ESORICS'2009

Conference Program at a Glance

September 21, 2009 (Maupertuis Amphitheater)

08:00am – 09:00am	Registration	
09:00am -- 09:30am	Openning Remarks	Maupertuis Amphitheater
09:30am – 10:30am	Invited Speaker: David Sands Paralocks: Role-Based Information Flow Control and Beyond	Maupertuis Amphitheater
10:30am -- 11:00am	Coffee Break	Rotonde Surcouf
11:00am -- 12:30pm	Session 1: Network Security I	Maupertuis Amphitheater
12:30pm -- 02:00pm	Lunch	Rotonde Surcouf
02:00pm -- 03:30pm	Session 2: Information Flow	Maupertuis Amphitheater
03:30pm -- 04:00pm	Coffee Break	Rotonde Surcouf
04:00pm -- 05:30pm	Session 3: Network Security II	Maupertuis Amphitheater

September 22, 2009

09:00am -- 10:30am	Session 4: Language-based Security	Maupertuis Amphitheater
10:30am -- 11:00am	Coffee Break	Rotonde Surcouf
11:00am – 12:30pm	Session 5: Network Security III - Session 6: Access Control	Maupertuis Amphitheater Room Vauban 2
12:30pm -- 02:00pm	Lunch	Rotonde Surcouf
02:00pm – 03:30pm	Session 7: Privacy I - Session 8: Distributed Systems Security	Maupertuis Amphitheater Room Vauban 2
03:30pm -- 04:00pm	Coffee Break	Rotonde Surcouf
04:00pm – 05:30pm	Session 9: Privacy II - Session 10: Security Primitives	Maupertuis Amphitheater Room Vauban 2
08:00pm --	Gala diner	

September 23, 2009

09:00am – 10:30am	Session 11: Web Security - Session 12: Cryptography	Maupertuis Amphitheater Room Vauban 2
10:30am -- 11:00am	Coffee Break	Rotonde Surcouf
11:00am – 12:30pm	Session 13: Protocols - Session 14: Systems Security and Forensics	Maupertuis Amphitheater Room Vauban 2
12:30pm -- 02:00pm	Lunch	Rotonde Surcouf

Conference Program

Session 1: Network Security - I

Learning More About the Underground Economy: A Case-Study of Keyloggers and Dropzones. *Thorsten Holz (University of Mannheim), Markus Engelberth (University of Mannheim), Felix Freiling (University of Mannheim)*

User-Centric Handling of Identity Agent Compromise. *Daisuke Mashima, Mustaque Ahamad, Swagath Kannan*

The Coremelt Attack. *Ahren Studer (Carnegie Mellon University), Adrian Perrig (Carnegie Mellon University)*

Session 2: Information Flow

Type-based Analysis of PIN Processing APIs. *Matteo Centenaro (University of Venice, Italy), Riccardo Focardi (University of Venice, Italy), Flaminia Luccio (University of Venice, Italy), Graham Steel (LSV, ENS Cachan & CNRS & INRIA, France)*

Declassification with Explicit Reference Points. *Alexander Lux (TU Darmstadt), Heiko Mantel (TU Darmstadt)*

Tracking Information Flow in Dynamic Tree Structures. *Alejandro Russo (Chalmers), Andrei Sabelfeld (Chalmers), Andrey Chudnov (Stevens)*

Session 3: Network Security - II

Lightweight Opportunistic Tunneling (LOT). *Amir Herzberg, Yossi Gilad (Bar Ilan University)*

Hide and Seek in Time - Robust Covert Timing Channels. *Yali Liu (University of California, Davis), Frederik Armknecht (Ruhr-University), Dipak Ghosal (University of California, Davis), Stefan Katzenbeisser (Technische Universität Darmstadt), Ahmad-Reza Sadeghi (Ruhr-University), Steffen Schulz (Ruhr-University)*

Authentic Time-Stamps for Archival Storage. *Alina Oprea (RSA Laboratories), Kevin Bowers (RSA Laboratories)*

