Modeling Hard vs Measurement
Hard

Jason Larsen
SANS Amsterdam 2015
It’s Been a Fun Year

• Hacked into a couple of power utilities over their wireless links
  – Weren’t we supposed to have this solved in 2015?
• Broke the cell modem interfaces to some cars
• Helped a manufacturing plant find a rouge admin interface into their process
• Found out you really can melt big wires off the wall if you change some values in the firmware
Stages of ICS Hacking

Access

Discovery

Control

Damage

Disruption

Cleanup

We’ll be talking about this stuff
Toy Processes vs Real Processes

- Everyone has a toy process they use for trying things out
- This is my rig for investigating negative pressure on pipes and tanks
- It also doesn’t look anything like a real process
- It contains only a few feedback loops and measured values
Real Processes

• As soon as a process is built, the data points are interrelated based on the physics of the process
  – Altering one aspect of the process has downstream effects on other parts of the process

• Changing the temperature might change the pressure and flow
  – Those changes propagate through the process as feedback loops seek to compensate for the disturbance

• Real processes are different than toy processes
Let’s look at three different research problems I’ve been working
1. Minimum Number of Implants
A tale of two toys….

Not all behavior can be estimated from the surrounding data

\[ \vec{v}_{1f} = \frac{m_1 - m_2}{m_1 + m_2} \vec{v}_{1i} \]

- Modeling Hard
- Measurement Hard
2. The Hidden Actor
Disrupting without Understanding

• There are some things in a process that are impossible to understand or model
• All is not lost, the process can still be destabilized
The Hidden Actor

• The attacker wants to drive the car off the road
  – She has control of the brakes
• The attacker closes the left front brake 100% and the car pulls to the left
• The driver compensates by steering to the right eventually coming back into a straight line
Maximizing the Overshoot

$$U_p = Ke(t) + U_b$$

Adjust the change of slope of AB to maximize overshoot
3. Control During Failure
What’s going on at the end of this graph isn’t what’s going on in the middle.

On the other hand, it’s not totally unrelated.
• Can we build a model that adapts to the process as we push it harder and faster than it’s ever been pushed before?
• Can we account for “unexpected physics”? 
These three are really one problem

• We need to drive the logic of an attack with a model
• The model has to be created and modified in real time
• There are things we will never be able to model
Let’s build the most trivial model that can be applied to all three problems
Methane vs CO$_2$
“It will eventually drain with the lowest holes loosing pressure last”

“Engineer

“It will be fully drained in 20.4 seconds and the pressure curve of every hole looks like this.”

Both of these answers are correct
Both of these answers are incorrect
Simple Scaling
Simple Scaling
Best-Fit Monotonic Line Approximation (Triangles)
Force Relaxing

Relaxing a graph matches points based on artifacts just like a human would.
Model Outputs

- For every pair of time series, we can calculate
  - Scale – 5.25
  - Offset - 52.64
  - Slope – 2.28
  - Delay – 9 seconds
  - Fitness – 88.06%
Correlation
Correlation Topology
Attack Feedback

- Given a set of time series and a model, a topology can be generated.
- In near real time, a measure can be produced regarding the fitness of the topology.
- The attacker can systematically manipulate variables until the topology changes.
Same Problem

- Each of these scenarios can be described as a set of time series that predict each other or not
- If a times series can be used to predict another, I call the relationship “Modeling Hard”
- If a time series is independent, I call the relationship “Measurement Hard”
Back to Driving People Off the Road

When the movement of the steering wheel is no longer a predictor of the direction of the car, something significant has changed.
Minimum Number of Implants
The Hidden Actor
Control During Failure

- Steam Transfer
- Temperature/Pressure Builds
- Vacuum Breaker - Move Along
Modeling Hard vs Measurement Hard

• A process can be described as a directed graph in time
• An arbitrary model can be used to partition the graph into sub-graphs where the relationships between the nodes are described (Modeling Hard) and not described (Measurement Hard) by the model
Modeling Hard vs Measurement Hard

• A change in the topology of the sub-graphs signals a disruption of the process
• Actions immediately during the topology change generally have greater impact than actions before or after the change
A Note on Incomplete Models

• I spent a bunch of research time looking for an auto-generating model that is complete and can be miniaturized enough to fit in a typical embedded device
  – No model will ever be complete enough

• A lesser model that adapts to changes in the environment is more desirable than a static model that is more accurate
TODO: Electric Power
Questions?

Jason Larsen
Jason.larsen@ioactive.com