ESORICS 2017 Conference Programme

MONDAY / SEP 11	
09:00 - 09:30	Introductions • General Chair • Organisation Chair • PC Chairs
09:30 – 10:30	**Keynote 1: Cormac Herley** "Justifying Security Measures" *Session Chair: Simon Foley*
10:30 – 11:00	Coffee break: coffee and fruit
11:00 – 12:30	**Session 1: Security of embedded things** *Session Chair: Frederic Cuppens* • Antonino Rullo, Edoardo Serra, Elisa Bertino and Jorge Lobo. "Shortfall-based Optimal Placement of Security Resources for Mobile IoT Scenarios" • Sibylle Froeschle and Alexander Stühring. "Analyzing the Capabilities of the CAN Attacker" • Steffen Schulz, André Schaller, Florian Kohnhäuser and Stefan Katzenbeisser. "Boot Attestation: Secure Remote Reporting with Off-The-Shelf IoT Sensors"
11:00 – 12:30	**Session 2: Cryptographic Application I** *Session Chair: Frederik Armknecht* • Gregory Demay, Peter Gazi, Ueli Maurer and Björn Tackmann. "Per-Session Security: Password-Based Cryptography Revisited" • Fabrice Benhamouda, Houda Ferradi, Rémi Géraud and David Naccache. "Non-Interactive Provably Secure Attestations for Arbitrary RSA Prime Generation Algorithm" • Martin Albrecht, Emmanuela Orsini, Kenneth Paterson, Guy Peer and Nigel Smart. "Tightly Secure Ring-LWE Based Key Encapsulation with Short Ciphertexts"
12:30 – 14:00	Lunch: specialty from Valdres in Buskerud
14:00 – 15:30	**Session 3: Documents and Authorship** *Session Chair: Pierangela Samarati* • Xiaozhu Meng, Barton Miller and Kwang-Sung Jun. "Identifying Multiple Authors in a Binary Program" • Herve Chabanne, Rodolphe Hugel and Julien Keuffer. "Verifiable Document Redacting" • Bander Alsulami, Edwin Dauber, Richard Harang, Spiros Mancoridis and Rachel Greenstadt. "Source Code Authorship Attribution using Long Short-Term Memory Based Networks"
14:00 – 15:30	**Session 4: Analysis of Security Protocols** *Session Chair: Peter Ryan* • Ivan Gazeau and Steve Kremer. "Automated analysis of equivalence properties for security protocols using else branches"

	• Cas Cremers, Martin Dehnel-Wild and Kevin Milner. "Secure Authentication in the Grid: A formal analysis of DNP3: SAv5" • Matthew Bauer, Rohit Chadha and Mahesh Viswanathan. "Modular Verification of Protocol Equivalence in the Presence of Randomness"
15:30 – 16:00	Coffee break: coffee and cake
16:00 – 17:30	**Session 5: Threat Analysis** *Session chair: Sushil Jajodia* • Juan E. Rubio, Cristina Alcaraz and Javier Lopez. "Preventing Advanced Persistent Threats in Complex Control Networks# • Alexandru G. Bardas, Sathya C. Sundaramurthy, Xinming Ou and Scott A. Deloach. "MTD CBITS: Moving Target Defense for Cloud-Based IT Systems" • Maxime Audinot, Sophie Pinchinat and Barbara Kordy. "Is my attack tree correct?"
16:00 – 17:30	**Session 6: Side Channels and data leakage** *Session Chair: Paul Syverson* • Kai Engelhardt. "A Better Composition Operator for Quantitative Information Flow Analyses" • Mordechai Guri, Yosef Solewicz, Andrey Daidakulov and Yuval Elovici. "Acoustic Data Exfiltration from Speakerless Air-Gapped Computers via Covert Hard-Drive Noise" • Moritz Lipp, Daniel Gruss, Michael Schwarz, David Bidner, Clémentine Maurice and Stefan Mangard. "Practical Keystroke Timing Attacks in Sandboxed JavaScript"
17:30 – 20:00	**Aperitiv in Gamle Museet**
TUESDAY / SEP 12	
09:00 – 10:00	**Keynote 2: Paul Syverson** "The Once and Future Onion" *Session Chair: Einar Snekkenes*
10:00 – 10:30	Group photo and Coffee break: coffee and fruit
10:30 – 12:00	**Session 7: Vulnerabilities and Malware** *Session Chair: Nora Cuppens- Boulahia* • Lorenzo Bordoni, Mauro Conti and Riccardo Spolaor. "Mirage: Toward a Stealthier and Modular Malware Analysis Sandbox for Android" • Siqi Ma, Ferdian Thung, David Lo, Cong Sun and Robert Deng. "VuRLE: Automatic Vulnerability Detection and Repair by Learning from Examples" • Kathrin Grosse, Nicolas Papernot, Praveen Manoharan, Backes Michael and Patrick McDaniel. "Adversarial Examples for Malware Detection"
10:30 – 12:00	**Session 8: Privacy in Systems** *Session Chair: Sibylle Froschle*

