ESORICS 2017 Workshop Programme

CyberICPS 2017

Friday, September 15 (Room: Møterom)

09:00 – 10:30 Session 1: Protecting Industrial Control and Cyber-Physical Systems

- *Vasily Mikhalev, Laurent Gomez, Frederik Armknecht and José Márquez*. "Towards End-to-End Data Protection in Low Power Networks".
- *Vincent Raes, Vincent Naessens and Jan Vossaert*. "Development of an Embedded Platform for Secure CPS Services".
- *Antonio La Marra, Fabio Martinelli, Paolo Mori, Athanasios Rizos and Andrea Saracino*. "Introducing Usage Control in MQTT protocol for IoT". (SHORT PAPER)

10:30 – 11:00 Coffee Break

11:00 – 12:30 Session 2: Threats, Vulnerabilities and Risks

- *Katja Tuma, Riccardo Scandariato, Mathias Widman and Christian Sandberg*. "Towards security threats that matter".
- *Bastien Sultan, Fabien Dagnat and Caroline Fontaine.* "A Methodology to Assess Vulnerabilities and Countermeasures Impact on the Missions of a Naval System".
- *Bojan Jelacic, Daniela Rosic, Imre Lendak, Marina Stanojevic and Sebastijan Stoja*. "STRIDE to a secure Smart Grid in a hybrid cloud".

12:30 – 14:00 Lunch Break

14:00 – 15:30 Session 3: Cyber Attacks in Industrial Control and Cyber-Physical Systems

- *Amit Kleinmann, Avishai Wool, Ori Amichay, David Tenenbaum, Ofer Bar and Leonid Lev*. "Stealthy Deception Attacks Against SCADA Systems".
- *Naman Govil, Anand Agrawal and Nils Ole Tippenhauer*. "On Ladder Logic Bombs in Industrial Control Systems".
- *Eyasu Getahun Chekole, John Henry Castellanos, Martín Ochoa and David Yau*. "Enforcing Memory Safety in Cyber-Physical Systems".

15:30 – 16:00 Coffee Break

16:00 – 17:30 Session 4: Detecting Attacks in Industrial Control and Cyber-Physical Systems

- *Kirsi Helkala, Benjamin J. Knox, Øyvind Jøsok, Rigardo G. Lugo, Stefan Sütterlin, Geir Olav Dyrkolbotn and Nils Kalstad Svendsen*. "Supporting the Human in Cyber Defence".
- *Ambika Shrestha Chitrakar and Slobodan Petrovic*. "CRBP-OpType: A Constrained Approximate Search Algorithm for Detecting Similar Attack Patterns".
- *Rizwan Qadeer, Carlos Murguia, Chuadhry Mujeeb Ahmed and Justin Ruths*. "Multistage Downstream Attack Detection in a Cyber Physical System". (SHORT PAPER)

ESORICS 2017 Workshop Programme

SECPRE 2017

Thursday, September 14 (Room: Bakgården Møterom)

09:00-10:30 Session 1: Designing a security assurance framework under V2I connectivity use cases: The SAFERtec approach and vision *(Presentations)*

10:30-11:00 Coffee Break

11:00-12:30 Session 2: Designing a security assurance framework under V2I connectivity use cases: The SAFERtec approach and vision *(Discussion)*

12:30-14:00 Lunch

Friday, September 15, 2017 (Room: Hovedsal)

14:00-15:30 Session 3: Security and Privacy Requirements Assurance and Evaluation

14:00-14:30: Keynote (TBA)
14:30-15:00: *Majed Alshammari and Andrew Simpson*. **A UML Profile for Privacy-Aware Data Lifecycle Models**
15:00-15:30: *Vasiliki Diamantopoulou, Michalis Pavlidis and Haralambos Mouratidis*. ***Evaluation of a Security and Privacy Requirements Methodology using the Physics of Notation***

15:30-16:00 Coffee Break

16:00-17:30 Session 4: Security Requirements Elicitation and Modelling

16:00-16:30: *Vivien Rooney and Simon Foley*. ***What users want: adapting qualitative research methods to security requirements elicitation***
16:30-17:00: *Mohammad Torabi Dashti and Sasa Radomirovic*. ***An Anti-Pattern for Misuse Cases***
17:00-17:30: *Nikolaos Argyropoulos, Konstantinos Angelopoulos, Haralambos Mouratidis and Andrew Fish*. ***Decision-Making in Security Requirements Engineering with Constrained Goal Models***

ESORICS 2017 Workshop Programme

SecSE 2017

Thursday, September 14 (Room: Bakgården Møterom)

14:00-14:45 Keynote talk "Experiences with Continuous Deployment and Software Security in Google, Netflix, Facebook and others". *Laurie Williams*

