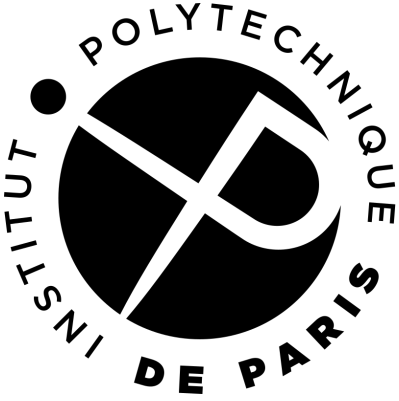


MIC-SEC 2022 - Retrospective

Maria MUSHTAQ,
maria.mushtaq@telecom-paris.fr

Retrospective Presentation

Outline

Outline

Organization

5 - 9 December 2022 : FIAP Paris

Organizers

- Maria Mushtaq (Télécom Paris , IP Paris)
- Ulrich Kühne (Télécom Paris, IP Paris)

Collaborators

- Karine Heydemann (LIP6, Sorbonne University)
- Quentin L. Meunier (LIP6, Sorbonne University)

An International Winter School

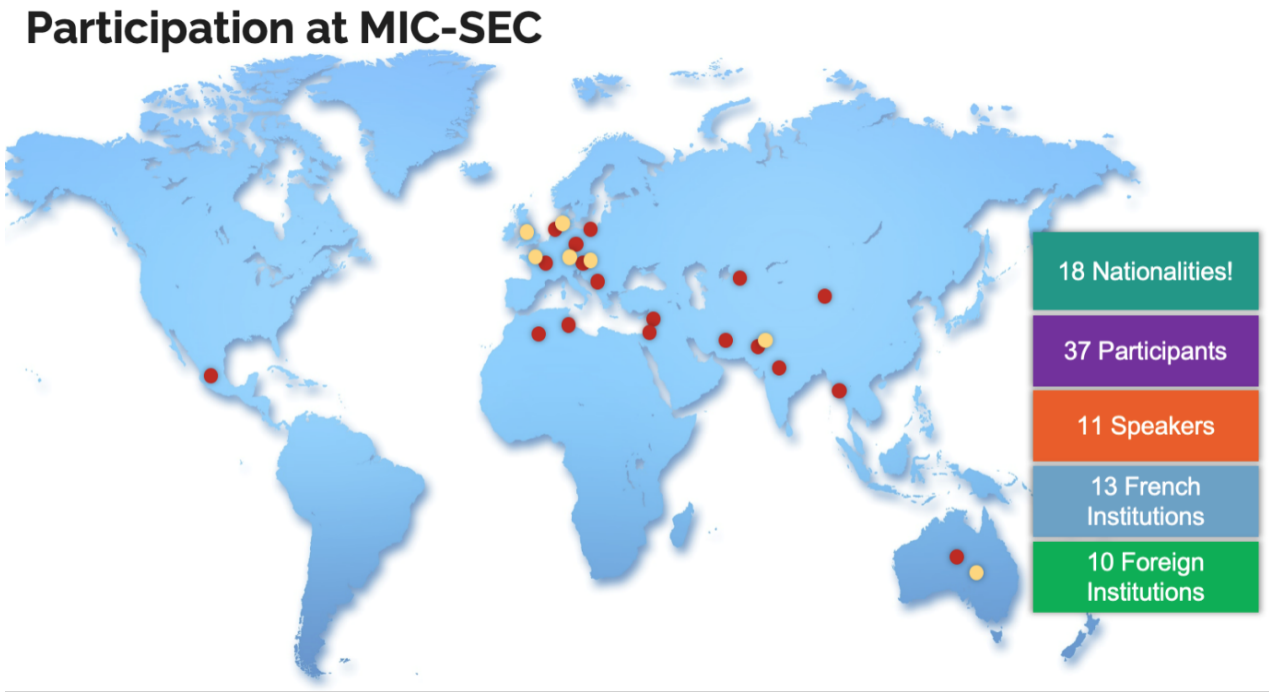


Figure: An international participation

Outline

Scope

3 Topics around Micro-Architectures security

1. Side Channel Attack and defenses
2. Role of Machine Learning in Microarchitectural security
3. Microarchitectural security at the interfaces of hardware and software, in particular industrial perspectives

Speakers

International and Top Researchers of the field

- Lejla BATINA, Radboud University, Netherlands
- Lorenzo CAVALLARO, University College London, UK
- Guy GOGNIAT, Université Bretagne Sud, France
- Sylvain GUILLEY, Secure-IC, France
- Jawad HAJ YAHYA, Rivos inc, Switzerland
- Nele MENTENS, Leiden University, Netherlands
- Stjepan PICEK, Radboud University, Netherlands
- Frank PIESSENS, KU Leuven, Belgium
- Michael SCHWARZ, CISPA, Germany
- Philippe TANGUY, Université Bretagne Sud, France
- Yuval YAROM, University of Adelaide, Australia

