ESORICS

ESORICS 2020 Workshops

# Workshops Program (online event)

17-18 September 2020
Guildford, United Kingdom

Edited by ESORICS 2020 Workshop Chair

Mark Manulis
Surrey Centre for Cyber Security
University of Surrey

Organized by

Sponsors

Last updated 08 September 2020

Disclaimer

This program book aggregates contents received from the organisers of workshops affiliated with ESORICS 2020, as listed on the conference website: https://www.surrey.ac.uk/esorics-2020/workshops

Each workshop's program includes links to 1-min Youtube videos where speakers introduce their papers; for some papers links might be missing. Presentations of workshop papers will be given live according to the schedule published in this book. **Time zones: United Kingdom (BST)**. Each workshop will have a dedicated Zoom Webinar link. Some workshops have shared sessions as indicated on the overall schedule. A shared session will be accessible from the webinar of one of the workshops; which workshop will be streaming a shared session is visible from their programs.

Links to Zoom Webinars for all workshops will be made available to registered ESORICS 2020 participants via Slack and are therefore not included into this programme book.

## Overview All Workshops – Thursday, 17th September 2020

| Time (UK) | STM | CBT | DPM | STAST | SECPRE | CyberICPS | DeSECSys | MSTEC |
|---|---|---|---|---|---|---|---|---|
| 09:00 - 09:15 | Welcome | Welcome | | Welcome | Welcome | | | Welcome |
| 09:15 - 09:30 | Session 1 | Keynote 1 | | Session 1 | Keynote | | | Session 1 |
| 09:30 - 09:45 | | | | | | | | |
| 09:45 - 10:00 | | | | | | | | |
| 10:00 - 10:15 | | | | | | | Welcome | |
| 10:15 - 10:30 | | Break | | Break | | | Keynote 1 | Session 2 |
| 10:30 - 10:45 | | Session 1 | Session 1 | Keynote | Session 1 | | | |
| 10:45 - 11:00 | Keynote 1 | | | | | | | |
| 11:00 - 11:15 | | | | | | | Session 1 | |
| 11:15 - 11:30 | | | | Break | | | | Session 3 |
| 11:30 - 11:45 | Session 2 | | | Session 2 | | | | |
| 11:45 - 12:00 | | | | | | | | |
| 12:00 - 12:15 | | | | | | | | |
| 12:15 - 12:30 | | | | | | | | Panel |
| 12:30 - 13:30 | Break | | | | | | | |
| 13:30 - 13:45 | | Session 2 | Session 2 | Session 3 | Session 2 | | Keynote 2 | Session 4 |
| 13:45 - 14:00 | | | | | | | | |
| 14:00 - 14:15 | | | | | | | | |
| 14:15 - 14:30 | | | | Break | | | Keynote 3 | |
| 14:30 - 14:45 | | | | Session 4 | Session 3 | | | Session 5 |
| 14:45 - 15:00 | | | | | | | | |
| 15:00 - 15:15 | | Break | | | | | Keynote 4 | |
| 15:15 - 15:30 | | | | | | | | |
| 15:30 - 15:45 | | Session 3 | Session 3 | | | | | Panel |
| 15:45 - 16:00 | | | | Break | | | Break | |
| 16:00 - 16:15 | | | | Session 5 | | | Session 2 | |
| 16:15 - 16:30 | | | | | | | | |
| 16:30 - 16:45 | | | | | | | | |
| 16:45 - 17:00 | | | | Closing | | | Closing | |

