Semantic Security Monitoring for Industrial Control Systems

BRO

ADAM SLAGELL, UNIVERSITY OF ILLINOIS AT URBANA-CHAMPAIGN

Cybersecurity Research Acceleration Workshop and Showcase, Indianapolis, IN
October 11, 2017

Cybersecurity Research Acceleration Workshop and Showcase

October 11, 2017 | Indianapolis, IN

Quad Chart for: Semantic Security Monitoring for Industrial Control Systems

Challenge:

Develop new network security monitoring techniques for Industrial Control System networks based off of protocol semantics & physical state

Solution:

- Understand the **high-level semantics** of key ICS protocols
- **Create proof-of-concept** new attack detection methodology for industrial control systems
- **Demonstrate feasibility** of non-signature-based detection against several attacks in the lab
- Develop & **release ICS protocol analyzers** to incorporate into Bro to support the research objectives of this award

NSF SaTC #1314891
NCSA/UIUC
PI: Adam Slagell, NCSA; Co-PI Ravi Iyer UIUC
Team: Daniel Thayer, Vlad Grigorescu, Jon Siwek, Phuong Cao, Hui Lin

Value proposition:

- Advance the understanding of ICS network defenses
- Provide a framework to develop new tools to detect 0-day exploits
- Protect critical infrastructure such as the power grid

What we need to TTP

- Additional ICS networks for Bro deployment
- Feedback on the set of analyzers already developed
- Real world traffic from ICS networks

Contact us

- slagell@illinois.edu
- rkiyer@illinois.edu
- info@bro.org

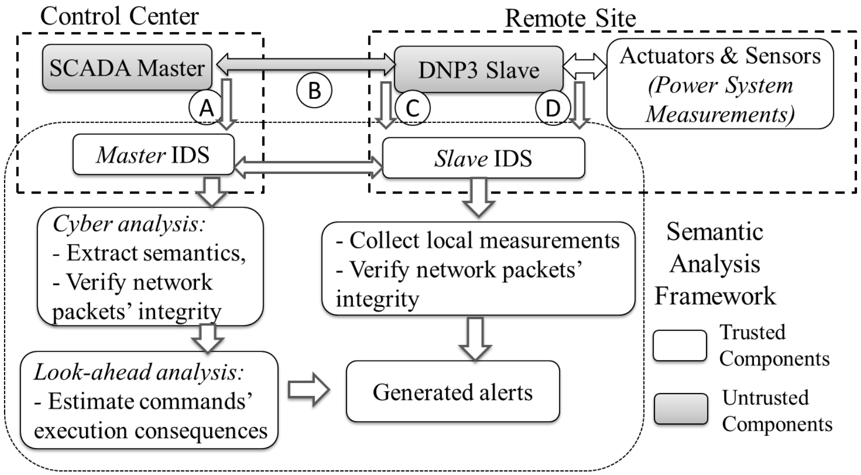
Runtime Semantic Security Analysis to Detect and Mitigate Control-Related Attacks in Power Grids

Challenge:

- Control-related attacks:
  - Penetrated isolated control networks
  - Use commands crafted in legitimate formats to cause damage
- Hard to detect control-related attacks
  - Few anomaly activities are found in SCADA networks
  - Few attack signatures are publically available

Solution:

- Extend Bro IDS to support protocols in Power Grids
- IDS at control center
  - Use power flow analysis to analyze commands
  - Adapt power flow analysis to balance detection latency and accuracy
- IDS at substations
  - obtain trusted measurements from local sensors
  - Validate absence of corrupted measurements at other locations



Control Center

Remote Site

SCADA Master

DNP3 Slave

Actuators & Sensors *(Power System Measurements)*

A

B

C

D

Master IDS

Slave IDS

Cyber analysis:
- Extract semantics,
- Verify network packets' integrity

- Collect local measurements
- Verify network packets' integrity

Look-ahead analysis:
- Estimate commands' execution consequences

Generated alerts

Semantic Analysis Framework

Trusted Components

Untrusted Components

Scientific Impact:

- Detect attacks by estimating the consequence of executing commands
- Balance detection accuracy and latency
  - Reduce the computation time by fifty percent compared with AC power flow analysis
  - Increase the accuracy by two orders of magnitudes compared with DC power flow analysis

Broader Impact:

- Provides protection to manual commands
  - Does not affect the normal operations
  - Can be extended to other industrial control systems
- IDS can be equipped with other scenario-specific policies

Semantic Security Monitoring for Industrial Control Systems, NSF Award #1314891

Contacts: Adam Slagell slagell@illinois.edu (PI), Ravishankar Iyer (Co-PI)

What is a Software TTP Success?

- Commonly cited or inferred:
  - Financial stability
  - Broad user base
  - Sustained development
  - Spinning off a startup
  - Not asking for money any more ☺
- What's the Problem?
  - These are neither necessary nor sufficient
- Real goal is hard to measure; has many paths
  - *A strong and diverse user base with a responsive development team*

Post hoc ergo propter hoc

- Globus
  - Serves 1000s of users; builds on nearly 20 years of history
  - Approach: SaaS and closed source
- Bro
  - Serves 100s of EDUs, many Fortune 50 companies; built into appliances
  - Exponential community growth over 20 year history;
  - Approach: Join a foundation for open source & startup company
- LLVM
  - Millions of developers use it for compiler and other tools
  - Google and Apple depend on it
  - Approach: Start a foundation, large sponsorship, 100s of contributors

Can we learn anything?

- Unlikely to predict successes, too many variables
- Almost every successful TTP has made hard trade-offs survive
  - SaaS is often not applicable
- User growth does NOT imply contributor growth
  - Complex software often has few contributors, harder to keep free
- Huge deployments can grow technical debts silently
  - E.g., OpenSSL crisis a couple years ago
- Software we make today can become tomorrow’s critical infrastructure
  - Tragedy of the commons to sustain

Conclusion

- *Transitioning research to practice is hugely important to realize the impacts from research, but we have not come close to solving the next problem,* ***transition to sustainability****.*