Outline

Talks

Day 1

- Jawad HAJ YAHYA, "Security Implications of Power Management Mechanisms in Modern Processors: Current Studies and Future Trends"
- Frank PIESSENS, "Transient execution attacks and defenses"
- Lorenzo CAVALLARO, "Trustworthy Machine Learning...for Systems Security"

Talks

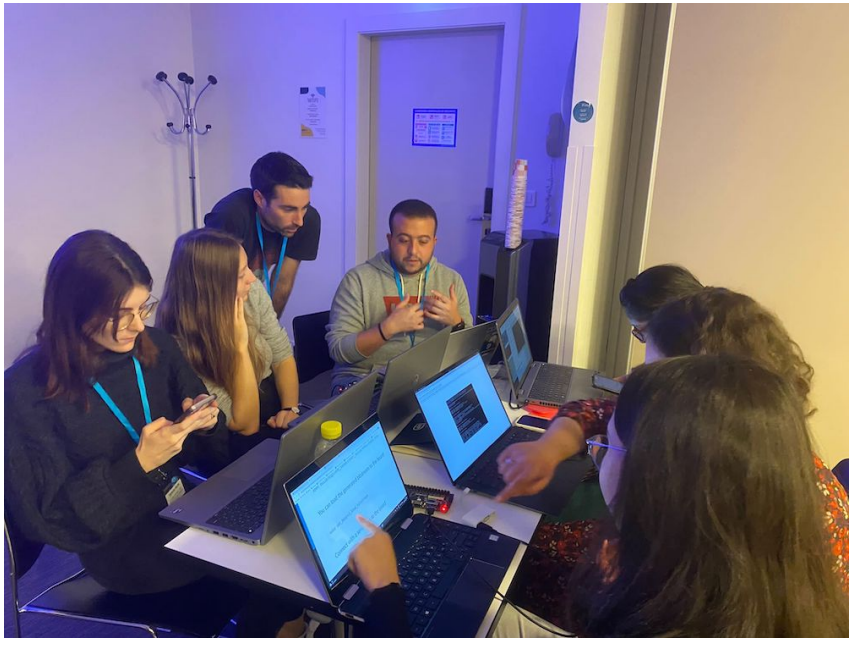
Day 2

- Michael SCHWARZ, "From Random Observations to Automated Leakage Discovery"
- Michael SCHWARZ, "Turning Timing Differences into Data Leakage" (hands-on session)
- Guy GOGNIAT, "Requirements and Security Challenges for Resource-Constrained IoT End-Devices Baseband Processor"
- Philippe TANGUY, "How to quickly deploy a SoC on FPGA to evaluate security solutions for communicating embedded systems?" (hands-on session)

Talks

Day 3

- Yuval YAROM, "A Primer on Cache Attacks" (tutorial)
- Yuval YAROM, "The Gates of Time: Improving Cache Attacks with Transient Execution" (talk)
- Sylvain GUILLEY, "The standards of embedded security"



Talks

Day 4

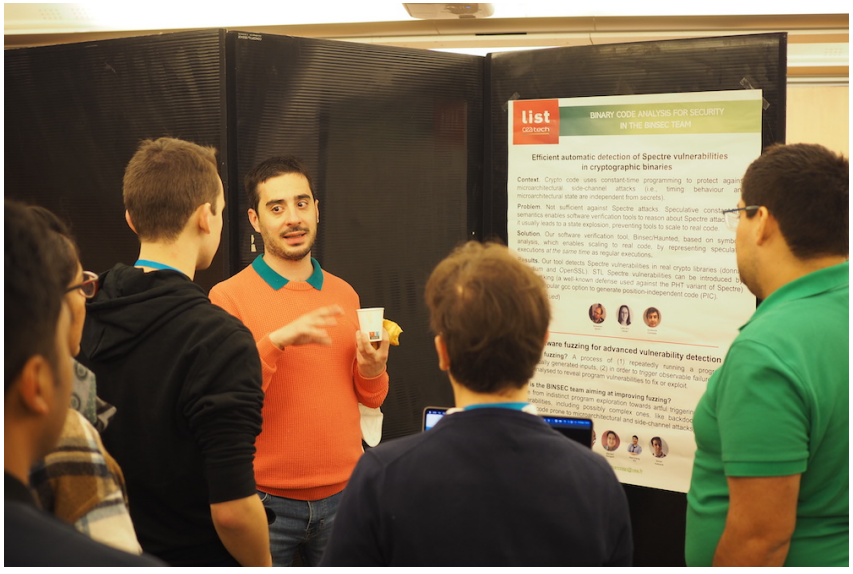
- Lejla BATINA, "AI and Side-channel analysis: Lessons learned so far"
- Stjepan PICEK, "Securing AI: On the Intentional Failures and How to Prevent Them"
- Nele MENTENS, "Security challenges and opportunities in emerging device technologies"

Posters Presentation

Day 5

9 Posters presentations selected by scientific committee

- Ph.D Thesis
- Research Topics
- University collaborations



Events

Sharing and networking moments

- Welcome Cocktail
- Coffee breaks and talks
- Gala Dinner on a Bateau Mouche

Outline

Testimonies

Conclusion

Thank you!