Preface of the 2nd Workshop on the Security of Software/Hardware Interfaces (SILM 2020)

Guillaume Hiet
IRISA
CentraleSupélec/Inria
Rennes, France
guillaume.hiet@centralesupelec.fr

Frédéric Tronel
IRISA
CentraleSupélec/Inria
Rennes, France
frederic.tronel@centralesupelec.fr

Jean-Louis Lanet
IRISA
Inria
Rennes, France
jean-louis.lanet@inria.fr

Message from the SILM 2020 organizers

The workshop on the Security of Software/Hardware Interfaces (SILM 2020) held its second edition on September 11th, 2020 as an all-digital event co-located with the 5th IEEE European Symposium on Security and Privacy (EuroS&P 2020).

This workshop was organized as part of the SILM thematic semester funded by the French DGA and managed by Inria for the different partners of the PEC General Partnership Agreement.

It is becoming increasingly important to combine software and hardware aspects to take into account new software attacks. For example, hardware vulnerabilities such as Spectre or Meltdown can be exploited by purely software attacks. Such attacks can be executed remotely and do not require physical access to the targeted hardware platform. At the other side of the coin, hardware features can be used to better detect and respond to traditional software attacks, such as memory corruption. Therefore, it is necessary to study in-depth the security of software/hardware interfaces, both in terms of attacks and defences.

The purpose of the SILM workshop is to share experiences, tools, and methodologies to handle security in software/hardware interfaces. On the one hand, we need to better assess the security guarantees provided by existing hardware architectures against software attacks, especially attacks against micro-architecture. This can be achieved by identifying new vulnerabilities using reverse engineering, fuzzing or other attack approaches. On the other hand, we also need to propose new architectures offering better resilience against software attacks. Theses architectures should rely on hardware-based security mechanisms to protect the software stack. One of the challenges is to formally specify and verify the security guarantees offered by such architectures.

The goal of this second edition of the SILM workshop is to provide a forum for researchers and practitioners from academia, industry, and government that work on the security of software/hardware interfaces.

We would like to thank the SILM 2020 Program Committee, authors, speakers and attendees who contributed to the fruitful discussions held during the workshop sessions, and the IEEE European Symposium on Security and Privacy workshops organizers for their support while organizing this event.

SILM 2020 Organization

Program and Organization Committee Chairs

Guillaume Hiet (CentraleSupélec/Inria)
Jean-Louis Lanet (Inria)
Frédéric Tronel (CentraleSupélec/Inria)

Program Committee

Pascal Cotret (ENSTA Bretagne)
Damien Couroussé (CEA)
Chris Dalton (HP Labs)
Lucas Davi (University of Duisburg-Essen)
Steven Derrien (University of Rennes 1)
Guy Gogniat (Univ. South Brittany)
Karine Heydemann (LIP6)
Vianney Lapôtre (Univ. South Brittany)
Cristofaro Mune (Pulse Security)
Yves-Alexis Perez (ANSSI)
Kaveh Razavi (ETH Zurich)
Jan Reineke (Saarland University)
Erven Rohou (Inria)
Simon Rokicki (ENS Rennes)
André Seznec (Inria)
Volker Stolz (HVL)
Arnaud Tisserand (CNRS)
Pierre Wilke (CentraleSupélec/Inria)
Yossi Oren (Ben-Gurion University)
Yuval Yarom (University of Adelaide and Data61)

DOI 10.1109/EuroSPW51379.2020.00097