SeRIM 2025

1st International Workshop on Security and Risk in Identity Management

July 4, 2025 • Venice, Italy

SeRIM 2025
Organizing Committees

General Co-Chairs:

- Riccardo Focardi (Ca' Foscari University of Venice)
- Silvio Ranise (Fondazione Bruno Kessler and University of Trento)

Program Co-Chairs:

- Flaminia Luccio (Ca' Foscari University of Venice)
- Giada Sciarretta (Fondazione Bruno Kessler)

Publication Co-Chairs:

- Matteo Busi (Ca' Foscari University of Venice)
- Marco Pernpruner (Fondazione Bruno Kessler)

Who We Are
Ca' Foscari University of Venice (UniVE)

- **Public University** in Venice, Italy
- 8 departments, 3 schools

UniVE at a glance

27.000+
alumni

23.000+
students

1.500+
intl. students/yr

7.000+
new students/yr

5.000+
graduates/yr

1.400+
faculty, researchers, and staff

100+
visiting professors

Who We Are

Department of Environmental Sciences, Informatics and Statistics: Cryptography Lab

Cybersecurity Lab

- Applied Cryptography
- Network and Web Security
- Software Security
- Embedded System Security
- Usable Security
- Authentication methods/Biometrics

Research group

- Matteo Busi
- Stefano Calzavara
- Paolo Falcarin
- **Riccardo Focardi**
- Flaminia Luccio

Collaborations

- Cispa Helmoltz center for Information Security, Germany
- Masaryk University, Brno, CZ
- TU Wien, Austria
- …

Who We Are
Cybersecurity Lab

Projects

SPOKE 6: Software and Platform Security

-SCAI Project

PRIN PNRR Project: AMADEUS Automatic Modelling and verificAtion of Dedicated sEcUrity deviceS

EU HORIZON-CL3-2024-CS-01 Increased Cybersecurity

Project Cybersecurity Certification and Assessment Tools (CCAT)

Spin offs

- **Cryoptosense**: produces software for security analysis of cryptographic systems

- **10Sec:** security for automotive, embedded, and IoT systems

Publications

- S Calzavara, S Casarin, R Focardi. Dynamic Security Analysis of JavaScript: Are We There Yet? Proceedings of the ACM on Web Conference 2025, 1105-1115
- Riccardo Focardi and Flaminia Luccio. A formally verified configuration for Hardware Security Modules in the cloud. In Giovanni Vigna, Elaine Shi, Proceedings of the ACM Conference on Computer and Communications Security (ACM CCS), pp. 412-428, 2021
- Stefano Calzavara, Riccardo Focardi, Matús Nemec, Alvise Rabitti, Marco Squarcina: Postcards from the Post- HTTP World: Amplification of HTTPS Vulnerabilities in the Web Ecosystem. IEEE Symposium on Security and Privacy (IEEE S&P 2019), pp. 281-298, 2019
- Claudio Bozzato, Riccardo Focardi, Francesco Palmarini. Shaping the Glitch: Optimizing Voltage Fault Injection Attacks. In Transactions on Cryptographic Hardware and Embedded Systems (TCHES), vol. 2019, pp. 199-224,2019
- Riccardo Focardi, Francesco Palmarini, Marco Squarcina, Graham Steel, Mauro Tempesta: Mind Your Keys? A Security Evaluation of Java Keystores. Proceedings of the Network and Distributed System Security Symposium (NDSS 2018), 2018
- Stefano Calzavara, Riccardo Focardi, Matteo Maffei, Clara Schneidewind, Marco Squarcina, Mauro Tempesta WPSE: Fortifying Web Protocols via Browser-Side Security Monitoring , Proceedings of the 27th USENIX Security Symposium, pp. 1493-1510, 2018

Who We Are
Fondazione Bruno Kessler (FBK)

- Research and Innovation institute in Trento, Italy
- 12 research centers: from technology to humanities and social sciences

Who We Are
Cybersecurity Center - FBK

Applied Cryptography

Match cutting-edge cryptography with real use scenarios (e.g., digital identity, e-voting, cloud computing)

- Privacy enhancing cryptography
- Cryptographic access control
- Threshold cryptography

Security in distributed computing environment

Develop novel AI-driven methods for cyber threat detection in distributed computing environments

