ARTINALI:
Dynamic Invariant Detection for Cyber-Physical System Security

Maryam Raiyat Aliabadi, Amita Kamath, Julien Gascon-Samson, Karthik Pattabiraman
Cyber-Physical Systems

Distributed Controllers

Network

Physical Process

Sensors

Actuators
Motivation
CPS Security Requirements

Goal:
Design an **Automated, Real-time** and **Attack-neutral** security solution for CPSes with respect to their **resource constraints**

- Real-time constraints
  - Zero-day attacks
  - No human-in-the-loop

- Resource constraints
Threat Model

Cyber Process (Control Algorithm)

Communication network

Physical Process

A → Measurements
Stuxnet[2010]

B
[USENIX’2015]

C
[HealthCom2013]

D
CVE-2016-1516[2016]

A → C → D

DENIED

DENIED
Previous work

• Intrusion Detection System (IDS)
  – Signature-based IDSs [CSUR2014]
  – Anomaly-based IDSs [Computers&Security2009]
  – Specification-based IDSs [SmarGridCom2010]
    • Static analysis ❌
    • Dynamic analysis ✓
Dynamic Analysis-based Techniques (Invariant-based)

- Invariant
  - Energy usage $\geq 0$

Diagram:
- Daikon [ICSE’01]
- Gk-tail [ICSE’08]
- Texada [ASE’15]
- Perfume property miner [ASE’14]
Main Idea: Break down the search space

D: Data
E: Event
T: Time
Methodology

- **ARTINALI**: A Real Time-specific Invariant Inference Algorithm
  - 3 dimensions and 6 classes of invariants
CPS platforms

• Advanced metering infrastructure (AMI)
  – SEGMeter
    • http://smartenergygroups.com

• Smart Artificial Pancreas (SAP)
  – OpenAPS
    • https://openaps.org/
Intrusion Detection System

- CPS
- To test to Tracing module
- Intrusion Detector
- IDS prototype
- Invariant converter Interface
- Daikon
- Texada
- Perfume
- ARTINALI
- CPS model (invariant set)
- Attack detected!
**Targeted attacks**

<table>
<thead>
<tr>
<th>CPS Platform</th>
<th>Targeted attack</th>
<th>Attack entry point</th>
</tr>
</thead>
<tbody>
<tr>
<td>AMI (SEGMeter)</td>
<td>Meter spoofing [ACSAC2010]</td>
<td>Deception on A</td>
</tr>
<tr>
<td></td>
<td>Sync. Tampering [ACSAC2010]</td>
<td>Deception on D</td>
</tr>
</tbody>
</table>

**Take away:**
ARTINALI detected all targeted attacks successfully
Arbitrary Attacks

Data mutations

Smart facial recognition system (CVE-2016-1516)

Branch flipping

CGM spoofing in SAP, [BHC2011]

Artificial delay insertion

Synchronization tampering in smart meter, [ACSAC2010]
Accuracy Metrics

• False Negative Rate (FNR)

\[
\text{FNR} = \frac{\text{Number of detected attacks}}{\text{Total number of injected attacks}} \times 100
\]

• False Positive Rate (FPR)

\[
\text{FPR} = \frac{\text{Number of raised alarms}}{\text{Total number of attack-free tests}} \times 100
\]

• F-Score(\(\beta\))

\[
F(\beta) = \frac{(1+\beta^2 \times TP)}{(1+\beta^2 \times TP + \beta^2 \times FN + FP)}
\]

- \(\beta > 1\)
- \(\beta = 1\)
- \(\beta < 1\)
F-Score(\(\beta\)) - Tuning/Training

SEGMeter

OpenAPS

(a) Daikon  (b) Texada  (c) Perfume  (d) ARTINALI
False Negatives’ Rate

- ARTINALI-based IDS reduces the ratio of FN by 89 to 95% compared with the other tools across both platforms.

![Graph showing FNR (%) with 95% confidence interval for Daikon, Texada, Perfume, and ARTINALI]
**False Positives’ Rate**

- ARTINALI-based IDS reduces the ratio of FP by 20 to 48% compared with the other tools across both platforms.

  - SEGMeter

  ![False Positives' Rate Chart]

  \[
  \frac{(15-12)}{15} = 20\% 
  \]

  FPR (%) - 95% confidence interval
## Overheads

### SEGMeter

<table>
<thead>
<tr>
<th></th>
<th>Performance Overhead (%)</th>
<th>Detection time (sec)</th>
<th>Memory usage</th>
</tr>
</thead>
<tbody>
<tr>
<td>Daikon</td>
<td>27.3</td>
<td>16.63</td>
<td>1.24 MB</td>
</tr>
<tr>
<td>Texada</td>
<td>23.7</td>
<td>14.45</td>
<td>3.21 MB</td>
</tr>
<tr>
<td>Pefume</td>
<td>32.08</td>
<td>19.57</td>
<td>3.94 MB</td>
</tr>
<tr>
<td>ARTINALI</td>
<td>31.6</td>
<td>19.25</td>
<td>2.96 MB</td>
</tr>
</tbody>
</table>

### Time

- **T0**
- **T0+60**
- **T0+120**

- **CPS 1st execution**
- **CPS 2nd execution**
- **CPS 3rd execution**

- **IDS 1st execution**
- **IDS 2nd execution**
Summary and Future Work

• ARTINALI: A Multi-Dimensional model for CPS
  – Captures data-event-time interplay
  – Introduces Real-time data invariants
  – Increases the coverage of IDS
  – Decreases the rate of false positives
  – Imposes comparable overheads

• Examine generalizability of ARTINALI
  – Unmanned Aerial Vehicle (UAV)

• https://github.com/karthikp-ubc/Artinali