Security Challenges in Cyber-Physical Systems

Francesco Regazzoni

ALaRI – USI, Switzerland, email: regazzoni@alari.ch

Cyber-Physical Systems (CPSs) tightly integrate cyber components (typically computation and communication elements) with physical components, such as sensors and actuators. These systems are often used in safety-critical applications, such as autonomous driving or medical devices, and are often used to manage and control our critical infrastructure, including smart grids and transportation systems. CPSs used in these application must withstand error and failures. These failures can be "natural" or caused by environmental conditions, but they can even be the outcome of a deliberated attack to the system. The capability of attackers have been demonstrated in different scenarios, including manipulation of industrial implant [1, 2] or hacking cars [3].

As embedded systems, CPSs are vulnerable to the cyber-attacks such as malware injection and to physical attacks such as power analysis and fault injection attacks. However, the presence of a physical component opens novel possibilities to adversaries. Side channels, for instance, can be used to extract design files from 3D printers while fabricating objects [4] and manipulations of the design tools can be used to increase the leak of information [5] or to alter the quality of a product.

Counteracting these threats is of utmost importance for the safe deployment of the applications relying on CPSs, including autonomous driving and industry 4.0. If on the one side there is a solid knowledge regarding cyber-attacks and physical attacks targeting the cyber part of a CPS, very little is know about attacks targeting the physical part and the possible countermeasures. Addressing this issue, this talk summarizes the main security and reliability challenges specific to CPS, discussing the main threats, the most relevant approaches to counteract them, and highlighting novel research directions.

References

1. R. Langner, "Stuxnet: Dissecting a cyberwarfare weapon," *IEEE Security & Privacy*, vol. 9, no. 3, pp. 49–51, 2011.
2. BBC News, "Hack attack causes 'massive damage' at steel works," 2014, http://www.bbc.com/news/technology-30575104.
3. C. Miller and C. Valasek, "Remote exploitation of an unaltered passenger vehicle," in *Black Hat USA*, 2015.
4. A. M. Al Faruque, S. R. Chhetri, A. Canedo, and J. Wan, "Acoustic side-channel attacks on additive manufacturing systems," in *Proceedings of the 7th International Conference on Cyber-Physical Systems*. IEEE Press, 2016, p. 19.
5. S. R. Chhetri, A. Barua, S. Faezi, F. Regazzoni, A. Canedo, and A. M. Al Faruque, "Tool of spies: Leaking your ip by altering the 3d printer compiler," in *IEEE Transactions on Dependable and Secure Computing*, 2019.