Scalable Hybrid Attack Graph Modeling and Analysis

John Hale and Peter Hawrylak, Institute for Information Security, The University of Tulsa
isec.utulsa.edu/HAG

How can we conduct effective security analysis on cyber physical systems?

Objective: Develop techniques and solutions for practical formal analysis of security properties in *cyber physical systems (CPSs)*

Challenges: CPSs are hybrid systems that exhibit behavior in the *discrete* and *continuous* domains, confounding conventional computational approaches to modeling and analysis

- Modeling: Acquisition and representation can be costly, incomplete, and *ad hoc*

- Analysis: Generation and processing are compute intensive

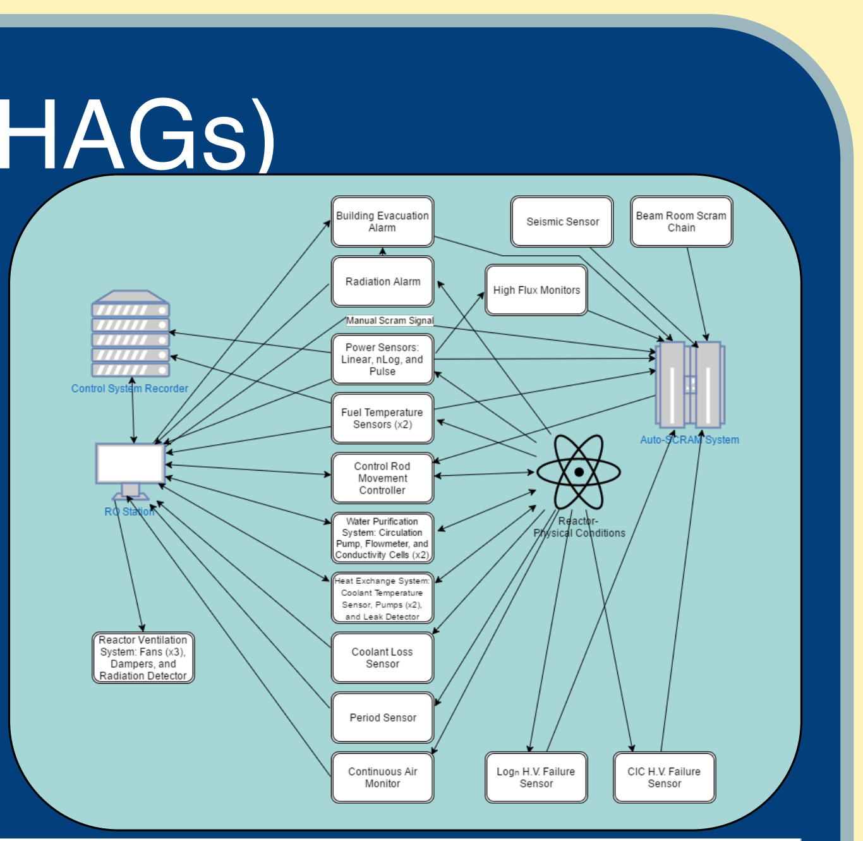
WANTED: A CPS Security Test Bed
- Match theory with simulation with experimentation
- Train students on CPS security issues and techniques

