Foundations of Secure Cyber-Physical Systems of Systems

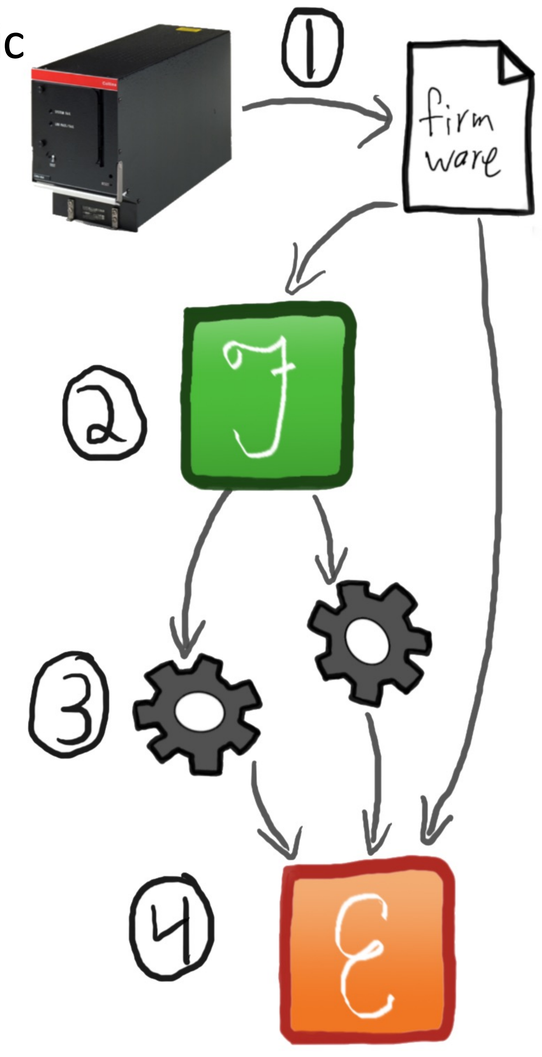
Stephen Checkoway (Oberlin College); Kirill Levchenko (University of Illinois)
Stefan Savage, Alex Snoeren, Ranjit Jhala (UC San Diego)

Challenge:

- How can we perform dynamic analyses of CPS firmware?
- Nonstandard/unknown embedded peripherals complicates firmware rehosting

Solution:

- Symbolic execution to learn peripheral interaction constraints
- Synthesize *synthetic hardware* device models
- Rehost firmware in emulator



1. Extract firmware
2. Run Jetset which
3. Outputs device models
4. Emulate firmware

Scientific Impact:

- Enables security analyses of cyber-physical systems
- Cross-architecture approach supports multiple CPS domains

Broader Impact:

- Open source tools
  - –Jetset rehosting tool
  - –Avionics testbed tools
- Tech transfer to MITRE, DHS, PNNL, LLNL
- Boeing Industry Cyber Technical Council
- Disclosure to Collins, Boeing
- Undergraduate CPS research

CNS-1901728, CNS-1646493
Start date: October 1, 2016