Cyber-Physical Security Through Information Flow

Bruce McMillin

Professor and Interim Chair, Department of Computer Science
2018-2020 Distinguished Visitor
Missouri University of Science and Technology
325 Computer Science, 500 W. 15th St., Rolla, MO 65409
o/ (573) 341-6435 e/ ff@mst.edu
Cyber-Physical Security Through Information Flow

Bruce McMillin

Professor and Interim Chair, Department of Computer Science
2018-2020 Distinguished Visitor
Missouri University of Science and Technology
325 Computer Science, 500 W. 15th St., Rolla, MO 65409
o/ (573) 341-6435 e/ ff@mst.edu
Where is Missouri S&T

- 9 Departments, 7500 Students in Engineering
  - ChBE: Chemical Engineering (326/62)
  - CArEE: Architectural Engineering (91/0)
  - Civil Engineering (213/64)
  - Environmental Engineering (58/9)
  - CS: Computer Science (605/93)
  - ECE: Computer Engineering (200/34)
  - Electrical Engineering (253/158)
  - EMSE: Engineering Management (201/41)
  - Systems Engineering (0/20)
  - GGPE: Geology and Geophysics (86/50)
  - Geological Engineering (75/47)
  - Petroleum Engineering (169/84)
  - MSE: Ceramic Engineering (103/9)
  - Materials Science (0/30)
  - Metallurgical Engineering (73/9)
  - MNE: Explosives Engineering (0/9)
  - Mining Engineering (122/26)
  - Nuclear Engineering (99/45)
  - MAE: Aerospace Engineering (215/42)
  - Manufacturing Engineering (0/16)
  - Mechanical Engineering (704/98)
  - Freshmen Engineering (2126/0)

© Bruce McMillin May 2020
CPS

- **Cyber-Physical Systems (CPS)** are physical systems that are controlled and monitored through computer-based systems.
- Critical infrastructures of a nation are CPS
  - Water treatment plant
  - Smart grid
  - Manufacturing plant
  - Autonomous Vehicle
  - Airspace Management
A modern Cyber-Physical System

- Community
- Local Management
- Locally Sourced
Modern Security Domains

- Community
- Local Management
- Locally Sourced
- Secure
- Privacy Preserving
Non-Intrusive Load Monitoring
Management and Governance

• Utility?
  – NISTIR 7628

• Cloud?
  – NERC CIP
  – Timing

• Fog?
  – IoT
  – Locally Managed
  – Locally Protected
Cloud

Dew

Fog

Mist

https://www.pubnub.com/blog/moving-the-cloud-to-the-edge-computing/
https://www.etsy.com/listing/559016362/there-is-no-cloud-its-just-someone-else
https://electronics4things.com/expert-opinion/fog-computing-relevance-iot/
Transactive Energy Management

Who needs Power?

Transfer Power
• Peer-to-peer transactive energy
Threats

• Physical
• Cyber
• Cyber-enabled Physical
• Physically-enabled Cyber

Stealing Plant Secrets
Firewalls

Figure Source, Manufacturers Automation, Inc.
Seems Simple, What could go wrong?

- Physical
- Cyber
- Cyber-enabled
- Physically-enabled
- Cyber
• Centralized Supervisory Control And Data Acquisition (SCADA)

• Electric Utility Control
Biba Model - 1975

• Integrity Levels:
• The higher the level, the more confidence
  – That a program will execute correctly
  – That data is accurate and/or reliable
• Note relationship between integrity and trustworthiness
• Important point: *integrity levels are not security levels*
Problems

• Subjects’ integrity levels decrease as system runs
  – Soon no subject will be able to access objects at high integrity levels
• Alternative: change object levels rather than subject levels
  – Soon all objects will be at the lowest integrity level
• Crux of problem is model prevents indirect modification
  – Because subject levels lowered when subject reads from low-integrity object
BIBA

