



# RAID2021 - The 24th International Symposium on Research in Attacks, Intrusions and Defenses

06.Oct - 08.Oct 2021

Cod. Z18-21



**Mod.:**

Streaming Face-to-face

**Edition**

2021

**Activity type**

Workshop

**Date**

06.Oct - 08.Oct 2021

**Location**

Kursaal

**Languages**

English

**Academic Validity**

30 hours

**Organising Committee**



## Description

**The Workshop will be held face-to-face and there will also be the possibility of participating live online through ZOOM. In the registration process, please select the participation of your choice: face-to-face or live online.**

Since its inception in 1997, the International Symposium on Research in Attacks, Intrusions and Defenses (RAID) has established itself as a venue where leading researchers and practitioners from academia, industry, and the government are given the opportunity to present novel research in a unique venue to an engaged and lively community.

The conference is known for the quality and thoroughness of the reviews of the papers submitted, the desire to build a bridge between research carried out in different communities, and the emphasis given on the need for sound experimental methods and measurement to improve the state of the art in cybersecurity.

This year we are soliciting research papers on topics covering all well-motivated computer security problems. We care about techniques that identify new real-world threats, techniques to prevent them, to detect them, to mitigate them or to assess their prevalence and their consequences. Measurement papers are encouraged, as well as papers offering public access to new tools or datasets, or experience papers that clearly articulate important lessons learned. Specific topics of interest to RAID include, but are not limited to:

- Computer, network, and cloud computing security
- Malware and unwanted software
- Program analysis and reverse engineering
- Mobile Security
- Web security and privacy
- Vulnerability analysis techniques
- Usable security and privacy
- Intrusion detection and prevention
- Hardware security
- Cyber physical systems security and threats against critical infrastructures
- IoT security
- Statistical and adversarial learning for computer security
- Cyber crime and underground economies
- Denial-of-Service attacks and defenses
- Security measurement studies
- Digital forensics

Papers will be judged on novelty, significance, correctness, and clarity. We expect all papers to provide enough detail to enable reproducibility of their experimental results. We encourage authors to make both the tools and data publicly available.

## Objectives

Present, discover and discuss techniques that identify new cyber threats in the real world, techniques to prevent, detect, mitigate them or evaluate their prevalence and consequences.

## Course specific contributors



**SOPHOS**



**RENIC**  
Red de Excelencia Nacional de  
Investigación en Ciberseguridad

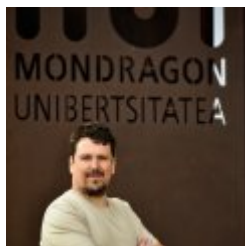


HEZKUNTZA SAILA  
DEPARTAMENTO DE EDUCACIÓN



GRUPO **Billingham**  
Regalos y Merchandising

## Directed by



### **Urko Zurutuza Ortega**

Mondragon Unibertsitatea

---

## Teachers



**Mathias Payer**

EPFL IC IINFCOM HEXHIVE

---

# Registration fees

<b>FACE-TO-FACE</b>	<b>UNTIL 06-09-2021</b>	<b>UNTIL 05-10-2021</b>	<b>UNTIL 08-10-2021</b>
Regular	600,00 EUR	700,00 EUR	850,00 EUR
Student	450,00 EUR	550,00 EUR	-
Student Grant holder	300,00 EUR	300,00 EUR	-
Collaborators	-	-	0 EUR

<b>LIVE ONLINE - ZOOM</b>	<b>UNTIL 06-09-2021</b>	<b>UNTIL 05-10-2021</b>	<b>UNTIL 08-10-2021</b>
Regular / Student	-	50,00 EUR	-
Author	-	250,00 EUR	-
Collaborators	-	0 EUR	-

## **Place**

### **Kursaal**

Avda. de la Zurriola,1 , 20002 Donostia/San Sebastián

Gipuzkoa