MONDAY, 23 SEPTEMBER, 2019

09:00 - 10:00 | Keynote | Europe A

The Insecurity of Machine Learning: Problems and Solutions
Prof. Dr. Adi Shamir, Weizmann Institute of Science, Israel

10:00 - 10:30 | Coffee Break

10:30 - 12:10 | Room TBC

Machine Learning

Privacy-Enhanced Machine Learning with Functional Encryption
Miha Stopar, Tilen Marc, Jan Hartman, Manca Bizjak and Jolanda Modic

Towards Secure and Efficient Outsourcing of Machine Learning Classification
Yifeng Zheng, Huayi Duan and Cong Wang

Confidential Boosting with Random Linear Classifiers for Outsourced User-generated Data
Sagar Sharma and Keke Chen

BDPL: A Boundary Differentially Private Layer Against Machine Learning Model Extraction Attacks
Huadi Zheng, Qingqing Ye, Haibo Hu, Chengfang Fang and Jie Shi

10:30 - 12:10 | Room TBC

Information Leakage

The Leakage-Resilience Dilemma
Bryan Ward, Richard Skowyra, Chad Spensky, Jason Martin and Hamed Okhravi

A Taxonomy of Attacks using BGP Blackholing
Loïc Miller and Cristel Pelsser

Local Obfuscation Mechanisms for Hiding Probability Distributions
Yusuke Kawamoto and Takao Murakami

A First Look into Privacy Leakage in 3D Mixed Reality Data
Jaybie de Guzman, Kanchana Thilakarathna and Aruna Seneviratne

12:10 - 13:45 | Lunch

13:45 - 15:25 | Room TBC

Signatures and Re-Encryption

Flexible Signatures: Making Authentication Suitable for Real-Time Environments
Duc Le, Mahimna Kelkar and Aniket Kate

A Dynamic & Revocable Group Merkle Signature
Maxime Buser, Joseph K. Liu, Ron Steinfeld, Amin Sakzad and Shi-Feng Sun

Puncturable Proxy Re-Encryption supporting to Group Messaging Service
Tran Viet Xuan Phuong, Willy Susilo, Guomin Yang, Jongkil Kim and Dongxi Liu

Generic Traceable Proxy Re-Encryption and Accountable Extension in Consensus Network
Hui Guo, Zhenfeng Zhang, Jing Xu and Mingyuan Xia

13:45 - 15:25 | Room TBC

Side Channels

Side-Channel Aware Fuzzing
Philip Sperl and Konstantin Böttinger

NetSpectre: Read Arbitrary Memory over Network
Michael Schwarz, Martin Schwarzl, Moritz Lipp, Jon Masters and Daniel Gruss

maskVerif: Automated Verification of Higher-Order Masking in Presence of Physical Defaults
Gilles Barthe, Sonia Belaïd, Gaëtan Cassiers, Pierre-Alain Fouque, Benjamin Grégoire and François-Xavier Standaert

Automated Formal Analysis of Side-Channel Attacks on Probabilistic Systems
Chris Novakovic and David Parker

15:25 - 15:55 | Coffee Break

15:55 - 17:35 | Room TBC

Formal Modelling and Verification

A Formal Model for Checking Cryptographic API Usage in JavaScript
Duncan Mitchell and Johannes Kinder

Contingent Payments on a Public Ledger: Models and Reductions for Automated Verification
Sergiu Bursuc and Steve Kremer

Symbolic Analysis of Terrorist Fraud Resistance
Alexandre Debant, Stephanie Delaune and Cyrille Wiedling

Secure Communication Channel Establishment: TLS 1.3 (Over TCP Fast Open) vs. QUIC
Shan Chen, Samuel Jero, Matthew Jagielski, Alexandra Boldyreva and Cristina Nita-Rotaru

15:55 - 18:00 | Room TBC

Attacks

Where to Look for What You See Is What You Sign? User Confusion in Transaction Security
Vincent Haupert and Stephan Gabert

On the Security and Applicability of Fragile Camera Fingerprints
Erwin Quiring, Matthias Kirchner and Konrad Rieck

Attacking speaker recognition systems with phoneme morphing
Henry Turner, Giulio Lovisotto and Ivan Martinovic

Practical Bayesian Poisoning Attacks on Challenge-based Collaborative Intrusion Detection Networks
Weizhi Meng, Wenjuan Li, Lijun Jiang, Kim-Kwang Raymond Choo and Chunhua Su

A Framework for Evaluating Security in the Presence of Signal Injection Attacks
Ilias Giechaskiel, Youqian Zhang and Kasper Rasmussen

18:15 - 20:00 | Welcome Reception

The Welcome Reception of ESORICS 2019 will be held at the conference venue, Alvisse Parc Hotel. Drinks and light food will be served.