# Overview All Workshops – Friday, 18th September 2020

| Time (UK) | STM | CBT | DPM | ETAA | SPOSE | ADIoT | DETIPS | MPS | CPS4CIP |
|---|---|---|---|---|---|---|---|---|---|
| 09:00 - 09:15 | | Keynote 2 | | Session 1 | Welcome | Welcome | Welcome | | Welcome |
| 09:15 - 09:30 | Keynote 2 | | | | Keynote | Session 1 | Session 1 | | Keynote 1 |
| 09:30 - 09:45 | | | | | | | | | |
| 09:45 - 10:00 | | | | | Session 1 | | | | Session 1 |
| 10:00 - 10:15 | Session 3 | | | | | | | | |
| 10:15 - 10:30 | | Break | | | | | | | |
| 10:30 - 10:45 | | Session 4 | | Break | | | | | |
| 10:45 - 11:00 | | | | | Break | | Break | | Break |
| 11:00 - 11:15 | | | | Session 2 | Session 2 | | Session 2 | | Session 2 |
| 11:15 - 11:30 | | | | | | | | | |
| 11:30 - 11:45 | Closing | | | | | | | | |
| 11:45 - 12:00 | | | | | | | | | Break |
| 12:00 - 12:15 | | | | | | | | | Session 3 |
| 12:15 - 12:30 | | | | | | | | | |
| 12:30 - 13:30 | Break | | | | | | | | |
| 13:30 - 13:45 | | Panel | | Break | | | | Welcome | Keynote 2 |
| 13:45 - 14:00 | | | | | | | | Keynote 1 | |
| 14:00 - 14:15 | | | | Session 3 | | | | | Sesssion 4 |
| 14:15 - 14:30 | | | | | | | | | |
| 14:30 - 14:45 | | | | | | | | Keynote 2 | |
| 14:45 - 15:00 | | | | | | | | | Break |
| 15:00 - 15:15 | | Farewell | | | | | | Break | Session 5 |
| 15:15 - 15:30 | | | | | | | | | |
| 15:30 - 15:45 | | | | | | | | Session 1 | Closing & Planning |
| 15:45 - 16:00 | | | | | | | | | |
| 16:00 - 16:15 | | | | | | | | | |
| 16:15 - 16:30 | | | | | | | | | |
| 16:30 - 16:45 | | | | | | | | | |
| 16:45 - 17:00 | | | | | | | | | |

# CBT: 4th International Workshop on Cryptocurrencies and Blockchain Technology

Workshop website: https://deic-web.uab.cat/cbt/cbt2020/

**Thursday, 17th September 2020**

09:00 – 10:15
WELCOME & KEYNOTE 1 (joint with DPM, use Webinar of CBT)
Workshop chairs (Jordi Herrera-Joancomartí & Joaquin Garcia-Alfaro)
**Title:** Design tradeoffs for Bitcoin Watchtowers
**Speaker:** *Sergi Delgado*, @Talaia Labs

10:15 – 10:30
BREAK

10:30 – 12:40
SESSION 1: Transactions, Mining & Second Layer

- 10:30-11:00 TxChain: Efficient Cryptocurrency Light Clients via Contingent Transaction Aggregation
  Abstract video link: https://youtu.be/CR34go3jN8U
  *Alexei Zamyatin, Zeta Avarikioti, Daniel Perez and William J. Knottenbelt*

- 11:00-11:30 VRF-Based Mining: Simple Non-Outsourceable Cryptocurrency Mining
  Abstract video link: https://youtu.be/CKWRvCs8xsQ
  *Runchao Han, Haoyu Lin and Jiangshan Yu*

- 11:30-12:00 On the selection of the LN client implementation parameters
  Abstract video link: https://youtu.be/5vu2oYxWqdw
  *Luis Esteban Oleas Chavez, Jordi Herrera and Cristina Pérez-Solà*

- 12:00-12:20 Fundamental Properties of the Layer Below a Payment Channel Network
  (Short Paper) Abstract video link: https://youtu.be/y-QF-LoeczE
  *Matthias Grundmann and Hannes Hartenstein*

- 12:20-12:40 ZeroJoin: Combining ZeroCoin and CoinJoin
  (Short Paper) Abstract video link: https://youtu.be/FxhIMVmgrig
  *Alexander Chepurnoy and Amitabh Saxena*

12:40 – 13:30
BREAK

13:30 – 15:00
SESSION 2: Signature Schemes & Formal Methods

- 13:30-14:00 Triptych: logarithmic-sized linkable ring signatures with applications
  Abstract video link: https://youtu.be/qGKUk35jbVU
  *Sarang Noether and Brandon Goodell*

- 14:00-14:30 Moderated Redactable Blockchains: A Definitional Framework with an Efficient Construct
  Abstract video link: https://youtu.be/yF5wfxHSZJM
  *Mohammad Sadeq Dousti and Alptekin Küpçü*

- 14:30-15:00 Radium: Improving Dynamic PoW Targeting
  Abstract video link: https://youtu.be/ZlILrfQcvhY
  *George Bissias*

15:00 – 15:30
BREAK

15:30 – 17:30
SESSION 3: Privacy, SNARKs & Anonymity

- 15:30-16:00 Proof of No-Work: How to Incentivize Individuals to Stay at Home
  Abstract video link: https://youtu.be/XapibI-la-4
  *Michael Bartholic, Jianan Su, Ryosuke Ushida, Yusuke Ikeno, Zhengrong Gu and Shinichiro Matsuo*

