Esorics 2009: List of accepted papers

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)

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)

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)

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)

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)

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

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)

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

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

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)

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)

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

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)

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)

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 (Eindhoven University of Technology and University of Luxembourg)

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

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)

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

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)

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

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)

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

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)

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

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

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

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)

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

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)

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

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)

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

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

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)

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)

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

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

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

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

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

Corruption-Localizing Hashing
Giovanni Di Crescenzo, Shaoquan Jiang, Reihaneh Safavi-Naini

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)