

About ESORICS

Computer security is concerned with the protection of information in environments where there is a possibility of intrusion or malicious action. The aim of ESORICS is to further the progress of research in computer security by establishing a European forum for bringing together researchers in this area, by promoting the exchange of ideas with system developers and by encouraging links with researchers in related areas.

Progressively organised in a series of European countries, the symposium is confirmed as the European research event in computer security. Since its inception in 1990, ESORICS has been hosted in a series of European countries and has established itself as the premiere European research event in computer security

ESORICS / This Year

This year the Symposium will be held in Copenhagen, Denmark on 26-30 September 2022 (26-28 Main Conference, 29-30 Workshops)

CPH Conference Center.
Tietgensgade 65,
1704 Copenhagen, Denmark.

Phone: +45 33 29 80 60
Email: esorics2022@easychair.org
Web: <https://esorics2022.compute.dtu.dk>

ESORICS

Program Booklet



ESORICS 2022

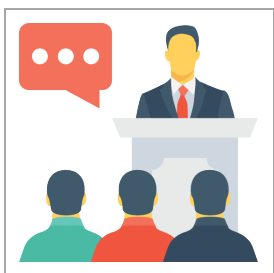
Copenhagen, Denmark (26, Sep. – 30, Sep.)

ESORICS 2022

ESORICS 2022
CPH Conference Center.
Tietgensgade 65,
1704 Copenhagen, Denmark.

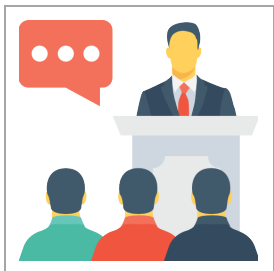
Conference Program

26th Sep. 2022



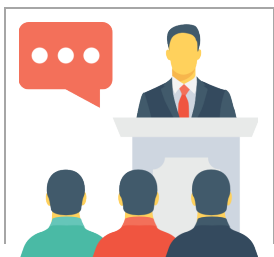
Keynote from Paulo Verissimo
Blockchain Security I / II Privacy I / II
Crypto I / II / III Attacks I / II
Digital Signatures I / II Posters
Side Channels
Anonymity
Access Control
Welcome Reception

27th Sep. 2022



Keynote from Ahmad Reza Sadeghi
Cyber-Physical System Security I
Cloud Security I / II Authentication I / II
Formal Analysis ML Technique I / II
Attacks III
Keynote from Giuseppe Ateniese
Social Event
Conference Banquet

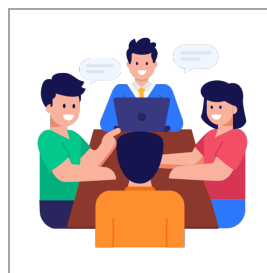
28th Sep. 2022



IoT Security I / II
Applications I / II
Network and SW Security I / II
Hardware Security
Web Security I / II
Cyber-Physical System Security II
Multiparty Computation

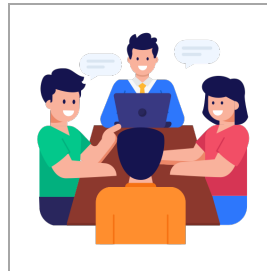
Workshop Session

29th Sep. 2022



STAST
CBT
CyberICPS
SECPRE
DPM
STM

30th Sep. 2022



ETAA
ADIoT
SP-MIoT
CPS4CIP
SPOSE
CDT & SECOMANE
SecAssure
EIS

Program – 26th Sep.

08:00 – 08:45	Registration
08:45 – 09:00	📍 Sankt Hans Torv & Nørrebros Runddel Welcome Ceremony
09:00 – 10:00	📍 Sankt Hans Torv & Nørrebros Runddel Cyber Resilience: an agenda for the future of cyberspace security.
10:00 – 10:20	☕ Coffee Break
	📍 Sankt Hans Torv & Nørrebros Runddel Session: Blockchain Security I
10:20 – 11:20	A Blockchain-based Long-term Time-Stamping Scheme
	Post-Quantum Verifiable Random Function from Symmetric Primitives in PoS Blockchain
	Opportunistic Algorithmic Double-Spending: How I learned to stop worrying and love the Fork
	📍 Hovedbanegården Session: Privacy I
10:20 – 11:20	Privacy Leakage in Privacy-Preserving Neural Network Inference
	Enhancing User Privacy in Mobile Devices Through Prediction of Privacy Preferences
	One vote is enough for analysing privacy
	📍 Kødbyen & Enghave Plads Session: Crypto I
10:20 – 11:20	Generic Construction of Trace-and-Revoke Inner Product Functional Encryption
	Spatial Encryption Revisited: From Delegatable Multiple Inner Product Encryption and More
	Public Key Authenticated Encryption with Keyword Search from LWE

Program – 26th Sep.

