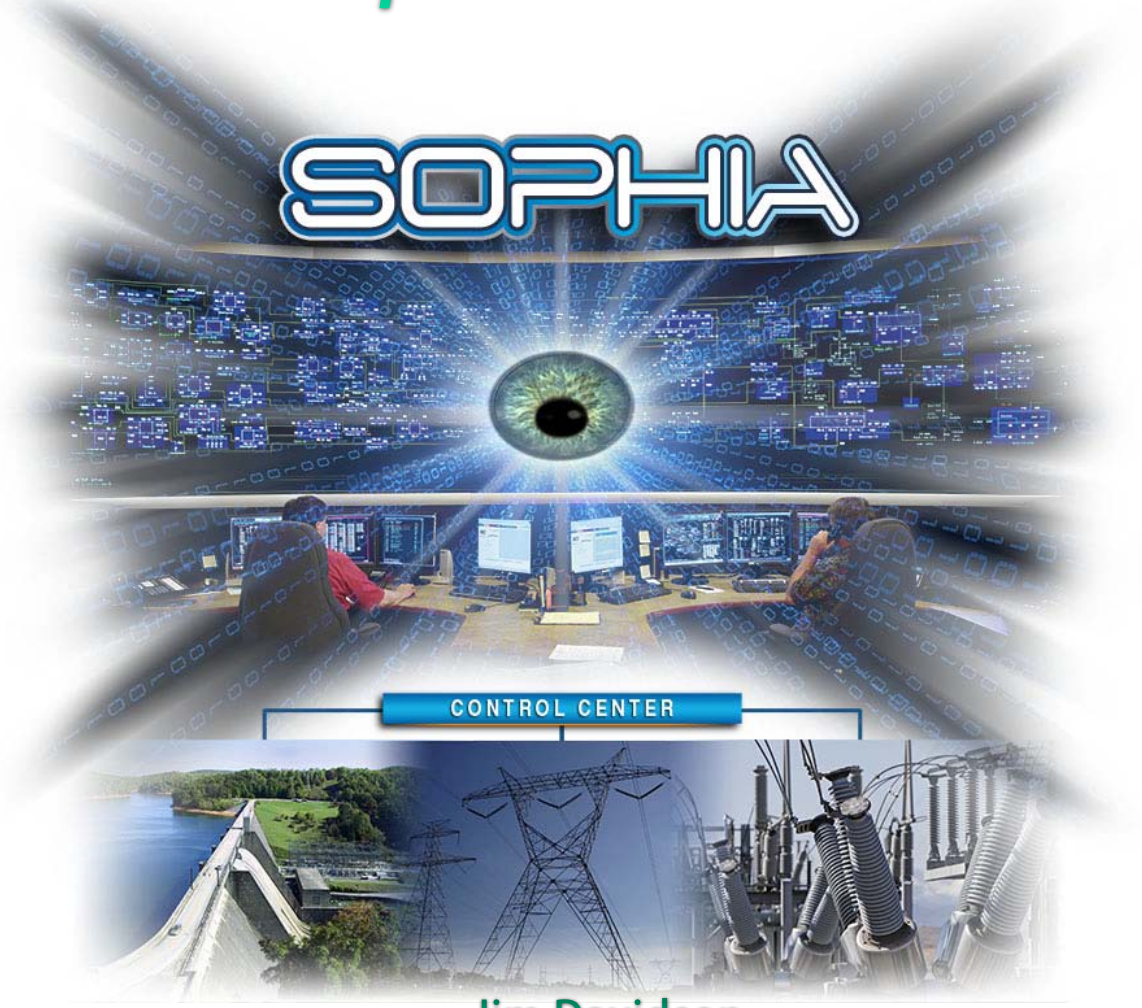
Tool development for ICS Security



Jim Davidson
Idaho National Laboratory

www.inl.gov

Idaho National Laboratory

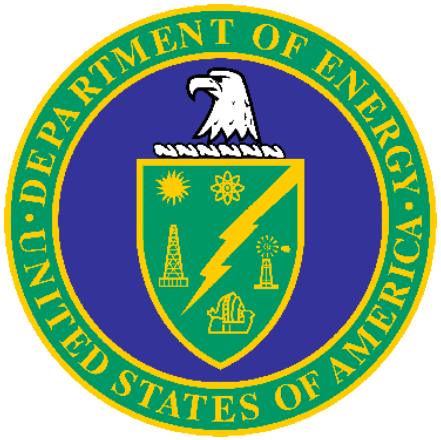
U.S. Department of Energy
Office of Electricity Delivery
and Energy Reliability

INL/CON-10-18077

DOE-OE

National SCADA Test Bed:

DOE OE Mission - Support industry and government in reducing control system vulnerabilities in the energy sector.



