### September 10, 2012 -- 10.45 – 12.45

**Session 1A: Security and data protection in real systems**

- 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**

- 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

- 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

- 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

- 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

- Exploring Linkability 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 -- 10.45 – 12.45

Session 4A: Location privacy

- 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

- 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

- 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

- Decision Procedures for Simulatability (Charanjit Jutla and Arnab Roy)
Tuesday, September 11, 2012 -- 16.15 – 17.45

Session 6A: Identity based encryption and group signature

- 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

- 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 -- 10.45 – 12.45

Session 7: Encryption key and password security

- 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

- 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

- 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)