SECODE

Inria / IRISA project-team PACAP
Contact: erven.rohou@inria.fr
damien.hardy@irisa.fr
nicolas.kiss@inria.fr

https://secode.enst.fr/

Secure Codes to thwart Cyber-physical Attacks

GOAL

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.
- **active attacks**, like stack smashing.

It addresses:

- **cyber attacks** (remote and software)
- **physical attacks** (local, side-channel or fault injection)

The objective is to protect software by implementing "Linear Complementary Dual" LCD codes. These codes will be designed with formal mathematical approaches which can prove their efficiency. Codes will be applied automatically at **compile time**. Some demonstrations will be performed on real platform with HW/SW implementations on real applications.

OUTCOMES

- An LLVM plugin to generate cyber-resilient software at compile time.
- Protection of data and its manipulation from physical threats like side-channel attacks.
- Results will be demonstrated by using a smart sensor application with hardened embedded firmware and tamper-proof hardware platform.

OTHER PARTNERS

SOME CHALLENGES

- **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).
- **Compiler-based approach**
  - Design and development of LLVM passes to automate the protection process.
  - Target-independent protection (IR level).
  - Transparent for software programmers.

Example: unprotected program

```
uint8_t data_a = get_key_byte();
uint8_t data_b = get_key_byte();
uint8_t data_res = data_a ⊕ data_b;
```

Example: protection with boolean masking

```
uint8_t data_a, data_b, data_res ;
data_a = get_key_byte() ⊕ mask_a;
data_b = get_key_byte() ⊕ mask_b;
data_res = data_a ⊕ data_b ⊕ mask_res;
```

PACAP research themes : Compilation, Microarchitecture, Real-time systems, Performance, Reliability, Security

https://team.inria.fr/pacap/