Cybersecurity Institute
Univ. Grenoble Alpes

INSTITUT FOURIER

L I G

Internship: Reverse engineering of FPGA firmware in control systems devices

Reference	CYBERINSTITUTE-INT-20015
Description	The objective of this internship is to develop a methodology for the reverse engineering of bitstreams, programs and configurations of FPGAs used in the context of industrial systems. Cybersecurity of industrial systems (also called SCADA systems) is a hot topic in cybersecurity research. Recent publicly know attacks (Stuxnet, BlackEnergy, Industroyer/CrashOverride) showed that industrial systems are vulnerable, and the vulnerability exploitation may occur in important industrial and economical losses. Consequently, the research for vulnerabilities, intrusion detection and protection mechanisms became an important topic in the industrial and academic research. Probably the most critical mission in a SCADA system is the one of the Programmable Logic Controllers (PLC). The PLC implements the control logic of the local loop in order to guarantee that the control objectives are fulfilled and the safety of the system is insured. The first-generation PLCs were built using general purpose CPU (most of them based on Motorola 68k), followed by a second generation using customized CPU (often based on x86 architectures or PPC). The main issue with hard-coded CPUs is that if a bug is discovered in the processor design (like the Pentium FDIV bug), the hardware cannot be patched and reliability of the entire PLC and therefore SCADA system is compromised. Most of the top-level PLC of the last generation are now based on small re-programmable FPGAs and the CPU is implemented on the FPGA so that it can be patched if a vulnerability is revealed. Most of the FPGA programming files for PLCs currently on the market may be found on the manufacturer web site. During this internship funded by the Grenoble Alpes Cybersecurity Institute, we are interested in the development of a methodology in order to retrieve as much information as possible on the embedded CPU and peripheral devices configuration in order to be able to ultimately assess the security of the PLC and its communication protocol. This methodology will allow to reverse the compilation process from the bitstream to the netlist of a small Lattice FPGA. Context: The Grenoble Alpes Cybersecurity Institute – in short, Cyber@Alps – is a project selected in 2017 by the Cross-Disciplinary Program (CDP) of the IDEX Univ. Grenoble Alpes and aims at undertaking ground-breaking interdisciplinary research in order to address cybersecurity and privacy protection challenges. Our main technical focus are on cost effective secure elements, security of critical infrastructures all along their life cycle, vulnerability analysis and global challenges in terms of risk analysis and validation of large systems, including practical resilience across the industry and the society. Our approach to cybersecurity is holistic, encompassing technical, legal, law-enforcement, economic, social, diplomatic, military and intelligence-related aspects with strong partnerships with the private sector and robust national and international cooperation with leading institutions in France and abroad (https://cybersecurity.univ-grenoble-alpes.fr) **Bibliography** • Recent Advances in FPGA Reverse Engineering, *Yu et al, Electronics 2018, 7(10), 246; https://doi.org/10.3390/electronics7100246* • Project IceStorm, *http://www.clifford.at/icestorm/*
Prerequisites	Applicants must be enrolled in an electronics engineering degree. A previous experience in FPGA programming is mandatory. A background on embedded systems and VxWorks programming will be a plus.
Tutors	Romain Xu-Darme (Institut Fourier), Stéphane Mocanu (LIG)
Applications	Please send your resume, application letter with two recommendations (including education director), first year master's degree grades (mandatory) and second year grades (if possible) to cyberalps-contact@univ-grenoble-alpes.fr For more information on the internship, please contact romain.xu@univ-grenoble-alpes.fr
Location	Institut Fourier (100 rue des mathématiques, Gières)
Starting date	February-March 2020
Duration	5-6 months
Allowance	In accordance with existing regulations (approx. 560€/month). Part of travel expenses can be covered.

financed by
IDEX Université Grenoble Alpes