

PHISIC 2019

Workshop on Practical Hardware Innovation in Security and Characterization

Tuesday 15 October 2019

	Session	Speaker	Subject
08:30			
(30m)	Registration / Coffee		
09:00			
(10m)		Technical Committee	Introduction
09:10			
(1h)	Keynote	Guénaél Renault	Post-Quantum Cryptography - A Pragmatic Point of View
10:10			
(10m)		Angeline Ottolini	Presentation of MicroPacks
10:20			
(20m)	Pause / Demos / Posters / Coffee		
10:40			
(25m+5m)	Security: From primitives to trust	Lilian Bossuet	Security of the Integrated Circuit Life Cycle
(25m+5m)		Mathieu Escouteloup	Microarchitecture security
(25m+5m)		Michael Pehl	Predictability Tests for Physical Unclonable Functions
(25m+5m)		Yan Loisel	RISC-V security
12:40			
(1h20m)	Lunch		
14:00			
(25m+5m)	Pole SCS: advances in hardware security through academic-industrial collaborations	Paul-Emmanuel Brun	How to optimize security in the IoT ?
(25m+5m)		Philippe Maurine	Electromagnetic injection: advanced platform & modeling & countermeasures
(25m+5m)		Laurent Masson	Secure Microcontroller for IoT
(25m+5m)		Pierre-Yvan Liardet	Advanced processes of Laser Injection for Sedentary Analyses
16:00			
(30m)	Pause / Demos / Posters		
16:10			
(...)	Departure by bus for touristic tour & Cocktail Dinner		
16:15			
(...)			
(...)	Touristic tour		
19h			
(...)	Cocktail Dinner		

October 15th-16th 2019
 Campus Georges Charpak Provence, Gardanne
<https://events.emse.fr/physic2019>

PHISIC 2019

Workshop on Practical Hardware Innovation in Security and Characterization

Wednesday 16 October 2019

	Session	Speaker	Subject
08:30			
(30m)	Registration		
09:00			
(25m+5m)	Fault injection: models and attacks	Julien Proy	ISA-Level Characterization of EM Pulse Effects on Superscalar Microarchitectures, A Secure Software Perspective
(25m+5m)		Ronan Lashermes	Electromagnetic fault injection against a System-on-Chip, new micro-architectural fault models
(25m+5m)		Jordi Mujal	LLFI: Lateral Laser Fault Injection Attack
(25m+5m)		Mathieu Dumont	Electromagnetic Fault injection, how fault occurs
11:00			
(20m)	Pause / Demos / Posters / Coffee		
11:20			
(25m+5m)	SCA I: Machine learning for Side channel	Gabriel Zaid	Methodology for Efficient CNN Architectures in Profiling Attacks
(25m+5m)		Loic Masure	A comprehensive study of Deep Learning for Side-Channel Analysis
12:20			
(1h20m)	Lunch		
13:40			
(25m+5m)	SCA II: Side channel without physical access	Giovanni Camurati	Screaming Channels: When Electromagnetic Side Channels Meet Radio Transceivers
(25m+5m)		Davide Alessio	Revisiting Higher-Order Computational Attacks against White-Box Implementations
(25m+5m)		Joseph Gravelier	Remote hardware attacks on connected devices
15:10			
(20m)	Pause / Demos / Posters		
15:30			
(25m+5m)	Protections: addressing a variety of threats	Luca di Féo	Side channel protections for CSIDH
(25m+5m)		Rémi Bernhard	Impact of Low-bitwidth Quantization on the Adversarial Robustness for Embedded Neural Networks
(25m+5m)		Nicolò Maunero	An FPGA-based Control-Flow Integrity solution for securing Embedded Systems
17:00			

