SAND2018-1585C

Containerized Application Security (CAPSec) for Industrial Control Systems (ICS)

Adrian R. Chavez, Ph.D.

Sandia National Laboratories

February 20, 2017

CAPSec Motivation

- Lockheed Martin Cyber Kill Chain
  - Gain reconnaissance information
  - Develop exploit
  - Deliver exploit
  - Launch exploit
  - Install malware
  - Command & control
  - Persist and perform actions
- BlackEnergy, Shamoon 2, Stuxnet, …

CAPSec Goals

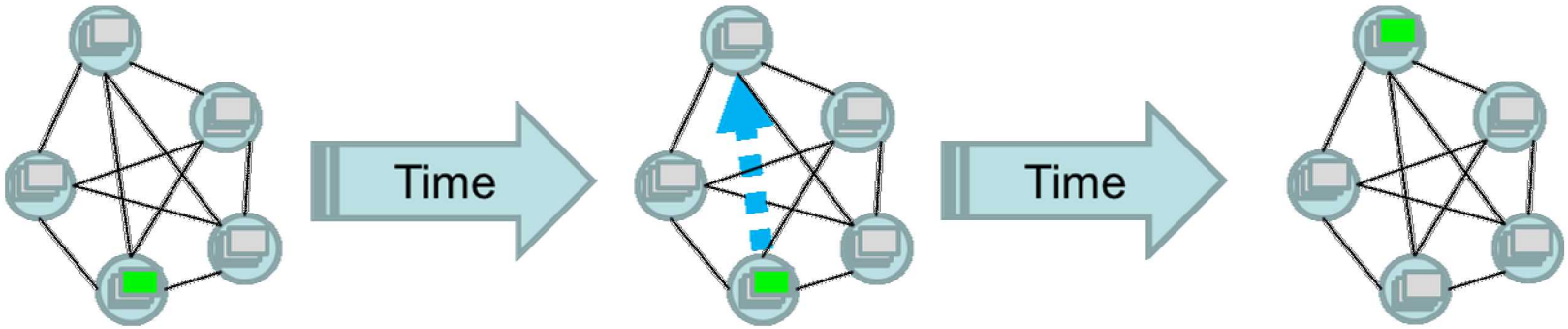
- Minimize downtime when upgrading/patching software in OT environments
- Improve resiliency of applications during a cyber event
  - Detect and recover from cyber threats
- Isolate and reduce impacts of potential compromise
  - Prevent and limit lateral movements

Project Scope

- DOE Cybersecurity for Energy Delivery Systems
- Timeline: March, 2018 – February, 2021
- Phase 1: R&D proof-of-concept
  - Application migration
  - Application live-upgrade
  - Independent 3rd party red team assessment
- Phase 2: Test & Evaluate proof-of-concept
  - Apply within industry partner testbeds
  - Capture and document performance metrics

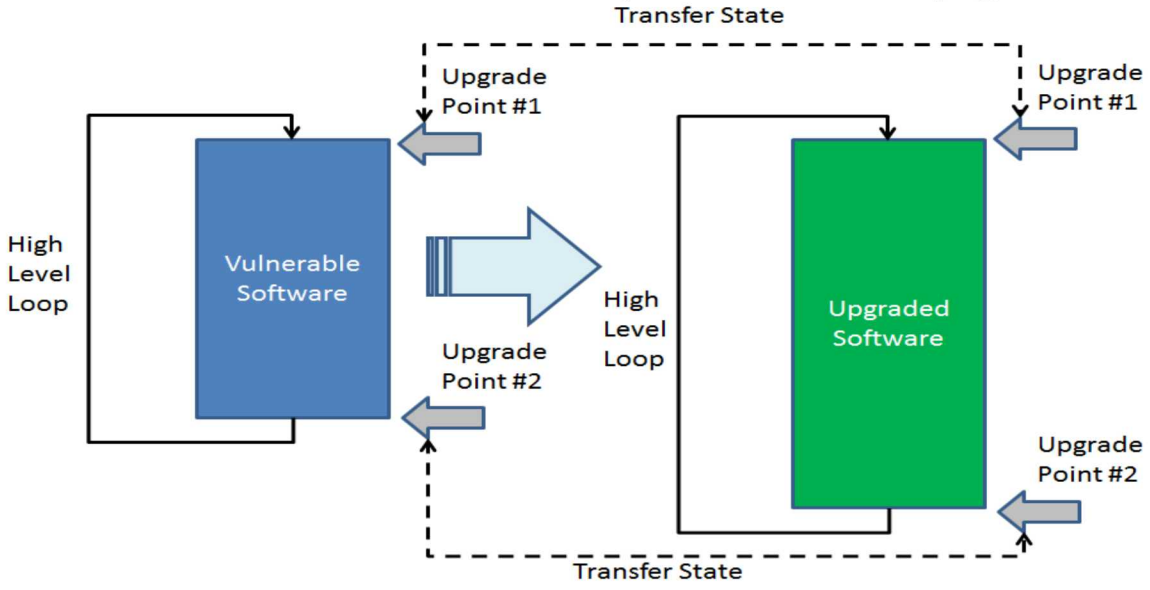
Application Live-Migration

- Migrate containers periodically or as needed
  - Leverage container orchestration for live migration
  - Checkpoint and transfer application state
  - Apply fault tolerant algorithms (Byzantine/crash) towards ICS applications



Live-Upgrade Applications

- Upgrade software in real-time to maintain high availability when patching/upgrading
  - Identify upgrade points
  - Transition software to patched/upgraded version



Available Container Solutions

- Container solutions
  - Docker
  - Linux LXC
  - FreeBSD jails
- Orchestration solutions
  - Docker Swarms
  - Kubernetes
  - Apache Mesos Marathon

Project Partners

- Vendor partner to guide/transition R&D
  - Schweitzer Engineering Laboratories
- Industry partners for testing and evaluation
  - Fort Belvoir Night Vision & Electronic Sensors Directorate
  - Sempra Energy
  - Chevron Corporation

Project Partners (Cont.)

- Laboratory Partner
  - Pacific Northwest National Laboratory
- Independent 3rd Party Red Team
  - Grimm (SMFS, Inc.)

Next Steps

- Identify applications to isolate within a contained environment
  - Ladder logic
  - Historian applications
  - HMI applications
- Leverage open source and commercially available OT technologies
  - libmodbus / opendnp3, SoftPLC
- Seeking additional collaboration

Questions?

Adrian R. Chavez

adrchav@sandia.gov

Sandia National Laboratories