	📍 Sankt Hans Torv & Nørrebros Runddel Session: Blockchain Security II
11:20 – 12:20	Zero-History Confidential Chains with Zero-Knowledge Contracts: A New Normal for Decentralized Ledgers?
	Secure Hierarchical Deterministic Wallet Supporting Stealth Address
	Zero-Knowledge Age Restriction for GNU Taler
	📍 Hovedbanegården Session: Privacy II
11:20 – 12:20	Local Differential Privacy for Federated Learning in Industrial Settings
	XSPIR: Efficient Symmetrically Private Information Retrieval from Ring-LWE
	Scaling Up GAEN Pseudorandom Processes: Preparing for a More Extensive Pandemic
	📍 Kødbyen & Enghave Plads Session: Crypto II
11:20 – 12:20	An Efficient Query Recovery Attack Against a Graph Encryption Scheme
	New Unbounded Verifiable Data Streaming for Batch Query with Almost Optimal Overhead
	A Formal Model for Credential Hopping Attacks
12:20 – 14:00	🍴 Luncheon

Program – 26th Sep.

📍 Sankt Hans Torv & Nørrebro Runddel Session: Crypto III	
14:00 – 15:20	No-directional and Backward-leak Uni-directional Updatable Encryption are Equivalent
	Efficient Circuits for Permuting and Mapping Packed Values Across Levelled Homomorphic Ciphertexts
	Towards Practical Homomorphic Time-Lock Puzzles: Usability and Verifiability
	Light the Signal: Optimization of Signal Leakage Attacks against LWE-Based Key Exchange
📍 Hovedbanegården Session: Digital Signatures I	
14:00 – 15:20	Half-Aggregation of Schnorr Signatures with Tight Reductions
	Ring Signatures with User-Controlled Linkability
	DualDory: Logarithmic-verifier linkable ring signatures through preprocessing
	Efficient Unique Ring Signatures From Lattices
15:20 – 15:40	☕ Coffee Break
📍 Sankt Hans Torv & Nørrebro Runddel Session: Attacks I	
15:40 – 16:40	Kallima: A Clean-label Framework for Textual Backdoor Attacks
	Two Types of Novel DoS Attacks against CDNs Based on HTTP/2 Flow Control Mechanism
	EVEExchange: A Relay Attack on Electric Vehicle Charging System

Program – 26th Sep.

📍 Hovedbanegården Session: Digital Signatures II	
15:40 – 16:40	Verifiable Timed Linkable Ring Signatures For Scalable Payments for Monero
	Deterministic Wallets for Adaptor Signatures
	Puncturable Signature: A Generic Construction and Instantiations
📍 Kødbyen & Enghave Plads Session: Side Channels	
15:40 – 16:40	We can hear your PIN drop: A new acoustic side channel attack to profile PIN pads keys
	Explore More, Reveal More - VAL: Volume and Access Pattern Leakage-abuse Attack with Leaked Documents
	BLEWhisperer: Exploiting BLE Advertisements for Data Exfiltration
📍 Sankt Hans Torv & Nørrebro Runddel Session: Attacks II	
16:40 – 17:40	Smart RPKI Validation: Avoiding Errors and Preventing Hijacks
	Cyber Network Resilience against Self-Propagating Malware Attacks
	INC: In-Network Classification of Botnet Propagation at Line Rate

Program – 26th Sep.

📍 Hovedbanegården Session: Anonymity	
16:40 – 17:40	A Machine Learning Approach to Detect Differential Treatment of Anonymous Users
	Utility Preserving Biometric Information Anonymization
	Anonymous Traceback for End to End Encryption
📍 Kødbyen & Enghave Plads Session: Access Control	
16:40 – 17:40	Administration of Machine Learning Based Access Control
	Real-time Policy Enforcement with Metric First-Order Temporal Logic
	A Tale of Four Gates Privilege Escalation and Permission Bypasses on Android through App Components
18:00 ~	Welcome Reception

Program – 26th Sep.

Poster Session	
18:00 ~	Is your password sexist? A gamification-based analysis of the cultural context of leaked passwords.
	A Fast, Practical and Simple Shortest Path Protocol for Multiparty Computation
	Audio Spoofing Detection Using Constant-Q Spectral Sketches and Parallel-Attention SE-ResNet
	MixCT: Mixing Confidential Transactions from Homomorphic Commitment
	Multi-Freq-LDPy: Multiple Frequency Estimation Under Local Differential Privacy in Python
	The Devil is in the GAN: Backdoor Attacks and Defenses in Deep Generative Models

Program – 27th Sep.