Session 4: Language Based Security

Towards a theory of accountability and audit. *Radha Jagadeesan (School of CDM, DePaul University, Chicago), Alan Jeffrey (Bell Labs, Alcatel-Lucent), Corin Pitcher (School of CDM, DePaul University, Chicago), James Riely (School of CDM, DePaul University, Chicago)*

Reliable Evidence: Auditability by Typing. *Nataliya Guts (MSR-INRIA Joint Centre), Cédric Fournet (Microsoft Research), Francesco Zappa Nardelli (INRIA)*

PCAL: Language Support for Proof-Carrying Authorization Systems. *Avik Chaudhuri (University of Maryland, College Park), Deepak Garg (Carnegie Mellon University)*

Session 5: Network Security - III

ReFormat: Automatic Reverse Engineering of Encrypted Messages. *Zhi Wang (North Carolina State University), Xuxian Jiang (North Carolina State University), Weidong Cui (Microsoft Research), Xinyuan Wang (George Mason University), Mike Grace (North Carolina State University)*

Protocol Normalization using Attribute Grammars. *Drew Davidson (University of Wisconsin-Madison), Randy Smith (University of Wisconsin-Madison), Nic Doyle (CISCO Systems), Somesh Jha (University of Wisconsin-Madison)*

Automatically Generating Models for Botnet Detection. *Peter Wurzinger (Technical University Vienna), Leyla Bilge (Institute Eurecom), Thorsten Holz (University of Mannheim), Jan Göbel (University of Mannheim), Christopher Kruegel (University of California, Santa Barbara), Engin Kirda (Institute Eurecom)*

Session 6: Access Control

Dynamic Enforcement of Abstract Separation of Duty Constraints. *David A. Basin (Information Security, Department of Computer Science, ETH Zurich), Samuel J. Burri (Security Group, Zurich Research Laboratory, IBM Research), Günter Karjoth (Security Group, Zurich Research Laboratory, IBM Research)*

Usable Access Control in Collaborative Environments: Authorization based on People-Tagging. *Qihua Wang (Purdue University), Hongxia Jin (IBM Almaden Research Center), Ninghui Li (Purdue University)*

Requirements and protocols for inference-proof interactions in information systems. *Joachim Biskup (Technische Universitaet Dortmund), Christian Gogolin (Technische Universitaet Dortmund), Jens Seiler (Technische Universitaet Dortmund), Torben Weibert (Technische Universitaet Dortmund)*

Session 7: Privacy - I

A Privacy Preservation Model for Facebook-Style Social Network Systems. *Philip W. L. Fong (University of Calgary), Mohd Anwar (University of Calgary), Zhen Zhao (University of Regina)*

New Privacy Results on Synchronized RFID Authentication Protocols Against Tag Tracing. *Ching Yu Ng (University of Wollongong), Willy Susilo (University of Wollongong), Yi Mu (University of Wollongong), Rei Safavi-Naini (University of Calgary)*

Secure Pseudonymous Channels. *Sebastian Moedersheim (IBM Zurich Research Laboratory), Luca Vigano (University of Verona)*

Session 8: Distributed Systems Security

Enabling Public Verifiability and Data Dynamics for Storage Security in Cloud Computing. *Qian Wang (Illinois Institute of Technology), Cong Wang (Illinois Institute of Technology), Jin Li (Illinois Institute of Technology), Kui Ren (Illinois Institute of Technology), Wenjing Lou (Worcester Polytechnic Institute)*

Content Delivery Network: Protection or Threat? *Sipat Triukose (Case Western Reserve University), Zakaria Al-Qudah (Case Western Reserve University), Michael Rabinovich (Case Western Reserve University)*

Model-Checking DoS Amplification for VoIP Session Initiation. *Ravinder Shankesi (University of Illinois), Musab AlTurki (University of Illinois), Ralf Sasse (University of Illinois), Carl Gunter (University of Illinois), Jose Meseguer (University of Illinois)*

Session 9: Privacy - II

The wisdom of Crowds: attacks and optimal constructions. *George Danezis (Microsoft Research), Claudia Diaz, Emilia Kasper, and Carmela Troncoso (K.U. Leuven/IBBT, ESAT/SCD-COSIC)*