09:00 - 10:00 | Europa A

Keynote: Electronic Voting: A Journey to Verifiability and Vote Privacy
Dr. Véronique Cortier, CNRS Research Director at Loria, Nancy, France

10:00 - 10:30 | Coffee Break

10:30 - 12:10 | Room TBC

Secure Protocols

Formalizing and Proving Privacy Properties of Voting Protocols Using Alpha-Beta Privacy
Sébastien Gondron and Sebastian A. Mödersheim

ProCSA: Protecting Privacy in Crowdsourced Spectrum Allocation
Max Curran, Xiao Liang, Himanshu Gupta, Omkant Pandey and Samir Das

Breaking Unlinkability of the ICAO 9303 Standard for e-Passports Using Bisimilarity
Ross Horne, Sjouke Mauw, Zach Smith and Ihor Filimonov

Symmetric-key Corruption Detection: When XOR-MACs Meet Combinatorial Group Testing
Kazuhiko Minematsu and Norifumi Kamiya

10:30 - 12:10 | Room TBC

Useful Tools

Finding Flaws from Password Authentication Code in Android Apps
Siqi Ma, Elisa Bertino, Robert Deng, Juanru Li, Diet Ostry, Surya Nepal and Sanjay Jha

Identifying Privilege Separation Vulnerabilities in IoT Firmware with Symbolic Execution
Yao Yao, Wei Zhou, Yan Jia, Lipeng Zhu, Yuqing Zhang and Peng Liu

iCAT: An Interactive Customizable Anonymization Tool
Momen Oqaily, Yosr Jarraya, Lingyu Wang, Mengyuan Zhang, Makan Pourzandi and Mourad Debbabi

Monitoring the GDPR
Emma Arfelt, David Basin and Søren Debois

12:10 - 13:45 | Lunch

13:45 - 15:50 | Room TBC

Blockchain/Smart Contracts

Incentives for Harvesting Attack in Proof of Work mining pools
Yevhen Zolotavkin and Veronika Kuchta

A Lattice-Based Linkable Ring Signature Supporting Stealth Addresses
Zhen Liu, Khoa Nguyen, Guomin Yang, Huaxiong Wang and Duncan S. Wong

Annotary: A Concolic Execution System for Developing Secure Smart Contracts
Konrad Weiss and Julian Schuette

PDFS: Practical Data Feed Service for Smart Contracts
Juan Guarnizo and Pawel Szalachowski

Towards a Marketplace for Secure Outsourced Computations
Hung Dang, Dat Le Tien and Ee-Chien Chang

13:45 - 15:50 | Room TBC

Software Security

Automatically Identifying Security Checks for Detecting Kernel Semantic Bugs
Kangjie Lu, Aditya Pakki and Qiushi Wu

Uncovering Information Flow Policy Violations in C Programs
Darion Cassel, Yan Huang and Limin Jia

BinEye: Towards Efficient Binary Authorship Characterization Using Deep Learning
Saed Alrabaee, El Mouatez Karbab, Lingyu Wang and Mourad Debbabi

Static Detection of Uninitialized Stack Variables in Binary Code
Behrad Garmany, Martin Stoffel, Robert Gawlik and Thorsten Holz

Towards Automated Application-Specific Software Stacks
Nicolai Davidsson, Andre Pawlowski and Thorsten Holz

16:00 - 19:00 | Excursion: Visit to the Wine Cellars *Caves St Martin*

The transportation from the conference venue to the excursion and banquet is organized. The bus will leave at 16:00. For the return journey, one additional stop is scheduled at City Center.

