General information

CEA List *Fabrice AUZANNEAU* *fabrice.auzanneau@cea.fr*
+33 1 69 08 90 60

Targeted topics

SU-INFRA01-2018-2019-2020	Prevention, detection, response and mitigation of combined physical and cyber threats to critical infrastructure	IA
SU-DS04-2018-2020	Electrical Power and Energy System	IA
SU-ICT-01-2018 – b)	Dynamic countering of cyber-attacks – strand b)	IA

Competencies

DATA PROTECTION

- *Lightweight cryptography*
  - **High performance cryptography for highly constrained things**
  - **8bit to 64bit CPU implementations of lightweight stream ciphers, with counters-measures against power/fault-injection attacks**

- *Homomorphic encryption*
  - **Computing with encrypted data, without decrypting it: enables processing of confidential data on untrusted servers.**
  - **CEA compiler transforms C++ algorithm into equivalent, privacy-preserving code, with minimal computational overhead.**
  - **Millisecond bootstrapping scheme to reduce cryptographic noise**

- *Detection of cyber-attacks in IoT*
  - **Physical and logical attacks**
  - **Monitoring and light-weight machine learning techniques**

Competencies

CODE PROTECTION

- *Compilation of software countermeasures*
  - **Countermeasures against side-channel attacks**
  - **Code polymorphism: behavioral variability to thwart side-channel attacks.**
  - **Suitable for computing & memory constrained embedded processors (IoT, mobile applications)**

- *Countermeasures against fault-injection attacks*
  - **Fault tolerance, including against multiple fault injections**
  - **Fault detection & Control-Flow Integrity**
  - **Fine-grain integrity of program execution: detection of integrity violations at the granularity of a single machine instruction**

HW PROTECTION

- *Secure hypervision with arm trustzone*
  - **Data protection & error isolation through memory partitioning and protection.**
  - **« Blind » hypervision protects from attacks from other domains, and from hypervisor itself**
  - **Minimal Trusted Computing Base implemented in ARM/TrustZone, security formally verified with static code analysis**
  - **Experiences of Intel/SGX secure environment**

- *Many-core systems safety*
  - **Deterministic execution and interference-free cohabitation of mixed critical applications**