ESORICS 2012

10-14 September 2012
Pisa, Italy

ESORICS 2012 Week - Complete Program

(ESORICS – DPM – EUROPKI – QASA – SETOP – STM)

(version 05 Sept. 2012)

ESORICS 2012 Program 2

Data Privacy Management Workshop 2012 (DPM) 10

9th European PKI Workshop: Research and Applications (EuroPKI 2012) 11

International Workshop on Quantitative Aspects in Security Assurance (QASA) 13

5th SETOP International Workshop on Autonomous and Spontaneous Security (SETOP 2012) 14

8th International Workshop on Security and Trust Management (STM 2012) 15

ESORICS 2012 Program

	September 10, 2012		September 11, 2012		September 12, 2012
	Auditorium	Room A27	Auditorium	Room A27	Auditorium
8.00 – 9.00	REGISTRATION				
9.00 - 9.15	Welcome and Opening (plenary)				
9.15 - 10.15	Invited talk: Prof. Ahmad-Reza Sadeghi		Invited talk: Prof. Gilles Barthe		Invited talk: Prof. Christian Cachin
10.15 - 10.45	Coffee Break		Coffee Break		Coffee Break
10.45 - 12.45	Session 1A: Security and data protection in real systems	Session 1B: Formal models for cryptography and access control	Session 4A: Location privacy	Session 4B: Voting protocols and anonymous communication	Session 7: Encryption key and password security
12.45 - 14.15	Lunch		Lunch		Lunch
14.15 - 15.45	Session 2A: Security and privacy in mobile and wireless networks	Session 2B: Counteracting Man-in-the-Middle attacks	Session 5A: Private computation in cloud systems	Session 5B: Formal security models	Session 8: Malware and phishing
15.45 - 16.15	Coffee Break		Coffee Break		Coffee Break
16.15 - 17.45	Session 3A: Network security	Session 3B: Users privacy and anonymity	Session 6A: Identity based encryption and group signature	Session 6B: Authentication	Session 9: Software security
19.30-21.30	Welcome Reception				
20.00-23.30			Social Dinner		

Monday, September 10, 2012 -- 9.15 – 10.15

Invited talk: Mind the Gap: Smartphone Security and Privacy in Theory and Practice
Prof. Ahmad-Reza Sadeghi
Technische Universität Darmstadt
http://www.trust.informatik.tu-darmstadt.de/people/ahmad-reza-sadeghi/?no_cache=1

Abstract: Mobile "smart" devices such as smartphones and tablets have already changed our daily lives in various ways. Many people are literally glued to these devices all through the day. The increasing computing and storage capabilities, new interfaces such as NFC or Smartcards, the vast number and variety of apps available on app stores and markets as well as the connectivity to cloud services are making smart devices convenient replacements for traditional (mobile) computing platforms such as laptops. Not surprisingly enterprises and governments have discovered the potential of these devices enabling "work on the go" for employees either by providing them with the corresponding smart devices, or by the "Bring Your Own Device (BOYED)" philosophy.

On the down side, the increased complexity of these devices as well as the increasing amount of sensitive information (private or corporate) stored and processed on them, from user's location data to credentials for online banking and enterprise VPN, raise many security and privacy concerns. In particular, the growing number and sophistication of the recent attacks and findings show that the default protection mechanisms offered by smart devices are indeed insufficient.

In this talk we will briefly go through different classes of threats and their relevance as well as the recent academic and industrial approaches and efforts on improving various security and privacy aspects of mobile devices and services with the focus on the currently most popular (open-source) Android OS: While academic research has proposed a number of solutions and tools to protect end-users ranging from security extensions of different Android's abstraction layers to analysis of apps and app markets, the enterprise solutions deployed today typically focus on device management aspects and malware detection. We will discuss this gap and point out some technical and non-technical challenges and practical problems as well as possible solutions towards establishing smartphone security architectures that allow for a reasonable fine-grained user-centric privacy-protection on the one hand, and corporate security on the other hand.

