ESORICS 2020

Programme

The 25th European Symposium on Research in Computer Security
14-18 September 2020
Guildford, United Kingdom

Organised by

UNIVERSITY OF SURREY

Surrey Centre for Cyber Security SCCS

Sponsors

HUAWEI

IBM

Springer

COVID-19 update

The safety and well-being of all conference participants is our priority. After evaluating the COVID19 situation, the decision was made to run ESORICS 2020 and the associated workshops as an all-digital conference experience, and it is therefore now an online event. The conference and workshop dates remain the same: September 14 - 18, 2020.

Conference access information will be available via the conference website:
https://www.surrey.ac.uk/esorics-2020

Twitter
@ESORICS2020

Keynotes

First keynote

Monday, 14 September 2020, 9:10am - 10:10am (BST)
Speaker: Aggelos Kiayias, University of Edinburgh and IOHK, UK

Biography

Professor Aggelos Kiayias is Chair in Cyber Security and Privacy and Director of the Blockchain Technology Laboratory at the University of Edinburgh. He is also the chief scientist of blockchain technology IOHK. Previously he was the Head of the Cryptography and Security group at the Department of Informatics and Telecommunications, University of Athens where he was Associate Professor of Cryptography and Security and, before that, Professor in residence at the University of Connecticut, USA.

His research interests are in computer security, information security, applied cryptography and foundations of cryptography with particular emphasis in blockchain technology, e-voting systems and privacy-preserving protocols and identity management.

His distinctions include an ERC grant, a Marie Curie fellowship, an NSF Career Award, and a Fulbright Fellowship. He holds a Ph.D. from the City University of New York and he is a graduate of the Mathematics department of the University of Athens. He has over 100 publications in journals and conference proceedings.

Decentralising information and communications technology: Paradigm shift or cypherpunk reverie?

In the last decade, decentralisation emerged as a much anticipated development in the greater space of information and communications technology. Venerated by some and disparaged by others, blockchain technology became a familiar term, springing up in a wide array of expected and sometimes unexpected contexts. With the peak of the hype behind us, in this talk I look back, distilling what have we learned about the science and engineering of building secure and reliable systems, then I overview the present state of the art and finally I delve into the future, appraising this technology in its potential to impact the way we design and deploy information and communications technology services.

Second keynote

Tuesday, 15 September 2020, 2:05pm - 3:05pm (BST)
Speaker: Rebecca Wright, Barnard College, New York, NY USA

Biography

Dr Rebecca Wright is the Druckenmiller Professor of Computer Science and Director of the Vagelos Computational Science Center at Barnard College. Prior to joining Barnard, she was a professor in the Computer Science Department and Director of DIMACS at Rutgers, a professor in the Computer Science Department at Stevens Institute of Technology in Hoboken, New Jersey, and a researcher in the Secure Systems Research Department at AT&T Labs and AT&T Bell Labs.

Her research is primarily in the area of information security, including cryptography, privacy, foundations of computer security, and fault-tolerant distributed computing. Recent work includes accountability, differential privacy, privacy-preserving data mining, and secure multiparty approximations. Her ongoing research goals are the design of protocols, systems, and services that perform their specified computational or communication functions even if some of the participants or underlying components behave maliciously, and that balance individual needs such as privacy with collective needs such as network survivability and public safety.

Dr Wright serves as an editor of the International Journal of Information and Computer Security and the Transactions on Data Privacy. She is a member of the board of the Computing Research Association's Committee on Widening Participation in Computing Research (CRA-WP). She was a member of the board of directors of the International Association for Cryptologic Research from 2001 to 2005 and the steering committee of the Information Security Conference from 2006 to 2010, and an editor of the Journal of Computer Security from 2001 to 2011.