A

System Control Center

EMS
Energy Management System

SCADA
Supervisory Control and Data Acquisition

Data to market and other systems

RTU
Remote Terminal unit

Sensor Actuators, etc.,

B

Business Network

Messages

© Bruce McMillin May 2020
Security? Bell-La Padula

- Military Multi-Level Security Model
  - No Read Up
  - No Write Down

- Military Commander
  - Write to troops?
  - Downgrade
Data to market and other systems

EMS
Energy Management System

SCADA
Supervisory Control and Data Acquisition

RTU
Remote Terminal unit

Sensor Actuators, etc.,
Fog Energy Management

Transfer Power
The overlapping security domains in an IoT smart grid environment.
Information Present in the Physical Entity
Information Flow Models

• A CPS performs physical actions that are observable
• Should keep these secret – loss of confidentiality/privacy
• Should not keep these secret – loss of integrity
• Some models
  – Non-interference – Goguen and Messegueur 1982
    • High-level events do not interfere with the low level outputs
  – Non-inference – O’Halloran 1990
    • Removing high-level events leaves a valid system trace
  – Non-deducibility – Sutherland 1986
    • Low-level observation is compatible with any of the high-level inputs.
Information Present in the Physical Entity (Non-interference view)

Not a good model for CPS
Information Flow Models

- A CPS performs physical actions that are observable
- Should keep these secret – loss of confidentiality/privacy
- Should not keep these secret – loss of integrity
- Some models
  - Non-interference – Goguen and Messegueur 1982
    - High-level events do not interfere with the low level outputs
  - Non-inference – O-Halloran 1990
    - Removing high-level events leaves a valid system trace
  - Non-deducibility – Sutherland 1986
    - Low-level observation is compatible with any of the high-level inputs.
Information Present in the Physical Entity (Non-inference view)

Command

Potentially a good model for CPS
Information Flow Models

- A CPS performs physical actions that are observable
- Should keep these secret – loss of confidentiality/privacy
- Should not keep these secret – loss of integrity
- Some models
  - Non-interference – Goguen and Messegeur 1982
    - High-level events do not interfere with the low level outputs
  - Non-inference – O-Halloran 1990
    - Removing high-level events leaves a valid system trace
  - Non-deducibility – Sutherland 1986
    - Low-level observation is compatible with any of the high-level inputs.
Information Present in the Physical Entity
(Non-deducibility view)

A good model for CPS
The overlapping security domains in a CPS environment.
Non-deducibility

- Non-deducibility
  – Good?
  
- Bad?

Non-deducibility is a bidirectional model.
The Challenge

• Prevent the bad guys from seeing confidential/private information.
• Make sure the good guys can deduce that an attack is happening from the bad guys
• In a CPS
• With the same model
Multiple Domain Nondeducibility

- Introduced a new model of Nondeducibility MSDND
- Defined with very few constraints
- Modal methods over Kripke frames
- Describes the CPS very well
- Provides a polynomial time reduction from ND to MSDND

MSDND:  
$$MSDND(ES) = \exists w \in W : w \vdash \square [ \big( s_x \lor s_y \big) \land \neg (s_x \land s_y) ]$$  
$$\land \big[ w \vdash (\neg \forall^i_x(w) \land \neg \forall^i_y(w)) \big]$$

On any given world, the valuation functions, $V^i_x(w)$, will return the value of the corresponding state variable $x$ as seen by an entity in a partition, $i$. 
Multiple Domains of Stuxnet

SD^2
(buffer)

PLC

STUXNET SD^1

DEVICE

SD^0

MONITOR STATION

SD^3

SD^4
(Human)

Universe (SD^5)
Stuxnet Attack

I2,1, B2I2,1 T2,1
I1,0, B1I1,0 T1,0

Universe (SD^5)

SD^2
(buffer)

