A Novel, Comprehensible, Ultra-Fast, Security-Aware CPS Simulator (COSSIM)

Nowadays, **Cyber Physical Systems** (CPS) are growing in capability at an extraordinary rate, promoted by the increased presence and capabilities of electronic control units as well as of the sensors and actuators and the interconnecting networks. One of the main problems CPS designers face is **the lack of simulation tools and models for system design and analysis**. This is mainly because the majority of the existing simulation tools for complex CPS handle efficiently only parts of a system (e.g. only the processing or only the network) while none of them support the notion of security. Moreover, the existing simulators need extreme amounts of processing resources and computation time to simulate a system at a low level (e.g. including the Operating System in a target platform at a close to cycle accurate level). Faster approaches are available however they function at higher levels of abstraction and cannot provide the necessary precision and accuracy.

The "*Novel, Comprehensible, Ultra-Fast, Security-Aware CPS Simulator*" (COSSIM) tool is an open-source framework that:

- Seamlessly simulates, in an integrated way, the networking and the processing parts of the CPS.
- Provides significantly more accurate results, especially in terms of power consumption, than existing solutions.
- Reports the, critical for many applications, security levels of the simulated CPS.

The novel COSSIM framework combines a state-of-the-art processing simulator (i.e. a "full-system simulator") with an established network simulator. These tools are integrated with high-level power estimators and the overall framework provides appropriate interfaces to security testing tools.

More specifically, the GEM5[1] simulator is utilized as the basis for the processing simulation sub-system; the presented sub-system can efficiently simulate different CPS processing units spanning from simple μ-controllers to **multi-core CPUs** (e.g. multi-core ARMs or x86-based) with **several levels of memory hierarchy** and complex peripherals (such as network cards, accelerators). The processing sub-system provides cycle-accurate simulation and supports simulation of full unix-based OSs and applications.

In the scope of CPS environments, where multiple heterogeneous nodes communicate with each other, the COSSIM framework uses one instance of the processing sub-system to model each node and binds all nodes together through a network simulator. For this reason the OMNET++[2] network simulation tool is used as the basis for the network simulation sub-system. Moreover, the MiXiM extension of OMNET++ is also utilized so as to provide realistic wireless simulations.

Additionally, the MacPat open-source tool and the MiXiM tool are providing accurate power consumption estimations for processing and network sub-systems respectively, while the COSSIM framework incorporates **Fuzz testing** & **DoS detection** components so as to allow for simulation of the security features of a CPS.

Bringing the processing and the network simulators together requires carefully designed communication interfaces and synchronization schemes. For this reason the IEEE High Level Architecture (HLA) standard and specifically the **CERTI**[3] HLA implementation is used to interconnect the processing and networking simulation sub-systems. Furthermore, HLA can extend the capabilities of the COSSIM framework by providing means to connect it to other established CPS simulation tools (such as Ptolemy II) that can model and simulate the physical processes of the CPSs.

Summarizing, **COSSIM is the first known simulation framework** that allows for the simulation of a **complete CPS** utilizing complex SoCs interconnected with sophisticated networks. Finally, the COSSIM system supports accurate power estimations while it is the first such tool supporting security as a feature of the design process.

---

[1] http://www.m5sim.org/

[2] https://omnetpp.org/

[3] http://savannah.nongnu.org/projects/certi