Intrusion detection for continuous state industrial control systems

Guillaume Hiet (guillaume.hiet@centralesupelec.fr) CentraleSupélec / IRISA Team CIDRE

Frédéric Majorczyk (frederic.majorczyk@irisa.fr) DGA-MI / IRISA Team CIDRE

Stephane Mocanu (Stephane.Mocanu@imag.fr) Inria / LIG Team CTRL-A

Industrial Control Systems (ICS) cybersecurity is an important issue not only for manufacturers and industrial users but also for governments. Indeed, if the critical mission of some control systems is compromised (nuclear plants or chemical facilities) the impacts on people and environment may be very severe and affect an entire country. Last decade cyberattacks (Stuxnet, BlackEnergy, CrashOverride) showed that cyberattacks on industrial facilities are real and the physical plant may be impacted.

A specialized class of attacks are these aimed to compromise the critical mission, i.e. the control of the physical process. Such attacks are called process-oriented attacks in the literacy. As they are specifically targeting the physical process, they may not be detected only by searching patterns in the network traffic. Detection of such attacks needs the use of cyber-physical models which include the state of the physical process (i.e. values of sensors and actuators).

The topic of this internship concerns process-oriented intrusion detection approaches that operate over the state of sensors and actuators in order to detect the physical domain manifestations of the attacks. A first approach for discrete state systems was developed in [1] using a runtime monitoring approach. The detection systems monitor a set of safety properties declared in LTL [2] and MTL [3] formalisms. The aim of the proposed work is to enlarge the previous study and consider the case of continuous state systems. We wish to relay on a similar monitoring approach. The expected results are: a comparative state of art of available formalisms for continuous cyber-physical systems, an evaluation of the adequacy of various models with the monitoring [4] and modelling of safety properties [5], development of a model using a chosen formalism and test on an ICS system.

References

[1] Oualid Koucham. Intrusion detection for industrial control systems. Automatic. Université Grenoble Alpes, 2018. English. ⟨NNT : 2018GREAT090⟩. ⟨tel-02108208⟩

[2] Amir Pnueli. The temporal logic of programs. InProc. SFCS'77, pages 46–57, Washington, DC, USA, 1977. IEEE Computer Society.

[3] David Basin, Felix Klaedtke, and Eugen Zălinescu. Algorithms for monitoring real-time properties. Acta Informatica, 55(4):309–338, Jun 2018.

[4] Andreas Bauer. Monitorability of omega-regular languages. CoRR, abs/1006.3638,2010

[5] M. B. Dwyer, G. S. Avrunin, and J. C. Corbett. Patterns in property specifications for finite-state verification. InProc. ICSE’99, 1999.