Einladung zum Vortrag

24. April 2018, 10 Uhr s.t.
Universität Bremen | MZH 4380
(ACHTUNG | SONDERTERMIS & -ORT)

Dr.-Ing. Shahin Tajik
TU Berlin | Security in Telecommunications

Threat Assessment of IC Reverse-Engineering through Optical Probing Attack

A wide variety of deployed embedded devices in consumer, industrial and military applications are targets of reverse-engineering and Intellectual Property (IP) piracy. The main motivation behind reverse-engineering is to get access to the stored secrets and employed IP on the integrated circuits (ICs) to counterfeit and overbuild the target products. Cloning of a design can be carried out by mounting physical attacks, such as side-channel analysis. Although modern ICs have integrated several countermeasures to mitigate such attacks, a proper protection scheme against optical attacks conducted from the IC backside is still missing. The primary reason that the IC backside protection is ignored by the vendors is the misconception that optical attacks cannot be scaled to the very latest nanoscale technologies without further effort and cost. In this talk, we assess the attack effort against a commercial device in a real scenario, where the adversary has no knowledge of underlying hardware implementation. We demonstrate that the adversary is able to extract the sensitive design information and IP from the target device in a short amount of time, with a limited budget. Finally, we propose and discuss potential countermeasures, which could protect the chips against optical attacks mounted from the IC backside.

Biografie

Shahin Tajik is a postdoctoral associate of the working group SECT, a collaboration of the Technical University of Berlin and Deutsche Telekom Innovation Laboratories. He completed his Ph.D. studies in the field of hardware security at the Technical University of Berlin in 2017. His field of research includes non-invasive and semi-invasive attacks, Physically Unclonable Functions (PUFs), security evaluation of FPGAs, and providing tamper protection mechanisms against attacks conducted from the IC backside. Shahin Tajik has already published several academic publications in the world’s top-tier hardware security conferences and journals, such as CHES and the Journal of Cryptology. Recently, his paper with the title “On the Power of Optical Contactless Probing: Attacking Bitstream Encryption of FPGAs” was awarded the 1st place in Applied Research Competition of European Cyber Security Awareness Week (CSAW) in 2017.

Dieser Gast wurde von Rolf Drechsler eingeladen.