08:00 – 09:00	Registration
09:00 – 10:00	<p>📍 Sankt Hans Torv & Nørrebros Runddel</p> <p>Lessons Learned from Building and Attacking Secure Computing Systems</p>
10:00 – 10:20	☕ Coffee Break
10:20 – 11:20	<p>📍 Sankt Hans Torv & Nørrebros Runddel</p> <p>Session: Attacks III</p>
	GAME: Generative-Based Adaptive Model Extraction Attack
	AttacKG: Constructing Technique Knowledge Graph from Cyber Threat Intelligence Reports
10:20 – 11:20	<p>📍 Hovedbanegården</p> <p>Session: Cloud Security I</p>
	Public Cloud Data Auditing Revisited: Removing the Tradeoff Between Proof Size and Storage Cost
	DEKS: a Secure Cloud-based Searchable Service can Make Attackers Pay
10:20 – 11:20	<p>📍 Hovedbanegården</p> <p>Session: Cloud Security I</p>
	MVOC: A Lighter Multi-Client Verifiable Outsourced Computation with Hybrid Homomorphic Encryption
10:20 – 11:20	<p>📍 Kødbyen & Enghave Plads</p> <p>Session: Authentication I</p>
	Cryptographic Software-Update Authentication
	On Committing Authenticated Encryption
10:20 – 11:20	Quantum-Resistant Password-Based Threshold Single-Sign-On Authentication with Updatable Server Private Key

Program – 27th Sep.

11:20 – 12:20	<p>📍 Sankt Hans Torv & Nørrebros Runddel</p> <p>Session: ML Techniques I</p>
	Hide and Seek: on the Stealthiness of Attacks against Deep Learning Systems
	Precise Extraction of Deep Learning Models via Side-Channel Attacks on Edge/Endpoint Devices
11:20 – 12:20	Real-time Adversarial Perturbations against Deep Reinforcement Learning Policies: Attacks and Defenses
11:20 – 12:20	<p>📍 Hovedbanegården</p> <p>Session: Cloud Security II</p>
	Verifying the Quality of Outsourced Training on Clouds
	SecQuant: Quantifying Container System Call Exposure
11:20 – 12:20	Robust and Scalable Process Isolation against Spectre in the Cloud
11:20 – 12:20	<p>📍 Kødbyen & Enghave Plads</p> <p>Session: Authentication II</p>
	The Revenge of Password Crackers: Automated Training of Password Cracking Tools
	Fuzzy Authenticated Key Exchange with Tight Security
11:20 – 12:20	Continuous Authentication in Secure Messaging
12:20 – 14:00	🍴 Luncheon






Program – 27th Sep.

	📍 Sankt Hans Torv & Nørrebros Runddel Session: ML Techniques II
14:00 – 15:20	FLMJR: Improving Robustness of Federated Learning via Model Stability
	MaleficNet: Hiding Malware into Deep Neural Networks using Spread-Spectrum Channel Coding
	Long-Short History of Gradients is All You Need: Detecting Malicious and Unreliable Clients in Federated Learning
	MLFM: Machine Learning Meets Formal Method for Efficient Security Verification in Network Functions Virtualization (NFV)
	📍 Hovedbanegården Session: Formal Analysis
14:00 – 15:20	A Formal Analysis of the FIDO2 Protocols
	Composable Security Treatment of ECVRF and Batch Verifications
	Efficient Proofs of Knowledge for Threshold Relations
	A tale of two models: formal verification of KEMTLS via Tamarin
	📍 Kødbyen & Enghave Plads Session: Cyber-Physical System Security I
14:00 – 15:20	Perspectives from a Comprehensive Evaluation of Reconstruction-based Anomaly Detection in Industrial Control Systems
	A Novel High-performance Implementation of CRYSTALS-Kyber with AI Accelerator
	From Click To Sink: utilizing AIS for command and control in maritime cyber attacks
	Efficient Hash-Based Redactable Signature for Smart Grid Applications





Program – 27th Sep.

15:20 – 15:40	☕ Coffee Break
15:40 – 16:40	📍 Sankt Hans Torv & Nørrebros Runddel What does the future hold for AI and privacy?
17:30 – 19:00	🎪 Social Event
19:00 ~	🍷 Conference Banquet

Program – 28th Sep.