She was Program Chair of Financial Cryptography 2003 and the 2006 ACM Conference on Computer and Communications Security (CCS) and General Chair of Crypto 2002. She has served on numerous program committees, including Crypto, the ACM SIGKDD International Conference on Knowledge Discovery and Data Mining, and the Usenix Security Symposium. She received a PhD in Computer Science from Yale University in 1994 and a BA from Columbia University in 1988. She received an honorary M.E. from Stevens Institute of Technology in 2006. She is a Fellow of the IEEE and a Distinguished Member of the ACM.

Accountability in computing

Accountability is used often in describing computer-security mechanisms that complement preventive security, but it lacks a precise, agreed-upon definition. We argue for the need for accountability in computing in a variety of settings and categorize some of the many ways in which this term is used.

We identify a temporal spectrum onto which we may place different notions of accountability to facilitate their comparison, including prevention, detection, evidence, judgment, and punishment. We formalize our view in a utility-theoretic way and then use this to reason about accountability in computing systems. We also survey mechanisms providing various senses of accountability as well as other approaches to reasoning about accountability-related properties.

This is joint work with Joan Feigenbaum and Aaron Jaggard.

Third keynote

Wednesday, 16 September 2020, 9am – 10am (BST)
Speaker: Vadim Lyubashevsky, IBM Research - Zurich, Switzerland

Biography

Vadim received his PhD in 2008 from the University of California, San Diego, and after spending two years at Tel-Aviv University as a postdoc, in 2010 he became a researcher at Inria and ENS in Paris.

Since 2015, he has been a research scientist at IBM Research in Zurich. Vadim's main research area is designing practical schemes based on the hardness of lattice problems. His work on the Ring-SIS (2006) and Ring-LWE problems (2010), Ring-LWE encryption (2010), and digital signatures (2012) forms the foundation for a lot of the most efficient constructions in the ongoing NIST standardisation effort.

Lattices and zero-knowledge

Abstract: Building cryptography based on the presumed hardness of lattice problems over polynomial rings is one of the most promising approaches for achieving security against quantum attackers. One of the reasons for the popularity of lattice-based encryption and signatures in the ongoing NIST standardisation process is that they are significantly faster than all other post-quantum, and even many classical, schemes.

This talk will discuss the progress in constructions of more advanced lattice-based cryptographic primitives. In particular, I will describe recent work on zero-knowledge proofs which leads to the most efficient post-quantum constructions for certain statements.

Programme overview

Note: Talks are split into two tracks, track A (LNCS 12308) and track B (LNCS 12309).

Monday 14 September 2020		
Time	**Track A**	**Track B**
9am – 9:10am	Welcome plenary PC chairs: Liqun Chen and Ninghui Li	
9:10am – 10:10am	First keynote - Speaker: Aggelos Kiayias Chair: Steve Schneider	
10:10am – 10:20am	Break	
10:20am – 11:35am	**Database and web security** Chair: Nishanth Sastry	**Formal modelling** Chair: Cristina Alcaraz
11:35am – 12:50pm	**System security I** Chair: Sotiris Moschoyiannis	**Applied cryptography I** Chair: Guomin Yang
12:50pm – 1:50pm	Lunch break	
1:50pm – 3:30pm	**Network security I** Chair: Santanu Dash	**Analysing attacks** Chair: Kehuan Zhang
3:30pm – 3:50pm	Break	
3:50pm – 5:30pm	**Software security I** Chair: Brijesh Dongol	**System security II** Chair: Linzhi Jiang

Tuesday 15 September 2020		
Time	**Track A**	**Track B**
9am – 11:05am	**Software security II** Chair: Fengwei Zhang	**Post-quantum cryptography** Chair: Dung Duong
11:05am – 11:25am	Break	
11:25am – 1:05pm	**Machine learning security I** Chair: Leandros Maglaras	**Security analysis** Chair: David Gerault
1:05 pm– 2:05pm	Lunch break	
2:05pm – 3:05pm	Second keynote - Speaker: Rebecca Wright Chair: Ninghui Li	
3:05pm – 3:25pm	Break	
3:25pm – 5:05pm	**Machine learning security II** Chair: Frédéric Cuppens	**Applied cryptography II** Chair: Kaitai Liang