14:45-15:00 "Research challenges in empowering agile teams with security knowledge based on public and private information sources". *Michael Felderer*

15:00-15:15 "Comparing Capability of Static Analysis Tools to Detect Security Weaknesses in Mobile Applications". *Marcos Chaim*

15:15-15:30 Ignite talks

15:30-16:00 Break

16:00-16:20 "Teaching Secure Software Development Through an Online Course". *Laurie Williams*

16:20-16:40 "Managing Security Work in Scrum: Tensions and Challenges". *Andreas Poller*

16:40-16:55 Ignite talks

16:55-17:15 "Dynamic Security Assurance in Multi-Cloud DevOps". *Erkuden Rios*

17:15-17:30 "SECBENCH: A Database of Real Security Vulnerabilities". *Sofia Reis*

ESORICS 2017 Workshop Programme

QASA 2017

Friday, September 15 (Room: Big Time)

14:00 - 15:30 Session 1: Trust, insurance and authentication

(Chair: Artsiom Yautsiukhin)

- **14:00-14:30 A Trust by Design approach for the Internet of Things.** *Davide Ferraris* (University of Malaga).
- **14:30-15:00 Cyber insurance and security interdependence: friends or foes?** *Ganbayar Uuganbayar* (CNR)
- **15:00-15:30 Demystifying Authentication in Smartphones: Types and Ways to Secure Access.** *Sandeep Gupta* (University of Trento)

15:30 - 16:00 Coffee Break

16:00-17:00 Session 2: Privacy and CTI sharing

(Chair: Artsiom Yautsiukhin)

- **16:00-16:30 An Architecture for Privacy-preserving Sharing of CTI with 3rd party Analysis Services** *Fabio Giubilo* (BT)
- **16:30-17:00 Description and analysis of email with malicious attachment within STIX framework** *Oleksii Osliak* (CNR)

ESORICS 2017 Workshop Programme

CBT 2017

Thursday, September 14 (Room: Møterom)

08:00 - 09:00 Registration

09:00 - 09:30 General Welcome

09:30 - 10:30 Keynote speaker

- **A Blockchain with Strong Consistency?**
  By Roger Wattenhofer.

10:30 - 11:00 Coffee Break

11:00 - 12:30 Session 1: Consensus and smart contracts

- **11:00-11:30 - Securing Proof-of-Stake Blockchain Protocols.**
  By Wenting Li, Sebasiten Andreina, Jens-Matthias Bohli and Ghassan Karame.
- **11:30-12:00 - Merged Mining: Curse or Cure?**
  By Aljosha Judmayer, Alexei Zamyatin, Nicholas Stifter, Artemios Voyiatzis and Edgar Weippl.
- **12:00-12:30 - Atomically Trading with Roger: Gambling on the success of a hardfork.**
  By Patrick McCorry, Ethan Heilman and Andrew Miller.

12:30 - 14:00 Lunch

14:00 - 15:30 Session 2: Smart contracts and blockchain identity

- **14:00-14:30 - In Code We Trust? Measuring the Control Flow Immutability of All Smart Contracts Deployed on Ethereum.**
  By Michael Fröwis and Rainer Böhme.
- **14:30-15:00 - Who Am I? Secure Identity Registration on Distributed Ledgers.**
  By Sarah Azouvi, Mustafa Al-Bassam and Sarah Meiklejohn.
- **15:00-15:30 - A User-centric System for Verified Identities on the Bitcoin Blockchain.**
  By Daniel Augot, Hervé Chabanne, Thomas Chenevier, William George and Laurent Lambert.

15:30 - 16:00 Coffee Break and poster session.

16:00-17:30 Session 3: Short papers

- **16:00-16:20 - Towards a Concurrent and Distributed Route Selection for Payment Channel Networks.**
  By Elias Rohrer, Jann-Frederik Laß and Florian Tschorsch.

- **16:20-16:40 - Graphene: A New Protocol for Block Propagation Using Set Reconciliation.**
  By A. Pinar Ozisik, Gavin Andresen, George Bissias, Amir Houmansadr and Brian N. Levine.
- **16:40-17:00 - Revisiting Difficulty Control for Blockchain Systems.**
  By Dmitry Meshkov, Alexander Chepurnoy and Marc Jansen.
- **17:00-17:20 - Secure Event Tickets on a Blockchain.**
  By Björn Tackmann.