- AI-driven Threat and Anomaly Detection
- Privacy-preserving training
- Service and Security OrchestratioN
- Cyber Deception
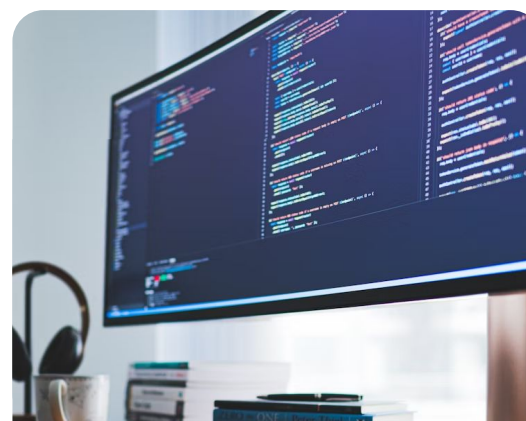
Software Security

Networking and application security

- Secure continuous integration
- Regular compliance
- AI for code security

Digital Identity Management

Design and security assessment of enrollment, authentication, and authorization solutions

- Multi factor authentication
- Single Sign-On
- Digital identity wallet

Who We Are
Cybersecurity Center - FBK

SERICS
SECURITY AND RIGHTS IN THE CYBERSPACE

Spoke 4 (Operating Systems and Virtualization Security) - project
Securing Containers (SecCo)

Spoke 5 (Cryptography and Distributed Systems Security) - project
Secure and TRaceable Identities in Distributed Environments (STRIDE)

CieID

Login with CIE
(Electronic Identity Card)

POLIGRAFICO E ZECCA DELLO STATO ITALIANO

eID.AS
NOTIFIED

OpenID Connect

transition from SAML 2.0 to OIDC

Digital Identity Wallet

IT Wallet technical specification

https://italia.github.io/eid-wallet-it-docs/versione-corrente/en/

POLIGRAFICO E ZECCA DELLO STATO ITALIANO

Credential Issuer

padppa

Wallet Provider

Large Scale Pilot (LSP)

Potential For European Digital Identity
Co-funded by the European Union

Trentino Digitale SpA
PROVINCIA AUTONOMA DI TRENTO

LSP APTITUDE
LSP WE BUILD

- A. Flamini, G. Sciarretta, M. Scuro, A. Sharif, A. Tomasi, S. Ranise. **On Cryptographic Mechanisms for the Selective Disclosure of Verifiable Credentials**. In: *JISA*.
- A. Sharif, Z. E. Ansaroudi, G. Sciarretta, D. Pöhn, M. Mollaeefar, W. Hommel, S. Ranise. **Protecting Digital Identity Wallet: A Threat Model in the Age of eIDAS 2.0**. In: *CRiSIS 2024*.
- Z. E. Ansaroudi, A. Sharif, G. Sciarretta, F. A. Marino, S. Ranise. **Secure and Reliable Digital Wallets: A Threat Model for Secure Storage in eIDAS 2.0**. In: *DBSec 2025*.
- R. Germenia, S. Manfredi, G. Sciarretta, M. Scuro, and A. Tomasi. **Comparison of Credential Status Mechanisms for the Digital Wallet Ecosystem**. In: SECRYPT 2025.

For more details https://cs.fbk.eu/

8

SeRIM 2025
Scope

Exploring security and risk assessment in identity management systems, by investigating how to evaluate the security posture of identity solutions, assess risks, identify suitable security controls together with privacy enhancing techniques, and ensure compliance with regulations.