19:00 - 23:30 | Conference Banquet and Cruise | Remich, Luxembourg

Photo: l'Office Régional du Tourisme Région Moselle

WEDNESDAY, 25 SEPTEMBER, 2019

09:00 - 10:00 | Keynote | Europe A

Cryptocurrencies and Distributed Consensus: Hype and Science
Prof. Dr. Bart Preneel, Katholieke Universiteit Leuven, Belgium

10:00 - 10:30 | Coffee Break

10:30 - 12:10 | Room TBC

Cryptographic Protocols

Identity-Based Encryption with Security against the KGC: A Formal Model and Its Instantiation from Lattices
Keita Emura, Shuichi Katsumata and Yohei Watanabe

Forward-Secure Puncturable Identity-Based Encryption for Securing Cloud Emails
Jianghong Wei, Xiaofeng Chen, Jianfeng Wang, Xuexian Hu and Jianfeng Ma

Feistel Structures for MPC, and More
Martin Albrecht, Loenzo Grassi, Leo Perrin, Sebastian Ramacher, Christian Rechberger, Dragos Rotaru, Arnab Roy and Markus Schofnegger

Arithmetic Garbling from Bilinear Maps
Nils Fleischhacker, Giulio Malavolta and Dominique Schroeder

10:30 - 12:10 | Room TBC

Security models

SEPD: An Access Control Model for Resource Sharing in an IoT Environment
Henrique G. G. Pereira and Philip W. L. Fong

Nighthawk: Transparent System Introspection from Ring -3
Lei Zhou, Jidong Xiao, Kevin Leach, Westley Weimer, Fengwei Zhang and Guojun Wang

Proactivizer: Transforming Existing Verification Tools into Efficient Solutions for Runtime Security Enforcement
Suryadipta Majumdar, Azadeh Tabiban, Meisam Mohammady, Alaa Oqaily, Yosr Jarraya, Makan Pourzandi, Lingyu Wang and Mourad Debbabi

Enhancing Security and Dependability of Industrial Networks with Opinion Dynamics
Juan E. Rubio, Mark Manulis, Cristina Alcaraz and Javier Lopez

12:10 - 13:45 | Lunch

13:45 - 15:25 | Room TBC

Searchable encryption

Dynamic Searchable Symmetric Encryption with Forward and Stronger Backward Privacy
Cong Zuo, Shi-Feng Sun, Joseph K. Liu, Jun Shao and Josef Pieprzyk

Towards Efficient Verifiable Forward Secure Searchable Symmetric Encryption
Zhongjun Zhang, Jianfeng Wang, Yunling Wang, Yaping Su and Xiaofeng Chen

Generic Multi-keyword Ranked Search on Encrypted Cloud Data
Shabnam Kasra Kermanshahi, Joseph Liu, Ron Steinfeld and Surya Nepal

An Efficiently Searchable Encrypted Data Structure for Range Queries
Florian Kerschbaum and Anselme Tueno

13:45 - 15:25 | Room TBC

Privacy

GDPiRated - Stealing Personal Information On- and Offline
Matteo Cagnazzo, Norbert Pohlmann and Thorsten Holz

Location Privacy-Preserving Mobile Crowd Sensing with Anonymous Reputation
Xun Yi, Kwok-Yan Lam, Elisa Bertino and Fang-Yu Rao

OCRAM-assisted Sensitive Data Protection on ARM-based Platform
Dawei Chu, Yuewu Wang, Lingguang Lei, Yanchu Li, Jiwu Jing and Kun Sun

Privacy-Preserving Collaborative Medical Time Series Analysis based on Dynamic Time Warping
Xiaoning Liu and Xun Yi

15:25 - 15:55 | Coffee Break

15:55 - 17:35 | Room TBC

Key exchange protocols

IoT-friendly AKE: Forward Secrecy and Session Resumption Meet Symmetric-key Cryptography
Gildas Avoine, Sébastien Canard and Loïc Ferreira

Strongly Secure Identity-Based Key Exchange with Single Pairing Operation
Junichi Tomida, Atsushi Fujioka, Akira Nagai and Koutarou Suzuki

A Complete and Optimized Key Mismatch Attack on NIST Candidate NewHope
Yue Qin, Chi Cheng and Jintai Ding

Breakdown Resilience of Key Exchange Protocols: NewHope, TLS 1.3, and Hybrids
Jacqueline Brendel, Marc Fischlin and Felix Günther

15:55 - 17:35 | Room TBC

Web Security

The Risks of WebGL: Analysis, Evaluation and Detection
Alex Belkin, Nethanel Gelernter and Israel Cidon

Mime Artist: Bypassing Whitelisting for the Web with JavaScript Mimicry Attacks
Stefanos Chaliasos, George Metaxopoulos, George Argyros and Dimitris Mitropoulos

Fingerprint Surface-based Detection of Web Bot Detectors
Hugo Jonker, Benjamin Krumnow and Gabry Vlot

Testing for Integrity Flaws in Web Sessions
Stefano Calzavara, Alvise Rabitti, Alessio Ragazzo and Michele Bugliesi