Univ. Grenoble Alpes
Université de l'innovation

PhD Position
Vulnerability search in Industrial Control Systems; a reverse engineering approach

SECTOR **:** Higher Education Institution

LOCATION: France, Grenoble

RESEARCHER PROFILE:
☐ *First stage researcher,*

INSTITUTION: Univ. Grenoble Alpes, University of Innovation

One of the major research-intensive French universities, Univ. Grenoble Alpes enjoys an international reputation in many scientific fields, as confirmed by international rankings. It benefits from the implementation of major European instruments (ESRF, ILL, EMBL, IRAM, EMFL*). The dynamic ecosystem, grounded on a close interaction between research, education and companies, has earned Grenoble to be ranked as the 5th most innovative city in the world. Surrounded by mountains, the campus benefits from a natural environment and a high quality of life and work environment. With 7000 foreign students and the annual visit of more than 8000 researchers from all over the world, Univ. Grenoble Alps is an internationally engaged university.

A personalized Welcome Center for international students, PhDs and researchers facilitates your arrival and installation.

In 2016, Univ. Grenoble Alpes was labeled «Initiative of Excellence ". This label aims at the emergence of around ten French world class research universities. By joining Univ. Grenoble Alpes, you have the opportunity to conduct world-class research, and to contribute to the social and economic challenges of the 21st century ("sustainable planet and society", "health, well-being and technology", "understanding and supporting innovation: culture, technology, organizations" "Digital technology").

* ESRF (European Synchrotron Radiation Facility), ILL (Institut Laue-Langevin), IRAM (International Institute for Radio Astronomy), EMBL (European Molecular Biology Laboratory), EMFL (European Magnetic Field Laboratory)

Key figures:

- + 50,000 students including 7,000 international students
- 3,700 PhD students, 45% international
- 5,500 faculty members
- 180 different nationalities
- 1st city in France where it feels good to study and 5th city where it feels good to work
- ISSO: International Students & Scholars Office affiliated to EURAXESS

Univ. Grenoble Alpes
Université de l'innovation

REFERENCES:

CDP-Idex Project: Grenoble Alpes Cybersecurity Institute
SUBJECT TITLE: Vulnerability search in Industrial Control Systems; a reverse engineering approach
RESEARCH FIELD: Computer science/Informatique
SCIENTIFIC DEPARTMENT (LABORATORY'S NAME): Laboratoire d'Informatique de Grenoble et Verimag
DOCTORAL SCHOOL'S: MSTII
SUPERVISOR'S NAME*:* Stéphane Mocanu/ Laurent Mounier

SUBJECT DESCRIPTION :

Industrial control systems are specialized computer systems used in many activities of vital importance like energy production and distribution, chemical industry or water management.

These systems consist in dedicated hardware and software (Programmable Logic Devices, Control Systems, Human Machine Interface) interacting via field-bus communications. Their components and communication protocols are often based on legacy and out-of-date hardware and software, not always in conformity with modern security standards and updates.
Thus, they might include vulnerabilities which may be used by attackers with potentially serious consequences. Vulnerability research and analysis are then a major concern for governmental agencies (ANSSI), component providers, and end-users.
The topic of this PhD lays in this field, dealing with vulnerability detection in industrial systems. Due to the unavailability of both the complete specifications and the source code of the software components, we propose a reverse engineering approach for vulnerability detection. This approach may target several layers like:
- Behavioral inference of the control automata of a PLC via active learning (observing the input/output dependences), considering first autonomous automata and then studying the extension to timed and/or hybrid automata;
- Code analysis of the embedded PLC software, namely the operation blocks and/or the communication layer implementations, combining static and dynamic analysis of binary code and execution traces. The main objective is to discover abnormal or unexpected behaviors that may be exploited by an attacker to modify or disrupt the physical process.
This study will be hosted by research teams CTRL-A (LIG department) and PACS (Verimag department), which hold strong knowledge in industrial systems analysis, reverse engineering and code analysis techniques.

References:
[1] Franck de Goër, Christopher Ferreira, Laurent Mounier. SCAT: Learning from a single execution of a binary. SANER 2017, Klagenfurt, Austria, February 2017.
[2] Franck de Goër, Roland Groz, Laurent Mounier. Lightweight heuristics to retrieve parameter associations from binaries. PPREW@ACSAC Workshop, Los Angeles, USA, December 2015.
[3] Muzammil Shahbaz, Roland Groz. Analysis and testing of black-box component-based systems by inferring partial models. Software Testing, Verifification and Reliability, volume 24, number 4, 2014
[4] Oualid Koucham, Stéphane Mocanu, Guillaume Hiet, Jean-Marc Thiriet, Frédéric Majorczyk. Efficient Mining of Temporal Safety Properties for Intrusion Detection in Industrial Control Systems. accepted to 10th IFAC Symposium on Fault Detection, Supervision and Safety of Technical Processes (SafeProcess 2018), Warsaw, Poland
[5] Oualid Koucham, Stéphane Mocanu, Guillaume Hiet, Jean-Marc Thiriet, Frédéric Majorczyk. Detecting Process-Aware Attacks in Sequential Control Systems. 21st Nordic Conference on Secure IT Systems (NordSec 2016), Nov 2016, Oulu, Finland. <http://nordsec.oulu.fi>.
[6] Maëlle Kabir-Querrec, Stéphane Mocanu, Jean-Marc Thiriet, Eric Savary. A Test bed dedicated to the Study of Vulnerabilities in IEC 61850 Power Utility Automation Networks. 21st IEEE Emerging Technologies and Factory Automation, Sep 2016, Berlin, Germany. Proceedings of IEEE 21th Conference on Emerging Technologies & Factory Automation (ETFA 2016), Berlin, Germany, September 2016, 2016, <http://www.etfa2016.org/index.php>.

[7] Maëlle Kabir-Querrec, Stéphane Mocanu, Pascal Bellemain, Jean-Marc Thiriet, Eric Savary. Corrupted GOOSE Detectors: Anomaly Detection in Power Utility Real-Time Ethernet Communications. GreHack 2015, Nov 2015, Grenoble, France. <hal-01237725>

ELIGIBILITY CRITERIA

Applicants must hold a Master's degree (or be about to earn one) or have a university degree equivalent to a European Master's (5-year duration).

Applicants will have to send an application letter in English and attach:
- Their last diploma
- Their CV
- A short presentation of their scientific project (2 to 3 pages max)
- Letters of recommendation are welcome.

Address to send their application: cyberalps-pilotage@univ-grenoble-alpes.fr, laurent.mounier@univ-grenoble-alpes.fr, stephane.mocanu@imag.fr

SELECTION PROCESS

Application deadline: June 30, 2018 at 17:00 (CET)

Applications will be evaluated through a three-step process:
1. Eligibility check of applications in first July 2nd 2018
2. 1st round of selection: the applications will be evaluated by a Review Board in July 5th 2018. Results will be given in July 6th 2018.
3. 2nd round of selection: shortlisted candidates will be invited for an interview session in Grenoble on July 12, 2018. (if necessary)

TYPE of CONTRACT: temporary-3 years of doctoral contract
JOB STATUS: Full time
HOURS PER WEEK: 35
OFFER STARTING DATE: June 5th 2018
APPLICATION DEADLINE: June 30, 2018
Salary: between 1768.55 € and 2100 € brut per month (depending on complementary activity or not)