U.S. DEPARTMENT OF ENERGY

Sophia Fingerprinting Tool

Funding Source: Department of Energy (OE)

Description

Sophia is a passive, real time tool for interdevice communication discovery and monitoring of the active elements in a Supervisory Control and Data Acquisition (SCADA) system.

Sophia monitors network traffic from which it extracts the source, destination, and port sets (conversations) between SCADA components. These conversations are stored in real time to establish a list of conversations that are valid.

After the tool has been in place for a period of time, the user accepts this list as representative of the normal conversations expected from their SCADA and the list of conversations is established as a baseline fingerprint (whitelist) of accepted conversations.

After the fingerprint is accepted, Sophia continues to monitor and capture conversations and generates an alarm on any conversation that is not a part of the system fingerprint.

The user then analyzes the alarm with three choices:

- Add it to the whitelist (fingerprint) – the conversation is valid.
- Add it to the blacklist – not required for system operation, always alarm.
- Do nothing, leave it on the greylist – Analyze it later, but do not alarm on any further occurrences.

Sophia software was developed based on an industry need. This need was identified during on-site cyber security assessments, discussions with users at various SCADA user group meetings and training sessions, and an understanding of open source tools used in evaluating the cyber security footprint of an SCADA.

The philosophy for the tool development was to identify concerns related to SCADA deployment by using the same techniques as cyber attackers and encourage mitigation of those concerns.

Sophia (Greek for Wisdom) provides the user with the knowledge to make wise decisions that enhance the security and reliability of their SCADA.

Based on asset owner feedback and DOE-OE milestones, Sophia is slated for commercialization for wide scale production distribution by October 2012.

Availability Status

Beta software: Currently soliciting applications for Beta testers from US Energy Companies. Apply at: https://secure.inl.gov/sophia

Commercialization Release: October 2012

Idaho National Laboratory

For More Information:
Gordon Rueff
208-526-0311
Gordon.Rueff@inl.gov

David Kuipers
(208) 526-4038
David.Kuipers@inl.gov

Sophia Fingerprinting Tool

Key Features

- Passive, online, real time conversation analysis; no interaction with the SCADA.
- SCADA network traffic visualization in a 3-D graphical environment.
- 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 SCADA operations.
- Fingerprint export for offline analysis.
- Software hooks allow sharing fingerprint data with third party tools for offline analysis.
- Provides full functionality for SCADA installations in the Energy sector.

Potential Applications

- Network traffic anomaly detection and alarming.
- Vulnerability and Red Team Assessments.
- Test Beds for Cyber Security System Analysis and Testing.
- Network Mapping Tools and Techniques.
- Secure Network Design Consultation.

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 SCADA 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.

Idaho National Laboratory

For More Information:
Gordon Rueff
208-526-0311
Gordon.Rueff@inl.gov

David Kuipers
(208) 526-4038
David.Kuipers@inl.gov