17:20 - 17:30 Farewell

ESORICS 2017 Workshop Programme

DPM 2017

Thursday, September 14 (Room: Big Time)

09:00 - 09:15 General Welcome

09:15 - 10:30 Keynote

- **Privacy models and disclosure risk: integral privacy**
  Vicenç Torra (University of Skövde)

10:30 - 11:00 Coffee Break

11:00 - 12:30 Session 1: Privacy, logics, and computational models

(Chair: Joaquin Garcia-Alfaro)

- **11:00-11:30 A Proof Calculus for Attack Trees in Isabelle.**
  By Florian Kammueller (Middlesex University London and TU Berlin).
- **11:30-12:00 Confidentiality of Interactions in Concurrent Object-Oriented Systems.**
  By Olaf Owe (University of Oslo), Toktam Ramezanifarkhani (University of Oslo).
- **12:00-12:30 Using Oblivious RAM in Genomic Studies.**
  By Nikolaos Karvelas (TU Darmstadt), Andreas Peter (University of Twente), Stefan Katzenbeisser (TU Darmstadt).

12:30 - 14:00 Lunch

14:00 - 15:30 Session 2: Privacy and encrypted search

(Chair: Guillermo Navarro-Arribas)

- **14:00-14:30 Towards Efficient and Secure Encrypted Databases: Extending Message-Locked Encryption in Three-Party Model.**
  By Yuuji Furuta (Osaka University), Naoto Yanai (Osaka University), Masashi Karasaki (Nippon Telegraph and Telephone West Corporation), Katsuhiko Eguchi (Nippon Telegraph and Telephone West Corporation), Yasunori Ishihara (Osaka University), Toru Fujiwara (Osaka University).
- **14:30-15:00 Searchable Encrypted Relational Databases: Risks and Countermeasures.**
  By Mohamed Ahmed Abdelraheem (SICS), Tobias Andersson (SICS), Christian Gehrmann (Lund University).
- **Private verification of access on medical data: an initial study**
  By Thais Bardini Idalino (University of Ottawa), Dayana Spagnuelo (University of Luxembourg), Jean Everson Martina (Universidade Federal de Santa Catarina).

15:30 - 16:00 Coffee Break

16:00-17:30 Session 3: Data Privacy, data mining, and applications

(Chair: Florian Kammueller)

- **16:00-16:25 Default Privacy Setting Prediction by Grouping User's Attributes and Settings Preferences**
  By Toru Nakamura (KDDI Research, Inc.), Welderufael Berhane Tesfay (Goethe University Frankfurt), Shinsaku Kiyomoto (KDDI Research, Inc.), Jetzabel Serna (Goethe University Frankfurt).
- **16:25-16:50 δ-privacy: Bounding Privacy Leaks in Privacy Preserving Data Mining.**
  By Zhizhou Li (The Voleon Group), Ten H. Lai (The Ohio State University).
- **16:50-17:15 Threshold Single Password Authentication.**
  By Devriş Işler (Koç University), Alptekin Küpçü (Koç University).
- **17:15-17:40 Towards A Toolkit for Utility and Privacy-Preserving Transformation of Semi-structured Data Using Data Pseudonymization.**
  By Saffija Kasem-Madani (University of Bonn), Michael Meier (University of Bonn), Martin Wehner (University of Bonn).

17:30-20:00 Aperitif in Gamle Museet

Friday, September 15 (Room: Big Time)

09:00 - 10:30 Session 4: User privacy

(Chair: Jordi Herrera-Joancomarti)

- **09:00-09:30 Privacy Dashcam - Towards Lawful Use of Dashcams Through Enforcement of External Anonymization.**
  By Paul Wagner (Karlsruhe Institute of Technology), Pascal Birnstill (Fraunhofer IOSB), Erik Krempel (Fraunhofer IOSB), Sebastian Bretthauer (Karlsruhe Institute of Technology), Jürgen Beyerer (Fraunhofer IOSB).
- **09:30-10:00 DLoc: Distributed Auditing for Data Location Compliance in Cloud.**
  Mojtaba Eskandari (University of Trento), Bruno Crispo (University of Trento), Anderson Santana De Oliveira (SAP).
- **10:00-10:30 Inonymous: Anonymous Invitation-Based System.**
  By Sanaz Taheri Boshrooyeh (Koç University), Alptekin Küpçü (Koç University).

10:30 - 11:00 Coffee Break

11:00 - 12:40 Session 5: Applied Cryptography and Privacy

(Chair: Cristina Perez-Sola)

- **11:00-11:30 PCS, a privacy-preserving certification scheme.**
  By Nesrine Kaaniche (Telecom SudParis), Maryline Laurent (Telecom SudParis), Pierre-Olivier Rocher (Telecom SudParis), Christophe Kiennert (Telecom SudParis), Joaquin Garcia-Alfaro (Telecom SudParis).

- **11:30-12:00 Order-Preserving Encryption Using Approximate Integer Common Divisors.**
  By James Dyer (University of Manchester), Martin Dyer (University of Leeds), and Jie Xu (University of Leeds).
- **12:00-12:30 Privacy-Preserving Deterministic Automata Evaluation with Encrypted Data Blocks.**
  By Giovanni Di Crescenzo (Vencore Labs), Brian Coan (Vencore Labs), Jonathan Kirsch (Vencore Labs).