IN DEVELOPMENT: Competitive learning and experimentation arena for CPS security

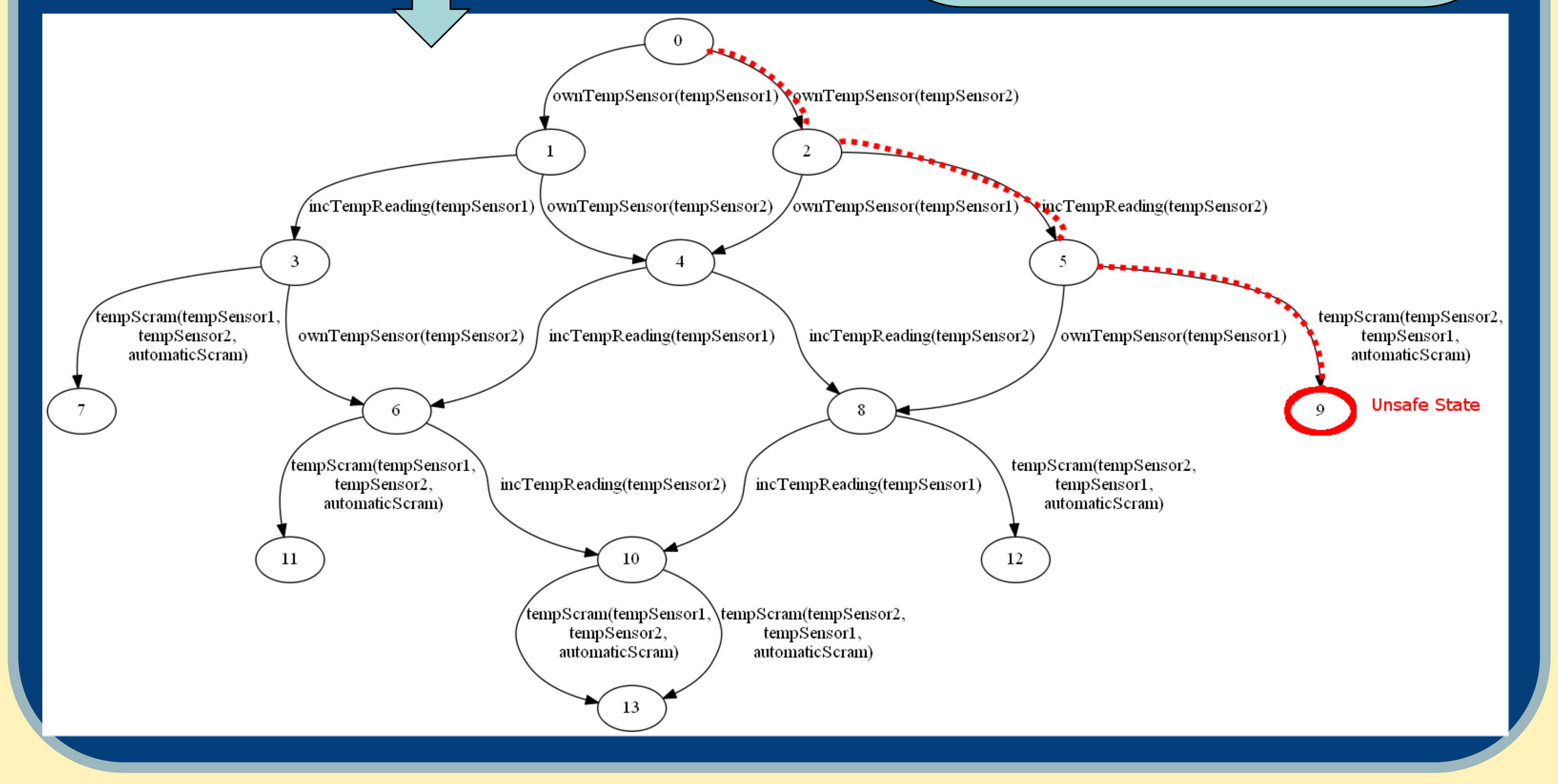
Hybrid Attack Graphs (HAGs)

CPS – Industrial Control System (ICS) for Nuclear Research Reactor (NRR)

CPS Model


Building Evacuation Alarm
Seismic Sensor
Beam Room Scram Chain
Radiation Alarm
High Flux Monitors
Manual Scram Signal
Control System Recorder
Power Sensors: Linear, nLog, and Pulse
Fuel Temperature Sensors (x2)
Auto-SCRAM System
Control Rod Movement Controller
RO Station
Water Purification System: Circulation Pump, Flowmeter, and Conductivity Cells (x2)
Reactor-Physical Conditions
Heat Exchange System: Coolant Temperature Sensor, Pumps (x2), and Leak Detector
Reactor Ventilation System: Fans (x3), Dampers, and Radiation Detector
Coolant Loss Sensor
Period Sensor
Continuous Air Monitor
Logn H.V. Failure Sensor
CIC H.V. Failure Sensor

HAG


0
ownTempSensor(tempSensor1)
ownTempSensor(tempSensor2)
1
2
incTempReading(tempSensor1)
ownTempSensor(tempSensor2)
ownTempSensor(tempSensor1)
incTempReading(tempSensor2)
3
4
5
tempScram(tempSensor1, tempSensor2, automaticScram)
ownTempSensor(tempSensor2)
incTempReading(tempSensor1)
incTempReading(tempSensor2)
ownTempSensor(tempSensor1)
tempScram(tempSensor2, tempSensor1, automaticScram)
7
6
8
9
Unsafe State
tempScram(tempSensor1, tempSensor2, automaticScram)
incTempReading(tempSensor2)
incTempReading(tempSensor1)
tempScram(tempSensor2, tempSensor1, automaticScram)
11
10
12
tempScram(tempSensor1, tempSensor2, automaticScram)
tempScram(tempSensor2, tempSensor1, automaticScram)
13

Approach

Hybrid Attack Graphs

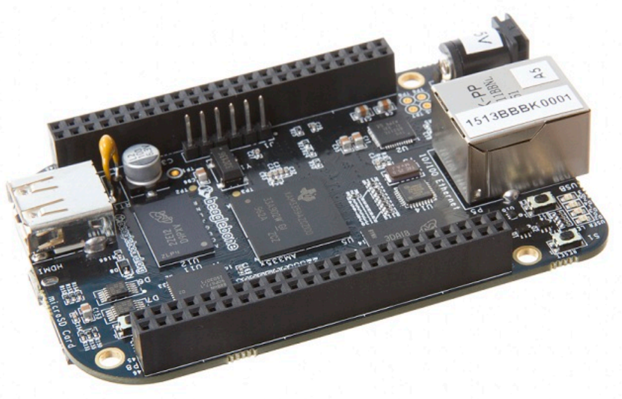
- •Extend conventional attack graphs to include continuous domain behaviors
- •HAG Generation and analysis – intelligent heuristics and exploit inherent parallelism

Key Enablers

- • High performance computing for HAG generation and analysis
- •Low cost point of presence network scanning platforms for distributed CPS model acquisition