The Network Dichotomy *(the CIA v.s. the AIC Model)*

Corporate IT Networking

- ***Prioritization***
  - **C**onfidentiality
  - **I**ntegrity
  - **A**vailability
- ***Network Reality***
  - Dynamic in Nature
  - Many Supported Apps
  - Significant Number of Users

Control System Networking

- ***Prioritization***
  - ***Availability***
  - ***Integrity***
  - ***Confidentiality***
- **Network Reality**
  - Static in Nature
  - Limited Number of Apps
  - Highly Specialized Users

Basis for ICS Tool Development

- Use AIC Networking Model
  - Static Environment
  - Limited Apps
  - Specialized Users
- Passive
  - Zero Impact on Production System
- Ease of Use
  - Should enhance capabilities with minimum effort
- Security
  - Designed in, not added
- Extensible
  - Allow for future needs

Sophia - a use case

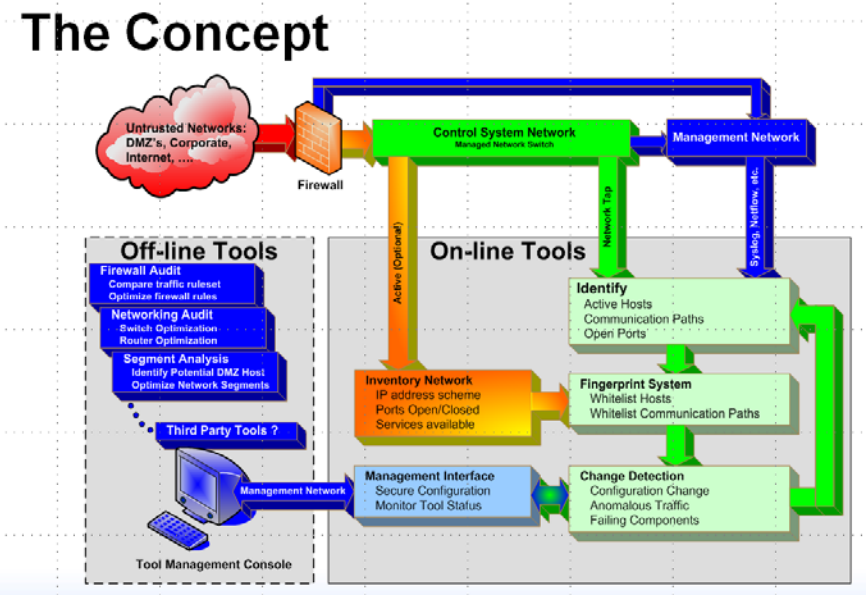
Overview:

- Present Concept
- Develop Proof-of-Concept
- Identify Use Extremes
- Select Test Sites
- Develop Additional Use Cases
- Final Design Development
- Proposal

Sophia - a use case: Present Concept

Future Tool Concepts

- Network Traffic Monitoring
- Identify Communications
- “Fingerprinting”
- “Whitelisting”
- Change Detection
- Optional Active Component
- Post fingerprint analysis
- Open Source Code



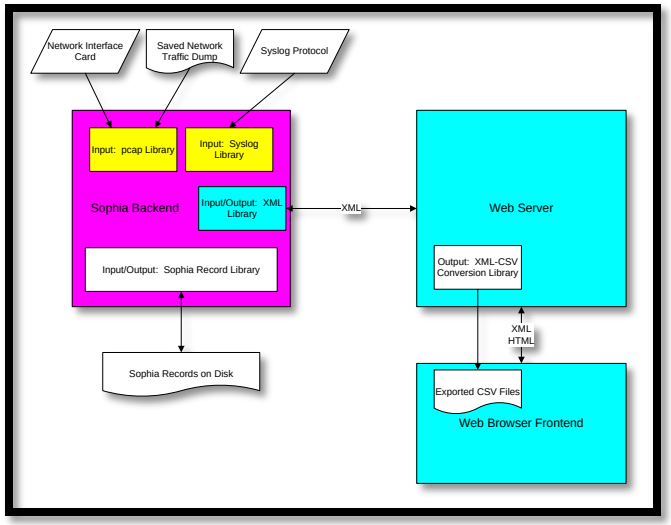
Sophia - a use case: Develop Proof-of-Concept

Philosophy: Identify concerns related to ICS deployment by using the same techniques as cyber attackers and encourage mitigation of those concerns.

Monitor network traffic using spanned port data and extract the source, destination, and port sets (conversations) between ICS components.

Whitelist Valid Conversations
Greylist New Conversations for Validation
Blacklist Prohibited Conversations

WEB Interface



Sophia - a use case: Identify Use Extremes

- Systems
  - Small Scale
  - Large Scale
- Network Architectures
  - Simple, Single LAN
  - Complex, Highly Segmented LAN Structure
- IT Skill Level
  - Entry Level
  - Advanced
- Users
  - Few
  - Many, Crossing IT Boundaries

Sophia - a use case: Selected Test Sites

- Utility 1
  - Simplified Network Architecture
  - IT Skill Level – Entry Level
  - Users 2
- Utility 2
  - Complex, Multi-segmented Network
  - IT Skill Level – Advanced
  - Users >15 at multiple levels
- Vendor
  - Various Network Architectures
  - IT Skill Level – Advanced
  - In-house & External Deployment

Sophia - a use case: Develop Additional Use Cases

Configuration Management:
Alarm may indicate the addition of a new component or process triggering a configuration management review.