Wednesday 16 September 2020		
Time	**Track A**	**Track B**
9am – 10am	Third keynote - Speaker: Vadim Lyubashevsky Chair: Liqun Chen	
10am – 10:20am	**Best paper announcement and ESORICS awards** Chair: Sokratis Katsikas	
10:20am – 10:30am	Break	

10:30am – 11:45am	**Network security II** Chair: Miroslaw Kutylowski	**Blockchain I** Chair: Cătălin Drăgan
11:45am – 1pm	**Privacy** Chair: Jinguang Han	**Applied cryptography III** Chair: Mark Manulis
1pm – 2pm	Lunch break	
2pm – 3:15pm	**Password and policy** Chair: Shujun Li	**Blockchain II** Chair: Gregory Chockler
3:15pm – 3:25pm	Break	
3:25pm – 3:40pm	**Closing plenary** Chair: Steve Schneider	

Detailed programme

Day 1: Monday 14 September 2020

<u>Track A</u>

10:20am – 11:35am: **Database and web security**

- Pine: Enabling Privacy-Preserving Deep Packet Inspection on TLS with Rule-Hiding and Fast Connection Establishment
    - Jianting Ning, Xinyi Huang, Geong Sen Poh, Shengmin Xu, Jason Loh, Jian Weng and Robert H. Deng
- Bulwark: Holistic and Verified Security Monitoring of Web Protocols
    - Lorenzo Veronese, Stefano Calzavara and Luca Compagna
- A Practical Model for Collaborative Databases: Securely Mixing, Searching and Computing
    - Rachit Garg, Nishant Kumar, Shweta Agrawal and Manoj Prabhakaran

11:35am - 12:50pm: **System security part 1**

- Deduplication-friendly Watermarking for Multimedia Data in Public Clouds
    - Weijing You, Bo Chen, Limin Liu and Jiwu Jing
- DANTE: A Framework for Mining and Monitoring Darknet Traffic
    - Dvir Cohen, Yisroel Mirsky, Yuval Elovici, Rami Puzis, Manuel Kamp, Tobias Martin and Asaf Shabtai
- Efficient Quantification of Profile Matching Risk in Social Networks Using Belief Propagation
    - Anisa Halimi and Erman Ayday

1:50pm - 3:30pm: **Network security part 1**

- Anonymity Preserving Byzantine Vector Consensus
    - Christian Cachin, Daniel Collins, Tyler Crain and Vincent Gramoli
- CANSentry: Securing CAN-Based Cyber-Physical Systems against Denial and Spoofing Attacks

    - Abdulmalik Humayed, Fengjun Li, Jingqiang Lin and Bo Luo
- Distributed Detection of APTs: Consensus vs. Clustering
    - Juan E. Rubio, Cristina Alcaraz, Ruben Rios, Rodrigo Roman and Javier Lopez
- Designing Reverse Firewall for the Real World
    - Angele Bossuat, Xavier Bultel, Pierre-Alain Fouque, Cristina Onete and Thyla van der Merwe

3:50pm - 5:30pm: **Software security part 1**

- Follow the blue bird: A study on threat data published on Twitter
    - Fernando Alves, Ambrose Andongabo, Ilir Gashi, Pedro M. Ferreira and Alysson Bessani
- Dynamic and Secure Memory Transformation in Userspace
    - Robert Lyerly, Xiaoguang Wang and Binoy Ravindran
- Understanding the Security Risks of Docker Hub
    - Peiyu Liu, Shouling Ji, Lirong Fu, Kangjie Lu, Xuhong Zhang, Wei-Han Lee, Tao Lu, Wenzhi Chen and Raheem Beyah
- DE-auth of the blue! Transparent De-authentication using Bluetooth Low Energy Beacon
    - Pier Paolo Tricomi, Mauro Conti and Gene Tsudik

