Dependable Service Automation
  Vangalur Alagar and Kaiyu Wan
- BlueWallet: The Secure Bitcoin Wallet
  Tobias Bamert, Christian Decker, Roger Wattenhofer and Samuel Welten

QASA Invited Talk, 14:00 - 15:00

- Defining assurance levels for user and server authentication
  Audun Jøsang

QASA Session 4, 15:00 - 16:10

- Introducing Probabilities in Controller Strategies
  Jerry Den Hartog and Ilaria Matteucci
- Automatically Calculating Quantitative Integrity Measures for Imperative Programs
  Tom Chothia, Chris Novakovic and Rajiv Ranjan Singh
- Risk-Aware Information Disclosure
  Alessandro Armando, Michele Bezzi, Nadia Metoui and Antonino Sabetta

BADGERS Session 3, 14:30 - 16:10

- Collaborative Repository for Cybersecurity Data and Threat Information
  Jean Lorchat, Cristel Pelsser and Romain Fontugne
- MATATABI: Multi-layer Threat Analysis Platform with Hadoop
  Hajime Tazaki, Kazuya Okada, Yuji Sekiya and Youki Kadobayashi
- EyeBit: Eye-Tracking Approach for Enforcing Phishing Prevention Habits
  Daisuke Miyamoto, Takuji Iimura, Gregory Blanc, Hajime Tazaki and Youki Kadobayashi

UaESMC Session 3, 14:00 - 16:10

- Practical Universally Verifiable Linear Programming
  Meilof Veeningen, Sebastiaan de Hoogh, Berry Schoenmakers, Niels de Vreede
- Transformation-Based Privacy-Preserving Linear Programming
  Peeter Laud, Alisa Pankova
- When the users don't know what to want: exploring privacy preserving technology adoption in highly uncertain conditions
  Laur Kanger, Pille Pruulmann-Vengerfeldt

BADGERS Keynote + Discussion, 16:40 - 18:00

- Opportunities and Challenges in Large-scale Data Analysis for System Security
  Davide Balzarotti
- Closing