Short Bio: Ahmad-Reza Sadeghi is a full professor of Computer Science at Technische Universitaet Darmstadt. He is the Director of System Security Lab at Center for Advance Security Research Darmstadt (CASED) and Scientific Director of Fraunhofer Institute for Secure Information Systems (SIT). Since January 2012 he is also the Director of Intel-TU Darmstadt Collaborative Research Institute for Secure Computing in Darmstadt, Germany.

He received his PhD in Computer Science with the focus on privacy protecting cryptographic protocols and systems from the University of Saarland in Saarbruecken, Germany. Prior to academia, he worked in Research and Development of Telecommunications enterprises, amongst others Ericson Telecommunications. He has been leading and involved in a variety of national and international research and development projects on design and implementation of trustworthy mobile computing platforms and trusted computing, security in hardware, cryptographic privacy protecting systems, and cryptographic compilers. He has been continuously contributing to the IT security research community and serving as general or program chair as well as program committee member of many conferences and workshops in information security and privacy. He is on Editorial Board of the ACM Transactions on Information and System Security.

Ahmad has been awarded with the renowned German prize “Karl Heinz Beckurts” for his research on Trusted and Trustworthy Computing technology and its transfer to industrial practice. The award honors excellent scientific achievements with high impact on industrial innovations in Germany. Further, his group received the second prize of German IT Security Competition Award 2010.

Monday, September 10, 2012 -- 10.45 – 12.45

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

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

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

- Effective Symbolic Protocol Analysis via Equational Irreducibility Conditions
  (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
  (Henning Schnoor)
- Satisfiability and Feasibility in a Relationship-based Workflow Authorization Model
  (Arif Khan and Philip Fong)
- Deciding Security for a Fragment of ASLan
  (Sebastian A. Mödersheim)

Monday, September 10, 2012 -- 14.15 – 15.45

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

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

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

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

Monday, September 10, 2012 -- 16.15 – 17.45

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

- The Silence of the LANs: Efficient Leakage Resilience for IPsec VPNs
  (Ahmad-Reza Sadeghi, Steffen Schulz and Vijay Varadharajan)

- Security of Patched DNS
  (Amir Herzberg and Haya Shulman)

- Revealing Abuses of Channel Assignment Protocols in Multi-Channel Wireless Networks: An Investigation Logic Approach
  (Qijun Gu, Kyle Jones, Wanyu Zang, Meng Yu and Peng Liu)

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

- Exploring Linkablility of User Reviews
  (Mishari Almishari and Gene Tsudik)

- Formal Analysis of Privacy in an eHealth Protocol
  (Naipeng Dong, Hugo Jonker and Jun Pang)

- PRIVATUS: Wallet-Friendly Privacy Protection for Smart Meters
  (Jinkyu Koo, Xiaojun Lin and Saurabh Bagchi)

Tuesday, September 11, 2012 -- 9.15 – 10.15

Invited talk: Computer-Aided Cryptographic Proofs and Designs
Prof. Gilles Barthe
IMDEA Software Institute
http://software.imdea.org/~gbarthe/index.html

Abstract: EasyCrypt is a tool for constructing and verifying cryptographic proofs. EasyCrypt can be used as a stand-alone application, or as a verifying back-end for cryptographic compilers. SyntheCrypt is a new tool that synthesizes public-key encryption schemes and generates proofs of security in EasyCrypt. The presentation will outline the language-based methods that underlie the design of both tools and illustrate some of their applications.

Short Bio: Gilles Barthe received a Ph.D. in Mathematics from the University of Manchester, UK, in 1993, and an Habilitation à diriger les recherches in Computer Science from the University of Nice, France, in 2004. He joined the IMDEA Software Institute in April 2008. He has been coordinator/principal investigator of many national and European projects, and served as the scientific coordinator of the FP6 FET integrated project "MOBIUS" for enabling proof-carrying code for Java on mobile devices (2005-2009). He has served as PC (co-)chair of conferences such as VMCAI'10, ESOP'11, and FAST'11. He is a member of the editorial board of the Journal of Automated Reasoning.
His research interests include formal methods, programming languages and program verification, software and system security, and cryptography, and foundations of mathematics and computer science. Since 2006, he is working on the development of formal verification tools for cryptographic proofs.