Track B

10:20am - 11:35am: **Formal modelling**

- Automatic generation of source lemmas in Tamarin: towards automatic proofs of security protocols
    - Veronique Cortier, Stephanie Delaune and Jannik Dreier
- When is a test not a proof?
    - Eleanor McMurtry, Olivier Pereira and Vanessa Teague
- Hardware Fingerprinting for the ARINC 429 Avionic Bus
    - Nimrod Gilboa Markevich and Avishai Wool

11:35am - 12:50pm: **Applied cryptography part 1**

- Semantic Definition of Anonymity in Identity-Based Encryption and Its Relation to Indistinguishability-based Definition
    - Goichiro Hanaoka, Misaki Komatsu, Kazuma Ohara, Yusuke Sakai and Shota Yamada
- SHECS-PIR: Somewhat Homomorphic Encryption-based Compact and Scalable Private Information Retrieval
    - Jeongeun Park and Mehdi Tibouchi
- Puncturable Encryption: A Generic Construction from Delegatable Fully Key-Homomorphic Encryption

    - Willy Susilo, Dung Hoang Duong, Huy Quoc Le and Josef Pieprzyk

1:50pm - 3:30pm: **Analysing attacks**

- Linear Attack on Round-Reduced DES Using Deep Learning
    - Botao Hou, Yongqiang Li, Haoyue Zhao and Bin Wu
- Detection by Attack: Detecting Adversarial Samples by Undercover Attack
    - Qifei Zhou, Rong Zhang, Bo Wu, Weiping Li and Tong Mo
- Big Enough to Care Not Enough to Scare! Crawling to Attack Recommender Systems
    - Mirko Polato, Fabio Aiolli, Mauro Conti and Stjepan Picek
- Active Re-identification Attacks on Periodically Released Dynamic Social Graphs
    - Xihui Chen, Ema Kepuska, Sjouke Mauw and Yunior Ramirez-Cruz

3:50pm - 5:30pm: **System security part 2**

- Fooling primality tests on smartcards
    - Vladimir Sedlacek, Jan Jancar and Petr Svenda
- An Optimizing Protocol Transformation for Constructor Finite Variant Theories in Maude-NPA
    - Damian Aparicio, Santiago Escobar, Raúl Gutiérrez and Julia Sapiña
- On the Privacy Risks of Compromised Trigger-Action Platforms
    - Yu-Hsi Chiang, Hsu-Chun Hsiao, Chia-Mu Yu and Tiffany Hyun-Jin Kim
- Plenty of Phish in the Sea: Analyzing Potential Pre-Attack Surfaces
    - Tobias Urban, Matteo Große-Kampmann, Dennis Tatang, Thorsten Holz and Norbert Pohlmann

---

Day 2: Tuesday 15 September 2020

Track A

9am - 11:05am: **Software security part 2**

- Similarity of Binaries across Optimization Levels and Obfuscations
    - Jianguo Jiang, Gengwang Li, Min Yu, Gang Li, Chao Liu, Zhiqiang Lv, Bin Lv and Weiqing Huang
- HART: Hardware-assisted Kernel Module Tracing on Arm
    - Yunlan Du, Zhenyu Ning, Jun Xu, Zhilong Wang, Yueh-Hsun Lin, Fengwei Zhang, Xinyu Xing and Bing Mao
- Zipper Stack: Shadow Stacks Without Shadow

    - Jinfeng Li, Liwei Chen, Qizhen Xu, Gang Shi, Kai Chen and Dan Meng
- Restructured Cloning Vulnerability Detection Based on Function Semantic Reserving and Reiteration Screening
    - Weipeng Jiang, Bin Wu, Xingxin Yu, Rui Xue and Zhengmin Yu
- LegIoT: Ledgered Trust Management Platform for IoT
    - Jens Neureither, Alexandra Dmitrienko, David Koisser, Ferdinand Brasser and Ahmad-Reza Sadeghi