12:30 - 12:40 Concluding Remarks

12:40 - 14:00 Lunch & Farewell

ESORICS 2017 Workshop Programme

STM 2017

Thursday, September 14 (Room: Hovedsal)

8.45 - 9.00 Welcome and opening

9.00 - 10.30 Session 1: Cryptosystems and Applied Cryptography

- *Kazuto Ogawa, Sakurako Tamura and Goichiro Hanaoka*. “Key Management for Versatile Pay-TV Services”
- *Daniel Homann, Christian Göge and Lena Wiese*. “Dynamic Similarity Search over Encrypted Data with Low Leakage”
- *Papa B. Seye and Augustin P. Sarr*. “Enhanced Modelling of Authenticated Key Exchange Security”

10.30 - 11.00 Coffee Break

11.00 - 12.30 Session 2: Software Security and Risk Management

- *Job Noorman, Jan Tobias Mühlberg and Frank Piessens*. “Authentic Execution of Distributed Event-Driven Applications with a Small TCB”
- *William Dash and Matthew J. Craven*. “Exploring Botnet Evolution via Multidimensional Models and Visualisation”
- *Per Håkon Meland, Inger Anne Tøndel, Marie Moe and Fredrik Seehusen*. «Facing uncertainty in cyber insurance policies”

12.30 - 14.00 Lunch Break

14.00 - 15.20 Session 3: Authorization

- *Hiroaki Kikuchi, Koichi Niihara and Michihiro Yamada*. “How much is risk increased by sharing credential in a group?”
- *Giacomo Giorgi, Antonio La Marra, Fabio Martinelli, Paolo Mori and Andrea Saracino*. “Smart Parental Advisory: A Usage Control and Deep Learning-based Framework for Dynamic Parental Control on Smart TV”
- *Audun Jøsang*. “A Consistent Definition of Authorization”

15.30 - 16.00 Coffee Break

16.00 - 17.00 Session 4: ERCIM STM Ph.D. award talk

Friday, September 15, 2017 (Room: Hovedsal)

9.10 - 10.30 Session 5: Security Vulnerabilities and Protocols

- *Jorden Whitefield, Liqun Chen, Frank Kargl, Andrew Paverd, Steve Schneider, Helen Treharne and Steve Wesemeyer*. “Formal Analysis of V2X Revocation Protocols”

- *Olga Gadyatskaya, Ravi Jhawar, Sjouke Mauw, Rolando Trujillo-Rasua and Tim A. C. Willemse.* “Refinement-Aware Generation of Attack Trees”
- *László Erdödi and Audun Jøsang*. “Exploit Prevention, Quo Vadis?”

10.30 - 11.00 Coffee Break

11.00 - 12.20 Session 6: Secure Systems

- *Daniele Canavese, Leonardo Regano, Cataldo Basile and Alessio Viticchié*. “Estimating Software Obfuscation Potency with Artificial Neural Networks”
- *Kalonji Kalala, Tao Feng and Iluju Kiringa*. “EigenTrust for Hierarchically Structured Chord”
- *Tim Grube, Markus Thummerer, Jörg Daubert and Max Mühlhäuser*. “Cover Traffic: A Trade of Anonymity and Efficiency”
- *Luca Arnaboldi and Charles Morisset*. “Quantitative Analysis of DoS attacks & Client Puzzles in IoT Systems”

12.30 - 14.00 Lunch

ESORICS 2017 Workshop Programme

SIoT 2017

Friday, September 15 (Room: Bakgården Møterom)

09:00 - 09:10 Welcome Message

09:10 - 10:30 Session 1 - Analysis and methods for secure IoT

Earworms Make Bad Passwords: An Analysis of the Noke Smart Lock Manual Override.
Jack Mcbride, Julio Hernandez-Castro and Budi Arief

- Offline Trusted Device and Proxy Architecture based on a new TLS Switching technique.
  Denis Migdal, Christian Johansen and Audun Josang
- Behavioral Authentication Method Utilizing Wi-Fi History Information Captured by IoT Device. *Ryosuke Kobayashi and Rie Yamaguchi*

10:30 - 11:00 Coffee Break

11:00 - 12:30 Session 2 - Access Control for IoT infrastructures

Securing Complex IoT Platforms with Token Based Access Control and Authenticated Key Establishment. *Timothy Claeys, Franck Rousseau and Bernard Tourancheau*

- Adaptive risk-aware access control model for Internet of Things
  Annanda Thavymony Rath and Jean-Noel Colin

12:30 - 12:45 Closing Remarks