Tuesday, September 11, 2012 -- 10.45 – 12.45

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

- SHARP: Private Proximity Test and Secure Handshake with Cheat-Proof Location Tags
  (Yao Zheng, Ming Li, Wenjing Lou and Y. Thomas Hou)

- Secure Proximity Detection for NFC Devices based on Ambient Sensor Data
  (Tzipora Halevi, Di Ma, Nitesh Saxena and Tuo Xiang)

- Enhancing Location Privacy for Electric Vehicles (at the right time)
  (Joseph Liu, Man Ho Au, Willy Susilo and Jianying Zhou)

- Design and Implementation of a Terrorist Fraud Resilient Distance Bounding System
  (Aanjhan Ranganathan, Nils Ole Tippenhauer, Boris Skoric, Dave Singelee and Srdjan Capkun)

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

- Applying Divertibility to Blind Ballot Copying in the Helios Internet Voting System
  (Yvo Desmedt and Pyrros Chaidos)

- Defining Privacy for Weighted Votes, Single and Multi-Voter Coercion
  (Jannik Dreier, Pascal Lafourcade and Yassine Lakhnech)

- TorScan: Tracing Long-lived Connections and Differential Scanning Attacks
  (Alex Biryukov, Ivan Pustogarov and Ralf Philipp Weinmann)

- Introducing the gMix Open Source Framework for Mix Implementations
  (Karl-Peter Fuchs, Dominik Herrmann and Hannes Federrath)

Tuesday, September 11, 2012 -- 14.15 – 15.45

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

- Secure and Efficient Outsourcing of Sequence Comparisons
  (Marina Blanton, Mikhail J. Atallah, Keith B. Frikken and Qutaibah Malluhi)

- Third-Party Private DFA Evaluation on Encrypted Files in the Cloud
  (Lei Wei and Michael Reiter)

- New Algorithms for Secure Outsourcing of Modular Exponentiations
  (Xiaofeng Chen, Jin Li, Jianfeng Ma, Qiang Tang and Wenjing Lou)

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

- Towards Symbolic Encryption Schemes
  (Naveed Ahmed, Christian Damsgaard Jensen and Erik Zenner)

- Decision Procedures for Simulatability
  (Charanjit Jutla and Arnab Roy)

- Model-Checking Bisimulation-based Information Flow Properties for Infinite State Systems
  (Deepak D'Souza and Raghavendra K. R.)

Tuesday, September 11, 2012 -- 16.15 – 17.45

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

- Identity-Based Traitor Tracing with Short Private Key and Short Ciphertext
  (Fuchun Guo, Yi Mu and Willy Susilo)

- Identity-Based Encryption with Master Key-Dependent Message Security and Leakage-Resilience
  (David Galindo, Javier Herranz and Jorge Villar)

- Unique Group Signatures
  (Matthew Franklin and Haibin Zhang)

Session 6B: Authentication
(chair: Nora Cuppens)

- Relations among Notions of Privacy for RFID Authentication Protocols
  (Daisuke Moriyama, Shin'Ichiro Matsuo and Miyako Ohkubo)

- PE(AR)^2: Privacy-Enhanced Anonymous Authentication with Reputation and Revocation
  (Kin Ying Yu, Tsz Hon Yuen, Sherman S.M. Chow, S.M. Yiu and Lucas C.K. Hui)

- Dismantling iClass and iClass Elite
  (Flavio D. Garcia, Gerhard de Koning Gans, Roel Verdult and Milosch Meriac)

Wednesday, September 12, 2012 -- 9.15 – 10.15

Invited talk: Integrity of Storage and Computations in the Cloud
Prof. Christian Cachin
IBM Research - Zurich
http://www.zurich.ibm.com/~cca/

