Foundations of Secure Cyber-Physical Systems of Systems: Firmware Rehosting via Synthetic Hardware

Stephen Checkoway (Oberlin), Kirill Levchenko (Illinois), Stefan Savage, Alex Snoeren, Ranjit Jhala (UC San Diego)
https://aerosec.org

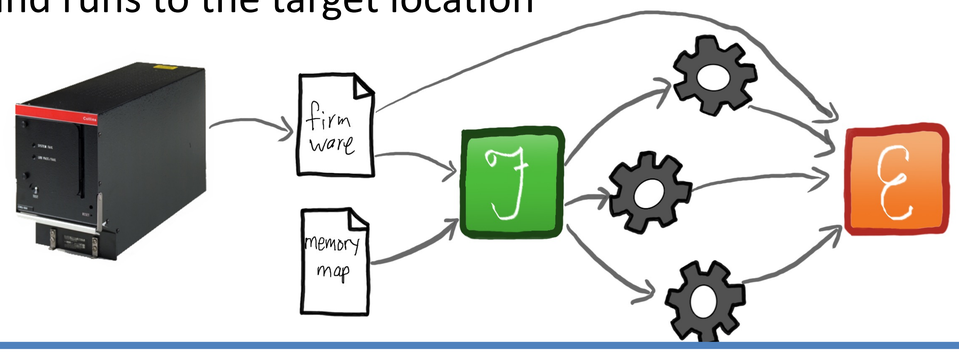
Motivating Question: How can we dynamically analyze firmware for cyber-physical systems?

Key Challenges

- Special-purpose/nonstandard hardware
  - Custom or unusual internal peripherals (either as part of a SoC or on the motherboard); e.g., ARINC-429 transceivers in avionics
- Standard emulation tools designed for desktop/mobile
  - Tools assume standard PC peripherals like timers and serial ports
- Firmware's boot routines initialize peripherals and wait for the them to return appropriate statuses
  - Emulation can't respond appropriately, so execution does not reach the code of interest

Our solution: Jetset (USENIX Security 2021)

- Use symbolic execution to learn peripheral interactions
  - Modify angr to use Tabu search to drive execution to analyst-chosen target location using novel path-sensitive distance function
- Concretize constraints learned during symbolic execution into device models (we call this *synthetic hardware*)
- Run firmware in emulator using device models
- Firmware boots and runs to the target location
- Perform analyses on code running in an emulator



Scientific Impact

- Jetset's cross-architecture approach supports multiple CPS domains including aviation and power systems
- Jetset enables security analyses
  - E.g., fuzzing found vulnerabilities in avionics firmware

Broader Impact

- Open source tools
  - Jetset tool
  - Avionics testbed tools
- Technology and knowledge transfer to MITRE, DHS, PNNL, and LLNL
- Boeing Industry Cyber Technical Council
- Vulnerability disclosure to Collins Aerospace and Boeing
- Undergraduate CPS research

2021 NSF Cyber-Physical Systems Principal Investigators' Meeting
June 2-4, 2021

Award ID#: CNS-1901728, CNS-1646493