General information

CEA List *Etienne HAMELIN* *Etienne.hamelin@cea.fr*
01 69 08 00 22

Targeted topics

SU-DS04-2018-2020	Electrical Power and Energy System	IA
SU-DS05-2018-2019	Critical sectors: Privacy Accountability	IA
SU-ICT-01-2018	Dynamic countering of cyber-attacks	IA

Competencies

PROTECTING DATA

- *Lightweight cryptography*
  - **High performance cryptography for highly constrained things**

- *Homomorphic encryption*
  - **Computing with encrypted data without deciphering**
  - **Compiler infrastructure for high-level cryptocomputing-ready programming**
  - **Parallel code generation and « crypto-execution » runtime environment**
  - **Millisecond bootstrapping scheme to reduce cryptographic noise**

- *Learning for security*
  - **Detection of abnormal behavior**
  - **Cyber-attacks detection by learning**

Competencies

CODE PROTECTION

- *Code polymorphism*
  - **Randomly vary the observable behavior of a component without changing its functionality**
  - **Increase the difficulty of hidden channel attacks: required number of observation multiplied by 10 000**
  - **Suited for computing & memory constrained embedded processors (IoT, mobile applications)**

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**

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

not mandatory slide

Project idea

- *Describe your project idea*
- *List of the complementary skills you need for your consortium*