	• Berk Gulmezoglu, Andreas Zankl, Thomas Eisenbarth and Berk Sunar. "PerfWeb: How to Violate Web Privacy with Hardware Performance Events" • Iraklis Symeonidis, Abdelrahaman Aly, Mustafa Asan Mustafa, Bart Mennink, Siemen Dhooghe and Bart Preneel. "SePCAR: A Secure and Privacy-enhancing Protocol for Car Access Provision" • Philipp Morgner, Christian Müller, Matthias Ring, Björn Eskofier, Christian Riess, Frederik Armknecht and Zinaida Benenson. "Privacy Implications of Room Climate Data"
12:00 – 13:30	Lunch: specialty from Gårsand in Vestfold
13:30 – 15:00	**Session 9: Network security** *Session Chair: Javier Lopez* • Rajib Ranjan Maiti, Sandra Siby, Ragav Sridharan and Nils Ole Tippenhauer. "Link-Layer Device Type Classification on Encrypted Wireless Traffic with COTS Radios" • Soyoung Kim, Sora Lee, Geumhwan Cho, Muhammad Ejaz Ahmed, Jaehoon Paul Jeong and Hyoungshick Kim. "Preventing DNS amplification attacks using the history of DNS queries with SDN" • Jacqueline Brendel and Marc Fischlin. "Zero Round-Trip Time for the Extended Access Control Protocol"
13:30 – 15:00	**Session 10: Controlling Access** *Session Chair: Marina Blanton* • Panagiotis Papadopoulos, George Christou, Giorgos Vasiliadis, Evangelos Markatos and Sotiris Ioannidis. "No sugar but all the taste! Memory Encryption without Architectural Support" • James Alderman, Naomi Farley and Jason Crampton. "Tree-based Cryptographic Access Control" • Swarup Chandra, Vishal Karande, Zhiqiang Lin, Latifur Khan, Murat Kantarcioglu and Bhavani Thuraisingham. "Securing Data Analytics on SGX With Randomization"
15:00 – 15:30	Coffee break: coffee and cake
15:30 – 17:00	**Session 11: Information Flow** *Session Chair: Heiko Mantel* • Musard Balliu, Daniel Schoepe and Andrei Sabelfeld. "We are Family: Relating Information-Flow Trackers" • Weijie Liu, Debin Gao and Mike Reiter. "On-Demand Time Blurring to Support Side-Channel Defense" • Abhishek Bichhawat, Vineet Rajani, Jinank Jain, Deepak Garg and Christian Hammer. "WebPol: Fine-grained Information Flow Policies for Web Browsers"
15:30 – 17:00	**Session 12: Blockchain and social networks** *Session Chair: Joaquin Garcia-Alfaro* • Amrit Kumar, Clément Fischer, Shruti Tople and Prateek Saxena. "A Traceability Analysis of Monero's Blockchain"

