Identification of Cyber Physical System (CPS)

&

Orchestration of fuzzing testing

Guillaume Nguyen

Researcher at the Computer Sciences Faculty - University of Namur

- Double master degree in business engineering.
- 4 years experience in Cyber Security (IT governance).
- Joined Cyber Excellence in September 2022.
- Under the supervision of Xavier Devroey and Jean-Noël Colin.

Research direction

How, when, and what to test using which fuzzing tool/technique?

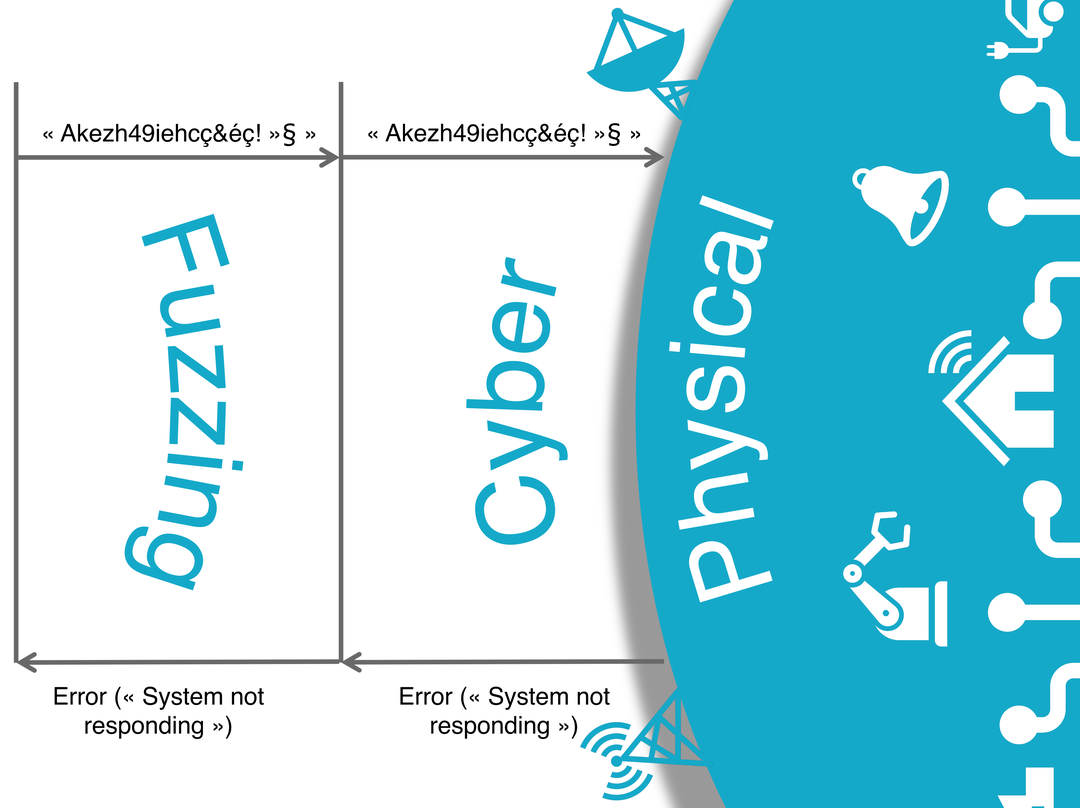
- **The capabilities of those machines in the real world should be under control.**
- CPS comprises of various technologies and are hard to test entirely.
- The concept of CPS is very close to IoT.
- Fuzzing allows for a wide coverage of possible test cases.

1 Defining and Classifying CPS

- There are many definitions of CPS.
- Mostly, those systems get information from the physical world and have the ability to affect it in return.
- Before going further and suggesting a classification scheme for this type of system we need to chose the most fitting definition.

2 Testing the tests

- There is a commonly used test set for “fuzzers” or fuzzing tools.
- We need to determine how much it covers the test cases for CPSs based on the (newly found) classification.



3 Unfuzzing fuzzers

- There are many fuzzers.
- However, they mainly focus on the same types of tests (using CLI).
- We will identify the missing ones for a more holistic testing of CPS.

4 It’s been a long way

- Compile the thesis.
- Develop a fuzzer missing from the CPS testing toolbox.

UNIVERSITÉ DE NAMUR