Network Modeling with PINDAQ

Practical Information Network Data Acquisition
- Distributed model acquisition solution
- Low cost Beaglebone platform
- Active network mapping (Nmap)
- Translation to HAG modeling substrate



Hybrid Attack Graph Generation

Serial / parallel generation algorithms

Parallel implementation in OpenMPI

Reference model – ICS for Nuclear research reactor control

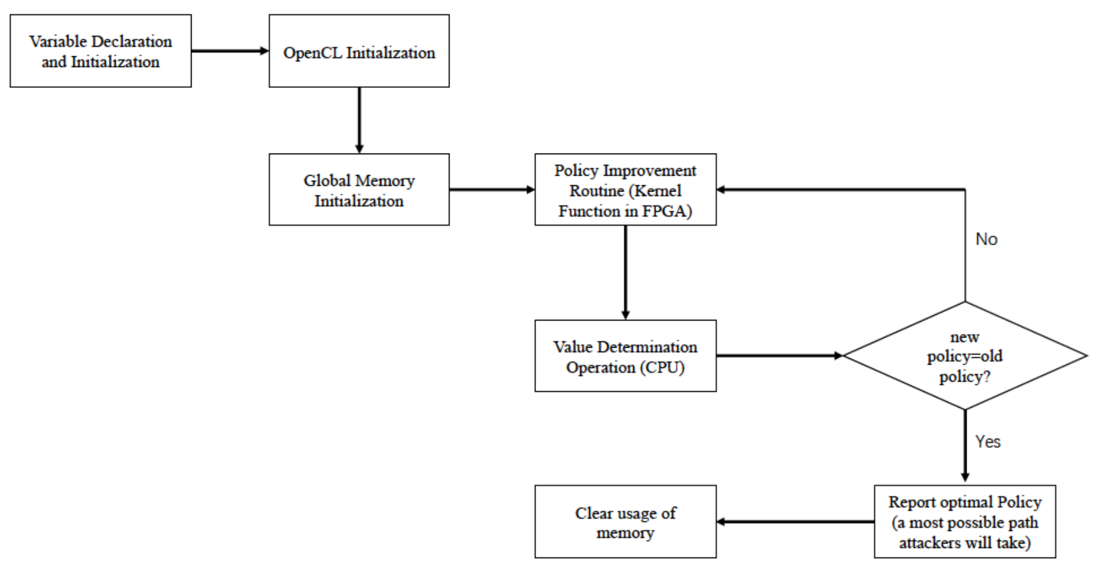
Deployed on heterogeneous compute node cluster (performance testing underway)

Hybrid Attack Graph Analysis

Markov Decision Processes
- Convert HAGs into MDPs
- Reward analysis

-Policy/value iteration

-FPGA implementation

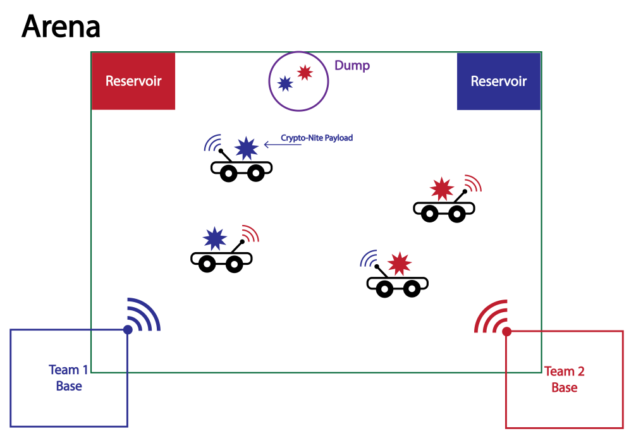

Variable Declaration and Initialization
OpenCL Initialization
Global Memory Initialization
Policy Improvement Routine (Kernel Function in FPGA)
No
Value Determination Operation (CPU)
new policy=old policy?
Yes
Clear usage of memory
Report optimal Policy (a most possible path attackers will take)

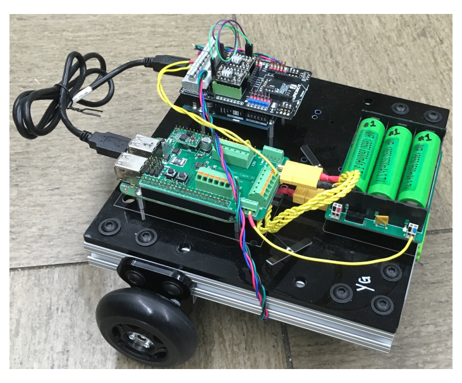
CPS Security Test Bed

Networked robotic vehicles play capture the flag

Hackable tech – CAN, Bluetooth, Wifi, NFC, Linux, Windows

Blended attacks– combine exposures in discrete and continuous domains





Interested in meeting the PIs? Attach post-it note below!

The 3rd NSF Secure and Trustworthy Cyberspace Principal Investigator Meeting
January 9-11, 2017
Arlington, Virginia

National Science Foundation
WHERE DISCOVERIES BEGIN

THE UNIVERSITY of TULSA