PLC

STUXNET SD^1

DEVICE

MONITOR STATION

SD^3

SD^4
(Human)
Stuxnet Attack

- I2,1, B2I2,1, T2,1
- I1,0, B1I1,0, T1,0
- I4,0, B4I4,0, T4,0
- SD^2
  - (buffer)
  - PLC
  - STUXNET SD^1
  - DEVICE
- SD^0
- SD^4
- Universe (SD^5)
- Alert, Mismatch
- Monitor Station
- I4,3, ~B4I4,3, ~T4,3
- (Human)
Secure Water Treatment Testbed (SWaT)
Process 1: Raw Water

Purpose is to supply water to other processes of SWaT
Working of MSDND

PROCESS 1

FIT101  SD₀  Flow Sensor
MV101  SD₁  Valve
LIT101  SD₂  RAW WATER TANK
P101  SD₃  PUMP
FIT101  SD₄  Flow Sensor

LIT – Level Indication Transmitter, FIT – Flow Indication Transmitter, MV101 – Motorized Valves and P - Pump
Working of MSDND (Cont.)

- SD0
  - FIT101
  - SD1
  - MV101
- LIT101
- Tank T101
- PUMP
- Operator
- PLC1
- FIT102
- SD4

Equations:

1. $I_{5,6} \sim I$
2. $B_{5,6} \sim I$
3. $T_{5,6} \sim I$
4. $I_{6,2} \sim I$
5. $B_{6,6,2} \sim I$
6. $T_{6,2} \sim I$
Working of MSDND (Cont.)

> Since \( B_{5,6} \land T_{5,6} \rightarrow B_5 \), the PLC believes the lie told in all cases. Therefore, unknown to entities in SD2, \( V_2l(w) \) and \( V_2\sim l(w) \) cannot be evaluated. Therefore \( l \) is MSDND secure from SD2.

> \( \text{MSDND}(ES) = \exists w \in W \rightarrow [(S_l \oplus S_\sim l)] \land [w \models (\not\exists V_{SD5} \sim l(w) \land \not\exists V_{SD5} l(w))] \)

> This is BAD for the plant as the threat goes undetected
Working of MSDND (Cont.)

Total Water = (Water Inflow – Water Outflow) * Const

SD8

SD0
FIT101

SD1
MV101

SD2
LIT101

SD3
PUMP

SD4
FIT102

SD5

SD6

Operator

PLC1

VIRUS

Tank

T101

LIT101

PUMP

© Bruce McMillin May 2020
Working of MSDND (Cont.)

- Now when we take the ‘and’ operation for both the normal working and when an invariant is considered, we can conclude that the system is working normally.

- $S_{\text{invariant}} \land S_l = S^*$; System is working normally if and if only this is true.