Abstract: A group of mutually trusting clients uses a remote provider to store data or to perform an arbitrary computation service on their behalf. The provider may be subject to attacks and the clients do not fully trust the provider. The clients do not communicate with each other during day-to-day operations, but they would like to verify the integrity of the stored data, the correctness of the remote computation process, and the consistency of the provider's responses.
We present protocols that guarantee atomic operations to all clients when the provider is correct and so-called fork-linearizable semantics when the provider is faulty. Fork-linearizability makes it much easier for the clients to detect violations of integrity and consistency by the provider; specifically, it means that all clients which observe each other's operations are consistent, in the sense that their own operations, plus those operations whose effects they see, have occurred atomically in one sequence. Otherwise, a faulty provider could answer with arbitrary values from past operations and return diverging results to different clients. We describe a protocol for securing an outsourced storage service in this way and show how to extend it to protect arbitrary remote computations.

Short Bio: Christian Cachin is a researcher in cryptography and security at IBM Research - Zurich. He graduated with a Ph.D. in Computer Science from ETH Zurich and has held visiting positions at MIT and at EPFL. Presently he serves as the Vice President of the International Association for Cryptologic Research (IACR) and is an author of the book "Introduction to Reliable and Secure Distributed Programming." His current research interests are the security of storage systems, secure protocols for distributed systems, and cryptography. He contributed to the OASIS Key Management Interoperability Protocol (KMIP) standard and is currently concerned with security in cloud computing.

Wednesday, September 12, 2012 -- 10.45 – 12.45

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

- Evaluation of Standardized Password-based Key Derivation against Parallel Processing Platforms
(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
(Cas Cremers and Michele Feltz)

- Bleichenbacher's Attack Strikes Again: Breaking PKCS#1 v1.5 in XML Encryption
(Tibor Jager, Sebastian Schinzel and Juraj Somorovsky)

- On The Security of Password Manager Database Formats
(Paolo Gasti and Kasper Rasmussen)

Wednesday, September 12, 2012 -- 14.15 – 15.45

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

- Scalable Telemetry Classification for Automated Malware Detection
(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
(Philippe Beaucamps, Isabelle Gnaedig and Jean-Yves Marion)

- Detecting Phishing Emails the Natural Language Way
(Rakesh Verma, Narasimha Shashidhar and Nabil Hossain)

Wednesday, September 12, 2012 -- 16.15 – 17.45

Session 9: Software security
(chair: Dieter Gollmann)

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

Data Privacy Management Workshop 2012 (DPM)

Thursday, September 13, 2012 -- 09.00 – 10.45

Session 1: Authentication, Anonymity and Location-Based Systems

- 09:05-09:30: Fair Anonymous Authentication for Location Based Services, by Panayiotis Kotzanikolaou, Emmanouil Magkos and Nikolaos Petrakos.
- 09:30-09:55: Enhancing Privacy in LTE Paging System using Physical Layer Identification, by Tuan Ta and John Baras.
- 09:55-10:20: Post-hoc User Traceability Analysis in Electronic Toll Pricing Systems, by Xihui Chen, David Fonkwe and Jun Pang.
- 10:20-10:45: An Efficient and Secure Coding-based Authenticated Encryption, by Mohammed Meziani and Rachid El Bansarkhani.

Thursday, September 13, 2012 -- 11.15 – 13.05

Session 2: Case Studies on Citizens' Privacy

- Invited Talk 1: Authentication, Anonymity and Location-Based Systems On the Foundations of Trust in Networks of Humans and Computers, Virgil Gligor (Carnegie Mellon University, USA)
- 12:15-12:40: Proposal of Non-Invasive Fingerprint Age Determination to Improve Data Privacy Management in Police Work from a Legal Perspective using the Example of Germany,
  by Ronny Merkel, Matthias Pocs, Jana Dittmann and Claus Vielhauer.
- 12:40-13:05: Differential Privacy in Tripartite Interaction: A Case Study with Linguistic Minorities in Canada,
  by Arnaud Casteigts, Marie-Hélène Chomienne, Louise Bouchard and Guy-Vincent Jourdan.