11:25am - 1:05pm: **Machine learning security part 1**

- PrivColl: Practical Privacy-Preserving Collaborative Machine Learning
    - Yanjun Zhang, Guangdong Bai, Xue Li, Caitlin Curtis, Chen and Ryan Ko
- An Efficient 3-Party Framework for Privacy-Preserving Neural Network Inference
    - Liyan Shen, Chen Xiaojun, Jinqiao Shi, Ye Dong and Binxing Fang
- Deep Learning Side-Channel Analysis on Large-Scale Traces–A Case Study on a Polymorphic AES
    - Loïc Masure, Nicolas Belleville, Eleonora Cagli, Marie-Angela Cornelie, Damien Couroussé, Cécile Dumas and Laurent Maingault
- Towards Poisoning the Neural Collaborative Filtering-Based Recommender Systems
    - Yihe Zhang, Jiadong Lou, Li Chen, Xu Yuan, Jin Li, Tom Johnsten and Nianfeng Tzeng

3:25pm - 5:05pm: **Machine learning security part 2**

- Data Poisoning Attacks Against Federated Learning Systems
    - Vale Tolpegin, Stacey Truex, M. Emre Gursoy and Ling Liu
- Interpretable Probabilistic Password Strength Meters via Deep Learning
    - Dario Pasquini, Giuseppe Ateniese and Massimo Bernaschi
- Polisma–A Framework for Learning Attribute-based Access Control Policies
    - Amani Jabal, Elisa Bertino, Jorge Lobo, Mark Law, Alessandra Russo, Seraphin Calo and Dinesh Verma
- A Framework for Evaluating Client Privacy Leakages in Federated Learning
    - Wenqi Wei, Ling Liu, Margaret Loper, Ka-Ho Chow, Mehmet Emre Gursoy, Stacey Truex and Yanzhao Wu

Track B

9am - 11:05am: Post-quantum cryptography

- Towards Post-Quantum Security for Cyber-Physical Systems: Integrating PQC into Industrial M2M Communication
  - Sebastian Paul and Patrik Scheible
- CSH: A Post-quantum Secret Handshake Scheme from Coding Theory
  - Zhuoran Zhang, Fangguo Zhang and Haibo Tian
- A Verifiable and Practical Lattice-Based Decryption Mix Net with External Auditing
  - Xavier Boyen, Thomas Haines and Johannes Mueller
- A Lattice-Based Key-Insulated and Privacy-Preserving Signature Scheme with Publicly Derived Public Key
  - Wenling Liu, Zhen Liu, Khoa Nguyen, Guomin Yang and Yu
- Post-Quantum Adaptor Signatures and Payment Channel Networks
  - Muhammed F. Esgin, Oguzhan Ersoy and Zekeriya Erkin

11:25am - 1:05pm: **Security analysis**

- Linear-Complexity Private Function Evaluation is Practical
  - Marco Holz, Ágnes Kiss, Deevashwer Rathee and Thomas Schneider
- Certifying Decision Trees Against Evasion Attacks by Program Analysis
  - Stefano Calzavara, Pietro Ferrara and Claudio Lucchese
- They Might NOT Be Giants: Crafting Black-Box Adversarial Examples Using Particle Swarm Optimization
  - Rayan Mosli, Yin Pan, Bo Yuan and Matthew Wright
- Understanding Object Detection Through An Adversarial Lens
  - Ka-Ho Chow, Ling Liu, Mehmet Emre Gursoy, Stacey Truex, Wenqi Wei and Yanzhao Wu

