PhD Position
Risk analysis and intrusion detection for critical infrastructure cyber security

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
MANDATORY REFERENCES:

CDP-Idex Project: Cybersecurity Institute
SUBJECT TITLE: Risk analysis and intrusion detection for critical infrastructure cyber security
RESEARCH FIELD: Computer science, Engineering
SCIENTIFIC DEPARTMENT (LABORATORY’S NAME): G-SCOP
DOCTORAL SCHOOL’S: EEATS
SUPERVISOR’S NAME: JM Flaus, R Groz, ML Potet

SUBJECT DESCRIPTION:

Nowadays, most of the control systems and many embedded systems are networked, local, or even the internet. In all cases, they are relatively easily accessible malware that would seek to take control to perform dangerous or obstructive actions for facilities. These systems have risks associated with their IT vulnerability. To reduce these several lines of action are possible. The first is to secure data exchange using a secure protocol. However, if malware manages to cross this level of protection, which is not to be excluded given its sensitivity to human error, the control system is fully accessible. This problem is encountered especially for sensor-driven systems for distances, as in the case of remote maintenance (rail, autonomous automatic systems ...) or remote readings (electricity, pollution ...).

The objective of this work is to use different sources of information to conduct a monitoring of ICS. The idea is to rely on different types of models that will be built specifically obtained or the other phases of the engineering project that will include:
1) The physical process model and the control system,
2) The model of network traffic, which can be obtained by machine learning,
3) The models of sequences contained in event logs of different equipment, which can be obtained by machine learning
4) The model from the risk analysis of the installation.

The first step is to propose a formality appropriate to represent each of the different models
Secondly, we will consider the design of an approach to detect attacks at the earliest and to separate defects from failures of the process, by combining information from different models, relying on diagnostic approaches and prognosis.
Next we look at how we can build these models automatically and if it is necessary to have expert knowledge (eg influence graphs, emergency patterns of behavior ...).
Finally, we will focus on the question of whether the models and patterns can help to attribute the authorship of the attacks or rank relative to existing approaches

References


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, jean-marie.flaus@univ-grenoble.fr, roland.groz@univ-grenoble-alpes.fr, Marie-Laure.Potet@univ-grenoble-alpes.fr

SELECTION PROCESS
Application deadline: June 28, 2018 at 17:00 (CET)
Applications will be evaluated through a three-step process:

1. Eligibility check of applications in June 29, 2018
2. 1st round of selection: the applications will be evaluated by a Review Board in Jule, 2018. Results will be given in July, 2018.
3. 2nd round of selection: shortlisted candidates will be invited for an interview session in Grenoble on July 5, 2018. (if necessary)

TYPE of CONTRACT: temporary-3 years of doctoral contract
JOB STATUS: Full time
HOURS PER WEEK: 35
OFFER STARTING DATE: October 2018
APPLICATION DEADLINE: June 28, 2018
Salary: between 1768.55 € and 2100 € brut per month (depending on complementary activity or not)