- $\text{MSDND(ES)} = \exists w \in W \rightarrow [(S^* \oplus S_{\sim l})] \land [w \models (\forall V^{SD5}_{\sim l}(w) \land \exists V^{SD5}_{\sim l}(w))]$
When an invariant fails, the tile with that invariant turns red.
<table>
<thead>
<tr>
<th>Process</th>
<th>Comp</th>
<th>Summary</th>
<th>Suggestions</th>
</tr>
</thead>
<tbody>
<tr>
<td>Process 1</td>
<td>4</td>
<td>Invariants Developed: 4 Invariants Matching: 4 Vulnerabilities remaining: 0</td>
<td>Invariants for FIT and LIT should be modified to better capture multipoint attacks</td>
</tr>
<tr>
<td>Process 2</td>
<td>11</td>
<td>Invariants Developed: 7 Invariants Matching: 0 Vulnerabilities remaining: 6</td>
<td>Chemical processes should be further analyzed for getting more reliable invariants. Chemical dosing pumps and level indication should be modified.</td>
</tr>
<tr>
<td>Process 3</td>
<td>9</td>
<td>Invariants Developed: 4 Invariants Matching: 3 Vulnerabilities remaining: 2</td>
<td>Several attacks can be performed on motorized valves for damaging pumps and draining water. Install PIT near UF Unit to generate invariant for DPIT</td>
</tr>
<tr>
<td>Process 4</td>
<td>7</td>
<td>Invariants Developed: 3 Invariants Matching: 3 Vulnerabilities remaining: 1</td>
<td>Dichlorination Unit and NaHSO3 dosings effects chemical properties of water, using this, better invariants should be made as it effects RO Unit</td>
</tr>
<tr>
<td>Process</td>
<td>Comp</td>
<td>Summary</td>
<td>Suggestions</td>
</tr>
<tr>
<td>---------</td>
<td>------</td>
<td>----------------------------------------------</td>
<td>-----------------------------------------------------------------------------</td>
</tr>
<tr>
<td>Process 5</td>
<td>16</td>
<td>Invariants Developed : 7</td>
<td>Many MSDND Secure paths are identified, invariants should be developed to break the MSDND security</td>
</tr>
<tr>
<td></td>
<td></td>
<td>Invariants Matching : 0</td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td>Vulnerabilities remaining : 9</td>
<td></td>
</tr>
<tr>
<td>Process 6</td>
<td>7</td>
<td>Invariants Developed : 2</td>
<td>Level switches should be replaced with level indicators, and more FIT’s should be installed for getting invariant</td>
</tr>
<tr>
<td></td>
<td></td>
<td>Invariants Matching : 0</td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td>Vulnerabilities remaining : 5</td>
<td></td>
</tr>
</tbody>
</table>
Another Typical Result

Power System Testbed in Singapore
- Solar
- Batteries
- Generators
- Loads

Summary

<table>
<thead>
<tr>
<th>Information paths analyzed</th>
<th>Count</th>
</tr>
</thead>
<tbody>
<tr>
<td>MSDND secure paths found</td>
<td>89</td>
</tr>
<tr>
<td>MSDND secure paths broken using invariants (Total invariants generated)</td>
<td>73</td>
</tr>
<tr>
<td>Invariants implemented in the system</td>
<td>24</td>
</tr>
</tbody>
</table>
WHAT TO DO WITH THIS INFORMATION?
What to do with this information?

- Measure System Security Resilience
  - Using the uniform information flow model
- Improve Design
  - Mitigate MSDND paths
- Mitigate Attacks through Engineered Knowledge to Break MSDND
  - Active defense against
    - Cyber Enabled Physical
    - Physically Enabled Cyber

This is Hard to Do
How to provide a functioning CPS without relying on assumptions of trust, but instead developing trust among components?

**Goals**

- Automated Security Domain Construction
  - Semantic Bridges and Oracle Owls
- Design-Centric
  - Port Hamiltonian Systems
- State Estimation
  - Algebraic, Spatio-temporal & Real-Time Dynamic State Estimation
- Data Science
  - Learn behavior with ground truth

- Experimentation on real infrastructures
  - Power, Water, Manufacturing, Transportation
Findings

Association Rule Mining, Generalized Linear Modeling

Subtle Theft, Slow Drift
Traditional View – Castle/Maginot Line/BLP
- High level vs low level
- Firewalls, Defense in Depth
- Does not address cyber-physical nor insider attacks

Modern Environment
- Multiple security domains
- High/low, Insider vs Outsider has changed
  - We are INSIDE the system
- How do we secure the cyber-physical?
Ethics in these systems

Trolley Problem
Will people use this?

- Privacy
  - Norway vs. USA
- Resilience
  - Cyber threats
- Fog?
  - Ethical Issues

Your Thoughts?
A Professional Society

- Local Seminars
- Get-together
- Quality
  - Accreditation
  - Peer Review
  - Standards
Cyber-Physical Security Through Information Flow

Bruce McMillin

Professor and Interim Chair, Department of Computer Science
2018-2020 Distinguished Visitor
Missouri University of Science and Technology
325 Computer Science, 500 W. 15th St., Rolla, MO 65409
o/ (573) 341-6435 e/ ff@mst.edu