- 16:00-16:30 Privacy Preserving Netting Protocol for Inter-bank Payments
  Abstract video link: https://youtu.be/4O_TPhRUQ8c
  *Hisham Galal and Amr Youssef*

- 16:30-16:50 Who let the DOGS out: a Group Signature scheme with Distributed Opening for Auditable but Anonymous communications
  (Short Paper) Abstract video link: https://youtu.be/7lTWAZizs5Y
  *Marina Dehez-Clementi, Jean-Christophe Deneuville, Jérôme Lacan, Hassan Asghar and Dali Kaafar*

- 16:50-17:10 Tracking Mixed Bitcoins
  (Short Paper) Abstract video link: https://youtu.be/qOBYS2rKYwY
  *Tin Tironsakkul, Manuel Maarek, Andrea Eross and Mike Just*

**Friday, 18th September 2020**

09:00 – 10:00
KEYNOTE 2 (joint with DPM, use Webinar of DPM)
**Title:** Is Website Fingerprinting Actually Practical?
**Speaker:** *Marc Juarez* (University of Southern California).

10:00 – 10:30
BREAK

10:30 – 12:30
SESSION 4: AI, Engineering & Authentication (joint with DPM, use Webinar of DPM)

- 10:30-11:00 Extracting speech from motion-sensitive sensors
  Abstract video link: https://youtu.be/WLPiONkwL38
  *Safaa Azzakhnini and Ralf C. Staudemeyer*

- 11:00-11:30 A Lightweight Approach for the Elicitation of Privacy and Data Protection Requirements
  Abstract video link: https://youtu.be/HdqqBa-VqWo
  *Nicolás E. Díaz Ferreyra, Patrick Tessier, Gabriel Pedroza and Maritta Heisel*

- 11:30-12:00 Towards Multiple Pattern type Privacy Protection in Complex Event Processing
  Abstract video link: https://youtu.be/XopvpbdoYYg
  *Saravana Murthy Palanisamy*

- 12:00-12:30 GPS-based Behavioral Authentication Utilizing Distance Coherence
  Abstract video link: https://youtu.be/SgMHRv5Jx-Q
  *Tran Phuong Thao and Rie Shigetomi Yamaguchi*

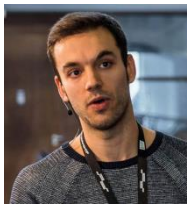
12:30 – 13:30
BREAK

13:30 – 15:00
PANEL (joint with DPM, use Webinar of DPM)

- **Title:** How cryptocurrency and blockchain technology will become a trust foundation for the New Normal while ensuring data privacy management?
  **Panel Moderator**: Shin'ichiro Matsuo (Georgetown University)
  **Panelists**: *Pindar Wong (VeriFi limited)*
  *Nat Sakimura (OpenID foundation)*
  *Julien Bringer (Convenor of ISO TC307/WG2)*
  *Florian Kammueller (Middlesex University London)*
  *Patrick McCorry (PISA Research)*

15:00 – 15:10
CLOSING (joint with DPM, use Webinar of DPM)

**KEYNOTE 1 TALK (check DPM program for KEYNOTE 2 TALK)**



Sergi Delgado is the CEO of Talaia Labs. He got his PhD in CS from the Autonomous University of Barcelona (UAB) focusing on Bitcoin and Distributed Systems. In the past he has worked in the blockchain laboratories at both UCL and UIUC. He co-founded and led the Bitcoin development at PISAResearch. His recent research has focused on measuring (and inferring) the Bitcoin peer-to-peer network which was presented at Financial Cryptography (18 & 19) and Scaling Bitcoin (18 & 19). He is currently building a watchtower protocol for Bitcoin.

**Title**: Design tradeoffs for Bitcoin Watchtowers

**Abstract:** Bitcoin layer 2 protocols, such as the Lightning Network, introduce some additional assumptions to the security model of the system. One of the most important ones is the always-online assumptions, meaning that the nodes of the network require to remain always online (or at least reconnect periodically) in order to prevent potential loss of funds. Watchtowers were introduced to reduce that assumption, acting as non-trusted, non-custodial third party relayers. While this is generally the case, some protocols may do with less strict requirements. In this talk we will cover the different tradeoffs in watchtower design, ranging from storage requirements to privacy concerns.