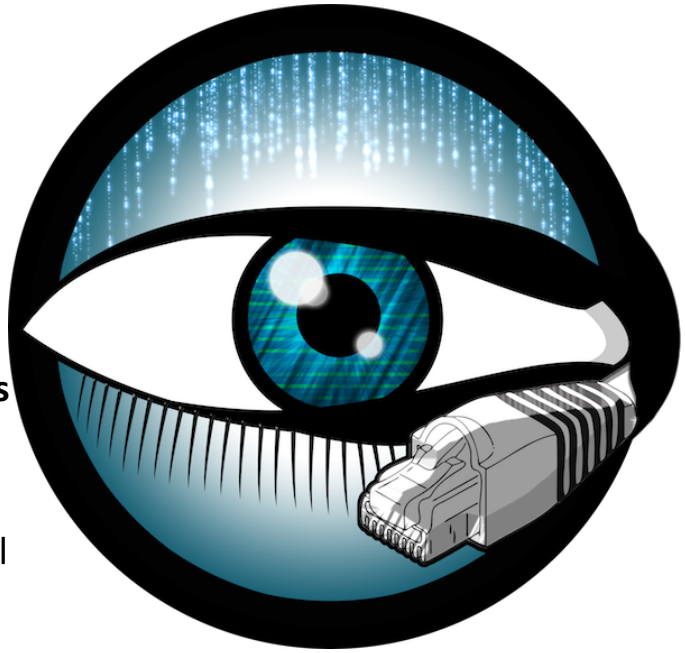
Cybersecurity Research Acceleration Workshop and Showcase

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



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

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

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

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

Contact us

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