08:00 – 09:00	Registration
09:00 – 10:00	 Sankt Hans Torv & Nørrebros Runddel A Perspective on IoT Security
10:00 – 10:20	 Coffee Break
10:20 – 11:20	 Sankt Hans Torv & Nørrebros Runddel Session: IoT Security I
	fASLR: Function-Based ASLR for Resource-Constrained IoT Systems
	An Infection-Identifying and Self-Evolving System for IoT Early Defense from Multi-Step Attacks
	IoTEnsemble: Detection of Botnet Attacks on Internet of Things
10:20 – 11:20	 Hovedbanegården Session: Applications I
	A toolbox for verifiable tally-hiding e-voting systems
	How to Verifiably Encrypt Many Bits for an Election?
	A framework for constructing Single Secret Leader Election from MPC
10:20 – 11:20	 Kødbyen & Enghave Plads Session: Network and SW Security I
	Towards a Systematic and Automatic Use of State Machine Inference to Uncover Security Flaws and Fingerprint TLS Stacks
	PanoptiCANs - Adversary-resilient Architectures for Controller Area Networks
	Detecting Cross-Language Memory Management Issues in Rust



Program – 28th Sep.

11:40 – 12:20	 Sankt Hans Torv & Nørrebros Runddel Session: IoT Security II
	IoTPrivComp: A Measurement Study of Privacy Compliance in IoT Apps
	No-Label User-Level Membership Inference for ASR Model Auditing
11:40 – 12:20	 Hovedbanegården Session: Applications II
	AppBastion: Protection from Untrusted Apps and OSes on ARM
	Collaborative anomaly detection system for charging stations
11:40 – 12:20	 Kødbyen & Enghave Plads Session: Network and SW Security II
	Reach Me if You Can: On Native Vulnerability Reachability in Android Apps
	Extensible Virtual Call Integrity
12:20 – 14:00	 Luncheon

Program – 28th Sep.

 Sankt Hans Torv & Nørrebros Runddel Session: Hardware Security	
14:00 – 15:00	CPU Port Contention Without SMT
	Protocols for a Two-Tiered Trusted Computing Base
	Using Memristor Arrays as Physical Unclonable Functions
 Hovedbanegården Session: Web Security I	
14:00 – 15:00	Browser-based CPU Fingerprinting
	Introducing polymorphic protocols to limit the influence of web bots
	Unlinkable Delegation of WebAuthn Credentials
 Kødbyen & Enghave Plads Session: Cyber-Physical System Security II	
14:00 – 15:00	Can Industrial Intrusion Detection Be SIMPLE?
	For your Voice Only: Exploiting Side Channels in Voice Messaging for Environment Detection
	Towards Efficient Auditing for Real-Time Systems
15:00 – 15:40  Coffee Break	
 Sankt Hans Torv & Nørrebros Runddel Session: Multiparty Computation	
15:40 – 16:40	SecureBiNN: 3-Party Secure Computation Framework for Binarized Neural Network Inference
	Mixed-Technique Multi-Party Computations Composed of Two-Party Computations
	PEA: Practical Private Epistasis Analysis using MPC

Program – 28th Sep.

 Hovedbanegården Session: Web Security	
15:40 – 16:40	Large Scale Analysis of DoH Deployment on the Internet
	Equivocal URLs: Understanding the Fragmented Space of URL Parser Implementations
	Exploring the Characteristics and Security Risks of Emerging Emoji Domain Names
16:40 – 17:00  Best Paper Award & Concluding Remarks	

Workshop – 29th Sep.

09:00 – 13:00	STAST	📍 Hovedbanegården
	CBT	📍 Tivoli
	CyberICPS	📍 Enghave Plads
	SECPRE	📍 Enghave Plads
	DPM	📍 Vesterbros Torv
10:00 – 10:20 ☕ Coffee Break	STM	📍 Kødbyen
12:20 – 14:00	🍷 Luncheon	
14:00 – 18:00	STAST	📍 Hovedbanegården
	CBT	📍 Tivoli
	CyberICPS	📍 Enghave Plads
	SECPRE	📍 Enghave Plads
	DPM	📍 Vesterbros Torv
15:20 – 15:40 ☕ Coffee Break	STM	📍 Kødbyen

Workshop – 30th Sep.

09:00 – 13:00	ETAA	📍 Kødbyen
	ADIoT	📍 Hovedbanegården
	SP-MIoT	📍 Hovedbanegården
	CPS4CIP	📍 Enghave Plads
	SPOSE	📍 Tivoli & Vesterbros Torv
10:00 – 10:20 ☕ Coffee Break	CDT & SECOMANE	🌐 Online-Only
12:20 – 14:00	🍷 Luncheon	
14:00 – 18:00	ETAA	📍 Kødbyen
	ADIoT	📍 Hovedbanegården
	SP-MIoT	📍 Hovedbanegården
	SecAssure	📍 Enghave Plads
	EIS	🌐 Online-Only
15:20 – 15:40 ☕ Coffee Break		