Thursday, September 13, 2012 -- 14.15 – 15.45

Session 3: Privacy in Distributed Systems

- 14:30-14:55: EsPRESSo: Efficient Privacy-Preserving Evaluation of Sample Set Similarity, by Carlo Blundo, Emiliano De Cristofaro and Paolo Gasti.
- 14:55-15:20: SlopPy: Slope One with Privacy,
  by Sebastien Gambs and Julien Lolive.
- 15:20-15:45: A Semi-Lattice Model for Multi-Lateral Security, by Florian Kammueller.

Thursday, September 13, 2012 -- 16.15 – 17.45

- Invited Talk 2: Privacy in Distributed Systems Re-using existing security infrastructures, by Chris Mitchell (Royal Holloway, UK).

Friday, September 14, 2012 – 10.00– 10.45

Session 4: Privacy Policies

- 10:00-10:25: Prioritized execution of privacy policies,
  by Paolo Mori and Marinella Petrocchi.
- 10:25-10:50: What Websites Know About You - Privacy Policy Analysis Using Information Extraction, by Elisa Costante, Jerry Den Hartog and Milan Petkovic.

Friday, September 14, 2012 -- 11.15 – 12.45

Invited talk 3: Data Protection in Cloud Scenarios: Issues and Directions,
by Pierangela Samarati (Universita` degli Studi di Milano, Italy).

9th European PKI Workshop: Research and Applications (EuroPKI 2012)

Thursday, September 13, 2012 -- 09.15 – 09.30
Welcome

Thursday, September 13, 2012 -- 09.30 – 10.45
Invited talk

- Key Reuse in Public Key Cryptography: Theory and Practice
  Kenny Paterson

Thursday, September 13, 2012 -- 11.15 – 12.45
Session 1: Cryptographic Schemas and Protocols

- Analysis of Lattice Reduction Attack against the Somewhat Homomorphic Encryption Based on Ideal Lattices
  Masaya Yasuda, Jun Yajima, Takeshi Shimoyama, Jun Kogure
- Group Key Exchange Resilient to Leakage of Ephemeral Secret Keys with Strong Contributiveness
  Cheng Chen, Yanfei Guo, Rui Zhang

Thursday, September 13, 2012 -- 14.15 – 15.45
Session 2: Public Key Infrastructure

- How to avoid the Breakdown of Public Key Infrastructures - Forward Secure Signatures for Certificate Authorities
  Johannes Braun, Andreas Hulsing, Alex Wiesmaier, Martin A. G. Vigil, Johannes Buchmann
- Personal PKI for the Smart Device Era
  John Lyle, Andrew Paverd, Justin King-Lacroix, Andrea Atzeni, Habib Virji, Ivan Flechais, Shamal Faily
- The Notary Based PKI
  Martin Vigil, Cristian Moecke, Ricardo Custodio, Melanie Volkamer

Thursday, September 13, 2012 -- 16.15 – 17.15
Session 3: Wireless Authentication and Trusted Computing

- How to bootstrap trust among devices in home wireless environments via EAP-STLS
  Massimiliano Pala
- Anonymity Revocation through Standard Infrastructures
  Jesus Diaz, David Arroyo, Francisco B. Rodriguez

Friday, September 14, 2012 -- 09.30 – 10.45
Invited talk: Roberto Di Pietro

Friday, September 14, 2012 -- 11.15 – 12.45
Session 4: Digital Signature and Trusted Computing

- Cross-Unlinkable Hierarchical Group Signatures
  Julien Bringer, Herve Chabanne, Alain Patey

- Non-Interactive Public Accountability for Sanitizable Signatures
  Christina Brzuska, Henrich C. Pohls, and Kai Samelin
- Waltzing the Bear, or: A Trusted Virtual Security Module
  Ronald Toegl, Florian Reimair, and Martin Pirker