3:25pm - 5:05pm: **Applied cryptography part 2**

- Signatures with Tight Multi-User Security from Search Assumptions
  - Jiaxin Pan and Magnus Ringerud
- Biased RSA private keys: Origin attribution of GCD-factorable keys
  - Adam Janovsky, Matus Nemec, Petr Svenda, Peter Sekan and Vashek Matyas
- MAC-in-the-Box: Verifying a Minimalistic Hardware Design for MAC Computation
  - Robert Künnemann and Hamed Nemati
- Evaluating the effectiveness of heuristic worst-case noise analysis in FHE
  - Anamaria Costache, Kim Laine and Rachel Player

Day 3: Wednesday 16 September 2020

Track A

10:30am - 11:45am: **Network security part 2**

- An Accountable Access Control Scheme for Hierarchical Content in Named Data Networks with Revocation
  - Nazatul Haque Sultan, Vijay Varadharajan, Seyit Camtepe and Surya Nepal
- PGC: Decentralized Confidential Payment System with Auditability
  - Yu Chen, Xuecheng Ma, Cong Tang and Man Ho Au
- Secure Cloud Auditing with Efficient Ownership Transfer
  - Jun Shen, Fuchun Guo, Xiaofeng Chen and Willy Susilo

11:45am - 1pm: **Privacy**

- Encrypt-to-self: Securely Outsourcing Storage
  - Jeroen Pijnenburg and Bertram Poettering
- PGLP: Customizable and Rigorous Location Privacy through Policy Graph
  - Yang Cao, Yonghui Xiao, Shun Takagi, Li Xiong, Masatoshi Yoshikawa, Yilin Shen, Jinfei Liu, Hongxia Jin and Xiaofeng Xu
- Where are you Bob? Privacy-Preserving Proximity Testing with a Napping Party
  - Ivan Oleynikov, Elena Pagnin and Andrei Sabelfeld

2pm - 3:15pm: **Password and policy**

- Distributed PCFG Password Cracking
  - Radek Hranicky, Lukas Zobal, Ondrej Rysavy, Dusan Kolar and David Mikus
- Your PIN Sounds Good! Augmentation of PIN Guessing Strategies Through Audio Leakage
  - Matteo Cardaioli, Mauro Conti, Kiran Balagani and Paolo Gasti
- GDPR -- Challenges for Reconciling Legal Rules with Technical Reality
  - Miroslaw Kutylowski, Anna Lauks-Dutka and Moti Yung

Track B

10:30am - 11:45am: **Blockchain part 1**

- How to Model the Bribery Attack: A Practical Quantification Method in Blockchain
  - Hanyi Sun, Na Ruan and Chunhua Su
- Updatable Blockchains

    - Michele Ciampi, Nikos Karayannidis, Aggelos Kiayias and Dionysis Zindros
- PrivacyGuard: Enforcing Private Data Usage Control with Blockchain and Off-chain Contract Execution
    - Yang Xiao, Ning Zhang, Jin Li, Wenjing Lou and Y. Thomas Hou

11:45am - 1pm: **Applied cryptography part 3**

- Identity-Based Authenticated Encryption with Identity Confidentiality
    - Yunlei Zhao
- Securing DNSSEC Keys via Threshold ECDSA From Generic MPC
    - Anders Dalskov, Marcel Keller, Claudio Orlandi, Kris Shrishak and Haya Shulman
- On Private Information Retrieval Supporting Range Queries
    - Junichiro Hayata, Jacob Schuldt, Goichiro Hanaoka and Kanta Matsuura

2pm - 3:15pm: **Blockchain part 2**

- 2-hop Blockchain: Combining Proof-of-Work and Proof-of-Stake Securely
    - Tuyet Duong, Lei Fan, Jonathan Katz, Phuc Thai and Hong-Sheng Zhou
- Generic Superlight Client for Permissionless Blockchains
    - Yuan Lu, Qiang Tang and Guiling Wang
- LNBot: A Covert Hybrid Botnet on Bitcoin Lightning Network for Fun and Profit
    - Ahmet Kurt, Enes Erdin, Mumin Cebe, Kemal Akkaya and Selcuk Uluagac