

# CYSARM

2<sup>ND</sup> WORKSHOP ON  
**CYBER-SECURITY  
ARMS RACE**

NOVEMBER 13, 2020 - VIRTUAL EVENT

Sponsors:

- FutureTPM (GA: 779391)
- INCOGNITO (GA:824015)
- ASTRID (GA: 786922) and
- GUARD (GA: 833456) projects.



All projects have received funding from the European Union's Horizon 2020 research and innovation programme under the above-mentioned grant agreement numbers.



INCOGNITO



GUARD

## AGENDA

# AGENDA

Please access the workshop via Zoom - [click here](#).

10am-2pm Eastern Time (4pm-8pm European Central Time)

10:00-10:15 Welcome and Introduction

**Morning Session Chair:** Daniele Sgandurra

10:15-11:00

**Keynote #1** – Software and hardware vulnerabilities in Intel SGX

**David Oswald** (University of Birmingham)

**Regular Papers Session #1** - [11:00-12:00]

11:00-11:30

Protecting Enclaves from Intra-Core Side-Channel Attacks through Physical Isolation

**Marno van der Maas** (University of Cambridge)  
**Simon Moore** (University of Cambridge)

11:30-12:00

Efficiency Improvements for Encrypt-to-Self

**Jeroen Pijnenburg** (Royal Holloway, University of London)  
**Bertram Poettering** (IBM Research)

● 12:00-12:15 **Virtual Break**

**Afternoon Session Chair:** Thanassis Giannetsos

12:15-13:00

**Keynote #2** – Enabling Trusted Digital Identities – From Connected Citizens to Connected Objects

**Ioannis Krontiris** (Huawei Technologies)

**Short Papers Session #2** - [13:00-14:00]

13:00-13:30

**Short paper:** Automatic configuration for an optimal channel protection in virtualized networks

**Daniele Brighenti** (Politecnico di Torino)  
**Guido Marchetto** (Politecnico di Torino)  
**Riccardo Sisto** (Politecnico di Torino)  
**Fulvio Valenza** (Politecnico di Torino)

13:30-14:00

**EU Project Presentations:** Short presentations for EU Projects FutureTPM, INCOGNITO, ASTRID, GUARD

14:00

**Closing Remarks**