Friday, September 14, 2012 -- 14.15 – 15.15

Session 5: Certificates and Public Key Encryption

- GeoPKI: Translating Spatial Trust into Certificate Trust
  Tiffany Hyun-Jin Kim, Adrian Perrig, Virgil Gligor
- Efficient Public Key Encryption Admitting Decryption by Sender
  Puwen Wei, Yuliang Zheng

International Workshop on Quantitative Aspects in Security Assurance (QASA)

Friday, September 14, 2012 -- 09.15 – 10.45

Session 1: Quantitative information flow

- Invited Talk: Boris Koepf, Quantitative Information-Flow -- Fundamental Techniques and Applications to Side-Channel Analysis
- Vladimir Klebanov. Precise Quantitative Information Flow Analysis Using Symbolic Model Counting

Friday, September 14, 2012 -- 11.15 – 12.45

Session 2: Information flow, risk, cooperation and decision making.

- Adedayo Adetoye and Michael Goldsmith. From Qualitative to Quantitative Information Erasure
- Alessandro Aldini and Alessandro Bogliolo. Trading Performance and Cooperation Incentives in User-Centric Networks
- Gencer Erdogan, Fredrik Seehusen, Ketil Stølen and and Jan Aagedal. Assessing the Usefulness of Testing for Validating the Correctness of Security Risk Models Based on an Industrial Case Study
- Adam Beautement, Angela Sasse, David Pym, Simon Arnell, Philip Inglesant and Brian Monahan. Systematic decision making in security management:: Modelling password usage and support

Friday, September 14, 2012 -- 14.15 – 15.45

Session 3: Panel

- Panel on Quantitative Aspects of Security

Friday, September 14, 2012 -- 16.15 – 17.45

Session 4: Quantitative aspects in access and usage control

- Francisco Moyano, Carmen Fernández Gag and Javier Lopez. Implementing Trust and Reputation Systems: A Framework for Developers' Usage
- Leanid Krautsevich, Aliaksandr Lazouski, Paolo Mori and Artsiom Yautsiukhin. Quantitative Methods for Usage Control
- Charles Morisset. Implementing Access Control Markov Decision Processes with GLPK/GMPL

5th SETOP International Workshop on Autonomous and Spontaneous Security (SETOP 2012)

Thursday, September 13, 2012 -- 09.15 – 10.45

Session 1:

- Analyzing HTTP User Agent Anomalies for Malware Detection
  Nizar Kheir
- AS5: A Secure Searchable Secret Sharing Scheme for Privacy Preserving Database Outsourcing
  Mohammad Ali Hadavi, Ernesto Damiani, Rasool Jalili, Stelvio Cimato and Zeinab Ganjei

Thursday, September 13, 2012 -- 11.15 – 12.45

- Shared Session with DPM (in the DPM room)

Thursday, September 13, 2012 -- 14.15 – 15.45

Session 2:

- On Adaptable Markov Chain based Anomaly Detection in Wireless Sensor Networks
  Denise Dudek
- µSec: A Security Protocol for Unicast Communication in Wireless Sensor Networks
  Amrita Ghosal, Sanjib Sur and Sipra Das Bit
- Security Monitoring for Content-Centric Networking
  David Goergen, Thibault Cholez, Jérôme François and Thomas Engel

Thursday, September 13, 2012 -- 16.15 – 17.45

Session 3:

- Automated Smartphone Security Configuration
  William Michael Fitzgerald, Ultan Neville and Simon Foley
- Configuration Assessment as a Service
  Matteo Maria Casalino, Henrik Plate and Serena Elisa Ponta

Friday, September 14, 2012 -- 09.15 – 10.45

Session 4:

- Towards Session-Aware RBAC Delegation: Function Switch
  Meriam Ben Ghorbel Talbi, Frédéric Cuppens, Nora Cuppens-Boulahia and Stephane Morrucci
- Policy Chain for Securing Service Oriented Architectures
  Wihem Arsac, Annett Laube and Henrik Plate
- Towards a Temporal Response Taxonomy
  Wael Kanoun, Layal Samarji, Nora Cuppens-Boulahia, Samuel Dubus and Frédéric Cuppens

Friday, September 14, 2012 -- 11.15 – 12.45

Shared Session with DPM (in the DPM room)

8th International Workshop on Security and Trust Management (STM 2012)

Thursday, September 13, 2012 -- 09.15 – 10.45
Session 1: Policy Enforcement and Monitoring

- Cost-aware Runtime Enforcement of Security Policies
  Peter Drabik, Fabio Martinelli, and Charles Morisset
- Enforcing More with Less: Formalizing Target-aware Run-time Monitors
  Yannis Mallios, Lujo Bauer, Dilsun Kaynar, and Jay Ligatti
- Lazy Security Controllers
  Giulio Caravagna, Gabriele Costa, and Giovanni Pardini

Thursday, September 13, 2012 -- 11.15 – 12.45
Session 2: Access control

- Automated Analysis of Scenario-based Specifications of Distributed Access Control Policies with Non-Mechanizable Activities
  Michele Barletta, Silvio Ranise, and Luca Viganò
- Labeled Goal-directed Search in Access Control Logic
  Valerio Genovese, Deepak Garg, and Daniele Rispoli
- A Use-based Approach for Enhancing UCON
  Christos Grompanopoulos, Antonios Gouglidis, and Ioannis Mavridis
- Analysis of Communicating Authorization Policies
  Simone Frau and Mohammad Torabi Dashti

Thursday, September 13, 2012 -- 14.15 – 15.45
Session 3: Trust, Reputation, and Privacy

- Building Trust and Reputation In: A Development Framework for Trust Models Implementation
  Francisco Moyano, Carmen Fernandez-Gago, and Javier Lopez
- Matrix Powers Algorithms for Trust Evaluation in Public-Key Infrastructures
  Jean-Guillaume Dumas and Hicham Hossayni
- Formal Modelling of (De)Pseudonymisation: A Case Study in Health Care Privacy
  Meilof Veeningen, Benne de Weger, and Nicola Zannone

Thursday, September 13, 2012 -- 16.15 – 17.45

ERCIM PhD Award Talk

Friday, September 14, 2012 -- 09.15 – 10.45
Session 5: Distributed Systems and Physical Security

- Switchwall: Automated Topology Fingerprinting & Behavior Deviation Identification
  Nelson Nazzicari, Javier Almillategui, Angelos Stavrou, and Sushil Jajodia
- DOT-COM: Decentralized Online Trading and COMmerce
  Moti Geva and Amir Herzberg
- Formalizing Physical Security Procedures
  Catherine Meadows and Dusko Pavlovic

Friday, September 14, 2012 -- 11.15 – 12.45

Session 6: Authentication

- A PUF-based Authentication Protocol to Address Ticket-Switching of RFID-tagged Items
  Sjouke Mauw and Selwyn Piramuthu
- Authenticating Email Search Results
  Olga Ohrimenko, Hobart Reynolds, and Roberto Tamassia
- Software Authentication to Enhance Trust in Body Sensor Networks
  Joep de Groot, Vinh Bui, Jean-Paul Linnartz, Johan Lukkien, and Richard Verhoeven
- YubiSecure? Formal Security Analysis Results for the Yubikey and YubiHSM
  Robert Künnemann and Graham Steel

Friday, September 14, 2012 -- 14.15 – 15.45

Session 7: Security Policies

- Boosting Model Checking to Analyse Large ARBAC Policies
  Silvio Ranise, Anh Truong, and Alessandro Armando
- Constrained Role Mining
  Carlo Blundo and Stelvio Cimato
- A Datalog Semantics for Paralocks
  Bart van Delft, Niklas Broberg, and David Sands