Secure Evaluation of Private Linear Branching Programs with Medical Applications. *Mauro Barni (University of Siena), Pierluigi Failla (University of Siena), Vladimir Kolesnikov (Bell Laboratories), Riccardo Lazzeretti (University of Siena), Ahmad-Reza Sadeghi (Ruhr-University Bochum), Thomas Schneider (Ruhr-University Bochum)*

Keep a Few: Outsourcing Data while Maintaining Confidentiality. *Valentina Ciriani (DTI - Universita' degli Studi di Milano), Sabrina De Capitani di Vimercati (DTI - Universita' degli Studi*

di Milano), Sara Foresti (DTI - Universita' degli Studi di Milano), Sushil Jajodia (CSIS - George Mason University), Stefano Paraboschi (DIIMM - University of Bergamo), Pierangela Samarati (DTI - Universita' degli Studi di Milano)

Session 10: Security Primitives

Data Structures with Unpredictable Timing. *Darrell Bethea (University of North Carolina at Chapel Hill), Mike Reiter (University of North Carolina at Chapel Hill)*

WORM-SEAL: Trustworthy Data Retention and Verification for Regulatory Compliance. *Tiancheng Li (Purdue University), Xiaonan Ma (IBM Almaden Research Center), Ninghui Li (Purdue University)*

Corruption-Localizing Hashing. *Giovanni Di Crescenzo (telcordia technologies), Shaoquan Jiang, Reihaneh Safavi-Naini*

Session 11: Web Security

Isolating JavaScript with Filters, Rewriting, and Wrappers. *Sergio Maffeis (Imperial College, London), John C. Mitchell (Stanford University), Ankur Taly (Stanford University)*

An Effective Method for Combating Malicious Scripts Clickbots. *Yanlin Peng (Iowa State University), Linfeng Zhang (Iowa State University), J. Morris Chang (Iowa State University), Yong Guan (Iowa State University)*

Client-Side Detection of XSS Worms by Monitoring Payload Propagation. *Fangqi Sun (UC Davis), Liang Xu (UC Davis), Zhendong Su (UC Davis)*

Session 12: Cryptography

Formal Indistinguishability extended to the Random Oracle Model. *Cristian Ene (Université Grenoble 1, CNRS, Verimag), Yassine Lakhnech (Université Grenoble 1, CNRS, Verimag), Van Chan Ngo (ETH Zürich)*

Computationally Sound Analysis of a Probabilistic Contract Signing Protocol. *Mihhail Aizatulin (University of Kiel), Henning Schnoor (University of Kiel), Thomas Wilke (University of Kiel)*

Ciphertext-Policy Attribute-Set Based Encryption. *Rakesh Bobba (University of Illinois), Himanshu Khurana (University of Illinois), Manoj Prabhakaran (University of Illinois)*

Session 13: Protocols

Synthesising Secure APIs. *Veronique Cortier (LORIA, Projet Cassis, CNRS & INRIA), Graham Steel (LSV, INRIA & CNRS & ENS-Cachan)*

ID-based Secure Distance Bounding and Localization. *Nils Ole Tippenhauer (ETH Zurich), Srdjan Capkun (ETH Zurich)*

Secure ownership and ownership transfer in RFID systems. *Ton van Deursen (University of Luxembourg), Sjouke Mauw (University of Luxembourg), Sasa Radomirovic (University of Luxembourg), Pim Vullers (Radboud University Nijmegen)*

Session 14: Systems Security and Forensics

Cumulative Attestation Kernels for Embedded Systems. *Michael LeMay (University of Illinois at Urbana-Champaign), Carl A. Gunter (University of Illinois at Urbana-Champaign)*

Super-efficient Aggregating History-independent Persistent Authenticated Dictionaries. *Scott A. Crosby (Rice University), Dan S. Wallach (Rice University)*

Set Covering Problems in Role-Based Access Control. *Liang Chen (Royal Holloway, University of London), Jason Crampton (Royal Holloway, University of London)*