	• Shi-Feng Sun, Man Ho Au, Joseph Liu and Tsz Hon Yuen. "RingCT 2.0: A Compact Linkable Ring Signature Based Protocol for Blockchain Cryptocurrency Monero" • Foteini Baldimtsi, Dimitrios Papadopoulos, Stavros Papadopoulos, Alessandra Scafuro and Nikos Triandopoulos. "Secure Computation in Online Social Networks"
19:00 – 19:15	Meeting at Gamle museet to walk to Gala Dinner venue
19:30 – 20:00	**Aperitiv in Stratos (Youngstorget 2A)**
20:00 – 24:00	**GALA DINNER in Stratos (Youngstorget 2A)**
WEDNESDAY / SEP 13	
09:00 – 10:00	**Keynote 3: Sandro Etalle** "From Intrusion Detection to Software Design" *Session Chair: Dieter Gollmann*
10:00 – 10:30	Coffee break: coffee and fruit
10:30 – 12:00	**Session 13: Web Security** *Session Chair: Cormac Herley* • Igino Corona, Battista Biggio, Matteo Contini, Luca Piras, Roberto Corda, Mauro Mereu, Guido Mureddu, Davide Ariu and Fabio Roli. "DeltaPhish: Detecting Phishing Webpages in Compromised Websites" • Mario Heiderich, Christopher Späth and Jörg Schwenk. "DOMPurify: Client-Side Protection against XSS and Markup Injection" • Arthur Gervais, Alexandros Filios, Vincent Lenders and Srdjan Capkun. "Quantifying Web Adblocker Privacy"
10:30 – 12:00	**Session 14: Cryptographic signatures** *Session Chair: Nigel Smart* • Marc Beunardeau, Aisling Connolly, Houda Ferradi, Remi Geraud, David Naccache and Damien Vergnaud. "Reusing Nonces in Schnorr Signatures" • Essam Ghadafi. "More Efficient Structure-Preserving Signatures - Or: Bypassing the Type-III Lower Bounds" • Ahto Buldas, Aivo Kalu, Peeter Laud and Mart Oruaas. "Server-Supported RSA Signatures for Mobile Devices"
12:00 – 13:30 13:00 – 13:30	Lunch: specialty from Persgaard in Sandefjord Optional: Game of Oslo
13:30 – 15:00	**Session 15: Formal techniques** *Session Chair: Audun Josang* • Joachim Biskup and Marcel Preuß. "Inference-Proof Updating of a Weakened View Under the Modification of Input Parameters" • Sandrine Blazy, David Pichardie and Alix Trieu. "Verifying Constant-Time Implementations by Abstract Interpretation" • Florian Dewald, Heiko Mantel and Alexandra Weber. "AVR Processors as a Platform for Language-Based Security"
13:30 – 15:00	**Session 16: Privacy and garbled circuits**

	Session Chair: Slobodan Petrovic • Manuel Barbosa, Dario Catalano and Dario Fiore. "Labeled Homomorphic Encryption: Scalable and Privacy-Preserving Processing of Outsourced Data" • Raymond K. H. Tai, Jack P. K. Ma, Yongjun Zhao and Sherman S. M. Chow. "Privacy-Preserving Decision Trees Evaluation via Linear Functions" • Yihua Zhang, Marina Blanton and Fattaneh Bayatbabolghani. "Enforcing Input Correctness via Certification in Garbled Circuit Evaluation"
15:00 – 15:30	Coffee break: coffee and cake Game of Oslo Winner Award
15:30 – 17:00	**Session 17: Intrusion Detection** *Session Chair: Sokratis Katsikas* • Shohei Miyama and Kenichi Kourai. "Secure IDS Offloading with Nested Virtualization and Deep VM Introspection" • Genki Osada, Kazumasa Omote and Takashi Nishide. "Network Intrusion Detection based on Semi-Supervised Variational Auto-Encoder" • Suryadipta Majumdar, Yosr Jarraya, Momen Oqaily, Amir Alimohammadifar, Makan Pourzandi, Lingyu Wang and Mourad Debbabi. "LeaPS: Learning-Based Proactive Security Auditing for Clouds"
15:30 – 17:00	**Session 18: Cryptographic Applications II** *Session Chair: Björn Tackmann* • David Leslie, Chris Sherfield and Nigel Smart. "Multiple Rate Threshold FlipThem" • Sam L. Thomas, Tom Chothia and Flavio D. Garcia. "Stringer: Measuring the Importance of Static Data Comparisons to Detect Backdoors and Undocumented Functionality" • Kotoko Yamada, Nuttapong Attrapadung, Keita Emura, Goichiro Hanaoka and Keisuke Tanaka. "Generic Constructions for Fully Secure Revocable Attribute-Based Encryption"