| Security | Risk | Privacy | Regulations |
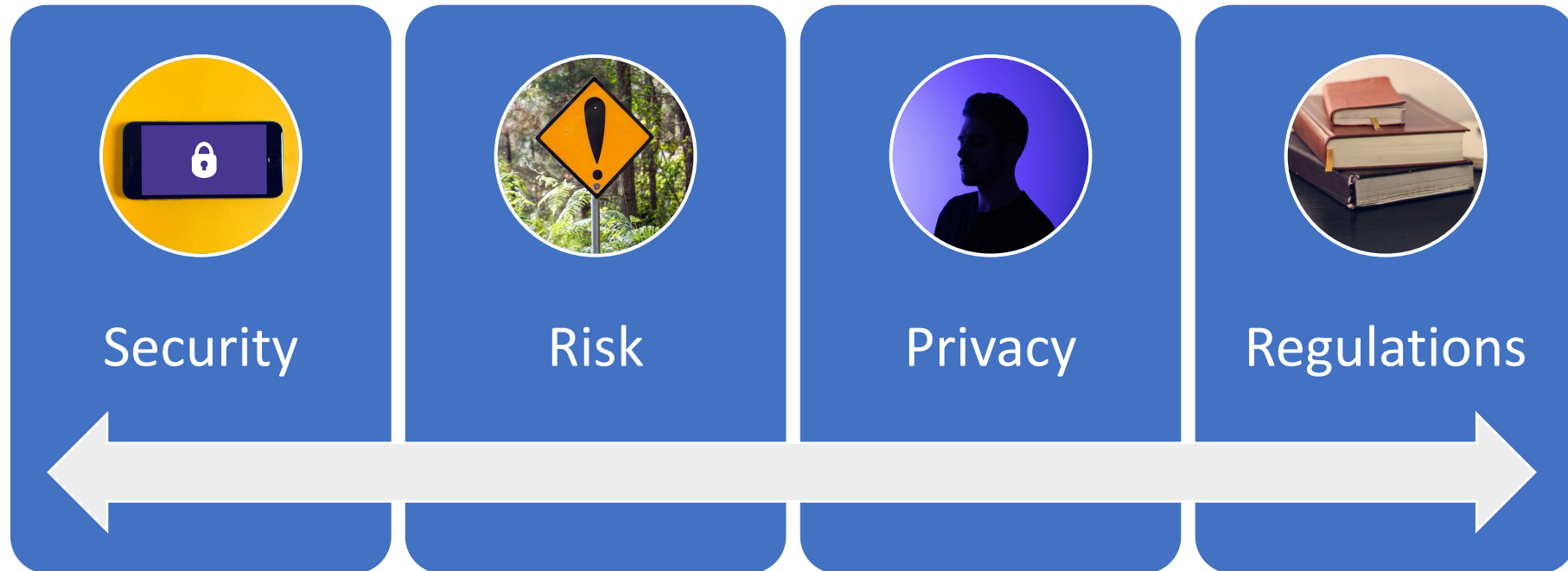
SeRIM 2025
Program Committee

- Roberto Carbone (Fondazione Bruno Kessler)
- Letterio Galletta (IMT School for Advanced Studies Lucca)
- Marino Miculan (University of Udine)
- Simone Onofri (W3C)
- Federica Maria Francesca Paci (University of Verona)
- Marco Patrignani (University of Trento)
- Pieter Philippaerts (KU Leuven)
- Avinash Sudhodanan (Independent Researcher)
- Luca Viganò (King's College London)

7 submissions

5 accepted

SeRIM 2025
Agenda

Introductory Remarks Riccardo Focardi, Silvio Ranise (General Co-Chairs), Flaminia Luccio, Giada Sciarretta (Program Co-Chairs)	9:00-9:15
Session 1: Keynote *Session Chair: Riccardo Focardi*	
Modeling the Web to Secure the Web: Formal Analysis of Single Sign-On Authentication and Authorization Protocol Standards Ralf Küsters (University of Stuttgart)	9:15-10:15
Session 2: Regular Papers *Session Chair: Matteo Busi*	
Decentralised Supply Chain Reputation: A Privacy and Self-Sovereign Identity Perspective Abubakar-Sadiq Shehu and Steve Schneider (University of Surrey)	10:15-10:35
Identity Threats and Where to Find Them: Mapping ITDR and MITRE ATT&CK Vitali Serzantov, Erwin Kupris and Thomas Schreck (Munich University of Applied Sciences)	10:35-10:55
Coffee Break	11:00-11:30
Replication Study: Cross-Country Evaluation of the Recognition-Based Graphical Authentication Scheme in AR and VR Environments Naheem Noah (University of Denver), Peter Mayer (University of Southern Denmark) and Sanchari Das (George Mason University)	11:30-11:50
Session 3: Short Papers *Session Chair: Roberto Carbone*	
Security Requirements Classification by Means of Explainable Transformer Models Luca Petrillo (IMT Lucca and IIT-CNR), Fabio Martinelli (ICAR-CNR), Antonella Santone (University of Molise) and Francesco Mercaldo (University of Molise and IIT-CNR)	11:50-12:05
Towards Privacy-Preserving Revocation of Verifiable Credentials with Time-Flexibility Francesco Buccafurri and Carmen Licciardi (University Mediterranea of Reggio Calabria)	12:05-12:20
Closing Remarks	12:20-12:30
Lunch	13:00-14:00