SCCyPhy : Security and Cryptology for CyberPhysical systems

Team leaders : C. Castelluccia (INRIA), J. Clédière (CEA), Ph. Elbaz-Vincent (UJF), R. Leveugle (INP).

Goals :

☞ structuration of the cybersecurity community of Grenoble (increase national and international visibility). Around 10 labs and more than 40 members.

☞ Analysis, design and implementation of efficient and certified cryptographic components, security protocols and privacy components, in both hardware and software, for cyber-physical systems.

Achievements :

☞ New arithmetic FPGA implementations and new attack for ECC (PhD thesis of Cornelie and Pontié) and for homomorphic encryption (ReConfig 2015).

☞ New framework for the modelisation of attackers on Bloom filters with applications to privacy vulnerabilities in the "Safe Browsing" service of Google. This work has forced Google to recently modify the privacy policies in "Google Safe Browsing" (PhD thesis of Kumar, published in DSN 2015 and 2016).

☞ New technics for the analysis of non-deterministic random-bit generators (PhD thesis of Layat).

☞ A end-to-end methodology for the evaluation of code robustness in presence of fault injection.

Awards, new projects and beyond

- ☞ The project-team is part of the consortium ARAMIS , led by Atos Worldgrid, selected as a world-class R&D initiative by the French government programme called "Investments for the Future".
- ☞ We are part of the new Cybersecurity research axis from the IRT Nanoelec of the CEA.
- ☞ SCCyPhy was involved in the French RESSI ("Rendez-vous de la Recherche et de l'Enseignement en Sécurité des Systèmes d'Information") network of academics in cybersecurity and in charge of organizing the RESSI 2017 event.
- ☞ SCCyPhy is also present in the rising french Cybersecurity network of the CNRS, as well as in the Allistene ("Alliance des Sciences et Technologies du Numérique") network.
- ☞ The ITEA-2 project Diamonds (including members from SCCyPhy team) got EUREKA Innovation Award 2015/2016.
- ☞ Integration of the law and geopolitical experts on cyberspace which is currently unique in France, within the framework of AMNECYS (Alpine Multidisciplinary NEtwork on Cyber-security Studies) network which has a central role in the French Cybersecurity Initiative launched by the French Government in January 2017.
- ☞ The adventure continue : proposal to the UGA IDEX CDP call 2017...