Fielding New Systems:
Use a fingerprint developed as part of the factory acceptance test (FAT) during the Site Acceptance Test (SAT) to identify required site specific communications.

Firewall Rule Validation/Development:
The fingerprint represents only what is needed for ICS operations, providing critical information necessary for simple quality firewall rules.

Switch and Router Configuration:
Switches and routers can be configured based on what is needed as identified in the fingerprint. Port security such as Access Control Lists (ACL) are easily created and used.

Component Hardening:
All necessary ports are identified in the fingerprint. All other ports are not required for operation and can be disabled or blocked by a personal firewall reducing exposure to cyber attack.

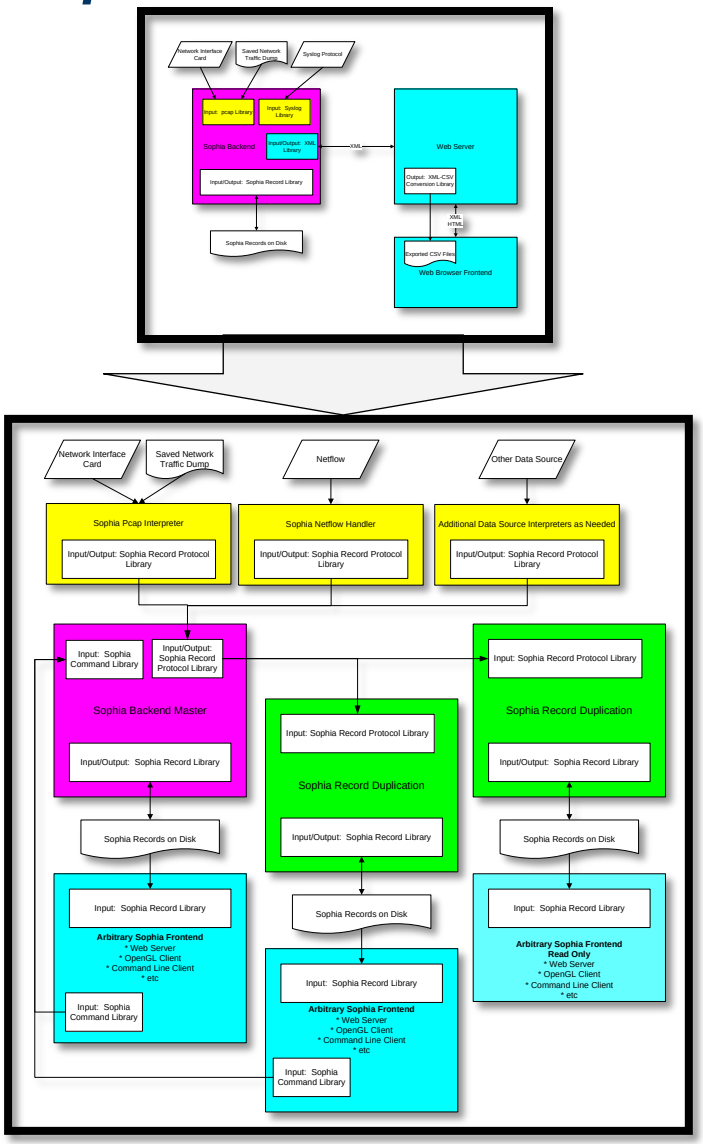
Patch Testing:
When used on a quality system, changes in normal operational communications will be quickly identified as patches are rolled out. Patches in some cases re-open previously disabled ports and services.

If newly identified ports are required, Sophia provides useful information necessary for a safe rollout of the patch on the active control system. Configuration management issues are identified; firewall rules may need changing, ACLs may need updating, etc.

Situational Awareness:
Alarms provide online identification of off normal events. These alarms could indicate a cyber attack, unauthorized access, hardware or software failures, new processes coming online, new equipment added, etc.

Sophia: a use case: Final Design Development

- Passive, online, real time ICS conversation analysis; no interaction with the ICS.
- Safe to use in a production environment.
- Works with new and legacy systems.
- Ease of use - can be learned in one to two days.
- Detects and alarms on conversations that are not part of normal ICS operations.
- Fingerprint export for offline analysis.
- Software hooks allow sharing fingerprint data with third party tools for offline analysis.
- Provides full functionality for ICS installations in all critical infrastructure sectors.



Sophia - a use case: Proposal

Questions ?

James R. Davidson
Idaho National Laboratory
Office: 208-526-0422
Cell: 208-520-2806
Email: james.davidson@inl.gov

www.inl.gov

Idaho National Laboratory

INL/CON-10-18077