



RTCPS call 2014

SECODE

Pr. Jean-Luc Danger Télécom ParisTech/LTCI

SECODE GOALS

Secure Codes to thwart Cyber-physical Attacks

- To specify and design **error correction codes** suitable for an efficient protection of sensitive information in the context of Internet of Things (IoT) and connected objects.
- The codes can mitigate:
 - **passive attacks**, like memory disclosure, and
 - **active attacks**, like stack smashing.

SECODE GOALS

- It addresses:
 - **cyber attacks** (remote and software)
 - **physical attacks** (local, side-channel or fault injection).
- The objective is to **leverage the codes** for protecting against both cyber and physical attacks.
- The cyber and physical protections will take advantage of formal mathematical approaches which can **prove** their effectiveness.
- Some **demonstrations** will be performed on real platform with HW/SW implementations on real applications.

SECODEpartners



CODES as protections

Attack	Cyber	Physical
Passive	Randomization (ASLR, DIFT)	Randomization (masking, shuffling, blinding)
Active	Detection (canaries, CFI), tolerance (ASLR, code encryption with ASIST [CSS12])	Detection (redundancy in time, space, information), tolerance (infective countermeasures)

SECODE challenges

- **Physical attacks:**
 - Masking and Detection Multivariate secure with Codes.
 - Porting to Table-based countermeasures.
- **Code specifications:** Design of "Linear Complementary Dual" LCD codes
 - which are "Generalized Quasi Cyclic" (GQC).
 - Relations between LCD codes and AG codes (codes defined by an algebraic curve).
- **Cyber physical protected platform:**
 - Modified LLVM embedding protections based on codes.
 - Protected cryptoprocessor with codes for masking and fault detection.
 - Demonstrator in FPGA and open source CPU

SECODE outcomes

- Method to generate and execute **cyber-resilient software**
- **Protection** of data and its manipulation from **physical threats** like side-channel attacks.
- These results are demonstrated by using a smart sensor application **with hardened embedded firmware and tamper-proof hardware platform.**

THANK YOU