General information

List, a CEA Tech Institute

Florent Kirchner (florent.kirchner@cea.fr) – Software Security

Alexis Olivereau (alexis.olivereau@cea.fr) – Network Security

Area of interest	Choose Y or N
○ Functional encryption and reduction of leakage (e.g., anonymization or obfuscation)	Y
○ Ultra-lightweight cryptology and ultra-high-speed cryptographic algorithms including quantum cryptography	
○ Physical cryptanalysis, including tampering, side channel, faults injection attacks, and security of tools for good software implementation and validation practices	
○ Authenticated encrypted token research for mobile payment solution	
○ Innovative cryptographic primitives and complementary non-cryptographic privacy-preserving mechanisms to enforce privacy	Y
○ New techniques, such as quantum safe cryptography, which are secure from quantum computers	Y
○ Quantum key distribution	
○ Automated proof techniques for cryptographic protocols	Y

Competencies

- *Organization competencies*
  - **RIA leadership and membership, CSA membership**
  - **active members of ENISA's NIS WG3, PPP Agenda, Allistene, ACN, IETF**
- *10+ years of European project experience:*
  - **OPEN TC (FP6): formal verification of Trusted Computing components**
  - **STANCE (FP7): formal code analysis for cybersecurity**
  - **RISC (H2020): models for the convergence of physical and cybersecurity**
  - **VESSEDIA (H2020): verification engineering for dynamic industrial systems**
  - **CHEKOFV (DARPA): gamifying and crowd-sourcing formal verification**
  - **TWISNet (FP7) , IoT-A (FP7), etc. : Lightweight network security for the IoT**
  - **and also eConfidential, OPEES, MBAT, IngoPCS, Anastasec, Aurochs, …**
- *What we can bring*
  - **Formal verification and validation techniques**
  - **Source and binary code analysis, Runtime monitoring**
  - **Applied to cryptographic primitives and middleware**
  - **As a refinement of higher-level verifications (e.g. Coq, Isabelle, Easycrypt)**
  - **Applied cryptographic primitives (ABE, proxy re-encryption, signcryption…)**
  - **Lightweight crypto-based security protocols (secure delegation, pre-computation…)**
  - **Quantum safe cryptography**
  - **Privacy-preserving approaches (anonymization, pseudonymity…)**

not mandatory slide

Project idea

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