An Instruction Set Randomization Framework for Developing Secure and Resilient CPS

Bradley Potteiger, Zhenkai Zhang, Xenofon Koutsoukos
Vanderbilt University

A number of successful attacks against cyber-physical systems have demonstrated that security and resilience of CPS is a critical problem and new methods and techniques are required to build high confidence systems. Among these attacks, code injection attacks are cited as a common attack vector taking advantage of software input processing vulnerabilities in order to run malicious code in a control process. Instruction set randomization is a very effective technique to mitigate against code injection attacks, randomizing the instruction set architecture of machine code for the purpose of making originally valid injected attack code invalid and un-executable. When the injected attack code is executed, the cpu will recognize the invalid instructions and the process will crash. However, system crashing is unacceptable in safety critical systems and continuous, reliable functionality has to be maintained. This poster illustrates a runtime framework that utilizes ISR techniques to mitigate against code injection attacks as well as integrating a control manager process to prevent the possibility of system crashing by reliably switching to a safe controller alternative. A traffic case study scenario is utilized to demonstrate the implementation of our control framework.