

Security Services Suite (SecSS)

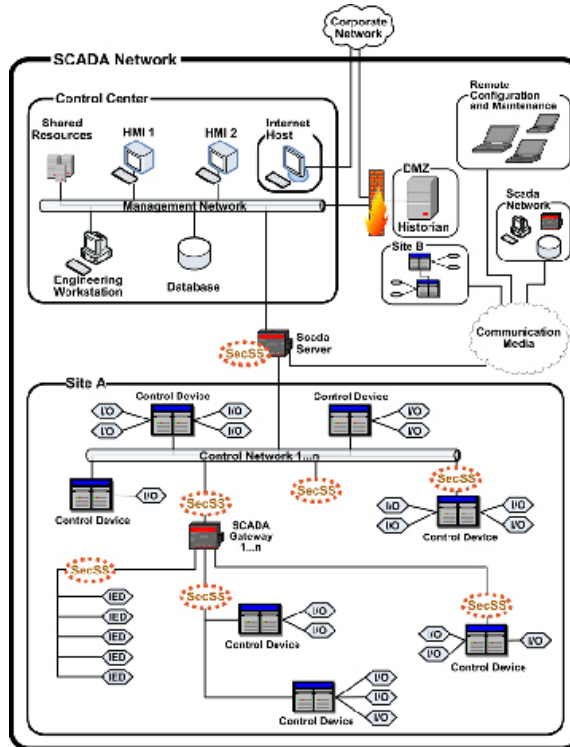
Monitoring tools for field level networks



Overview

The security services suite provides technical solutions to protect communication networks in Industrial Control Systems. The suite incorporates five approaches that provide security functionality at different levels of the network infrastructure: message monitoring, protocol-based solutions, tunneling services, middleware components and key management. The suite provides security mechanisms that can be integrated with legacy systems, allowing them to establish trusted and secure communication paths.

The current research focuses on message monitoring to provide enhanced situational awareness for industrial control operators. This tool will provide a distributed scanner that remotely verifies the functionality and state of field devices in Modbus networks. The scanner accommodates the delicate TCP/IP stacks of field devices and scanning activities can be scheduled so as not to impact control operations. Tests on laboratory-scale and virtual environments indicate that the distributed scanner is scalable, distributable and operates satisfactorily in low bandwidth environments. These features make it an attractive tool for providing situational awareness in pipeline control networks, including those incorporating legacy systems.



Network Architecture

What vulnerabilities does this tool address?

- *Spoofing*: rogue devices that impersonate master devices
- *Tampering*: malicious modification of control messages in the network
- *Repudiation*: control traffic that cannot be traced to a valid member of the control network
- *Information disclosure*: eavesdropping on control traffic leading to disclosure of sensitive information
- *Denial of service*: malicious traffic that misconfigures or perturbs operations

Why is Monitoring Important?

Security measures are put in place to prevent unauthorized access. However, no systems are 100% effective. Monitoring is the only way to know exactly what communication is taking place. Some practical benefits are the identification of available devices, assurance of proper operation and the discovery of network services and capabilities in use. Monitoring also provides a good indication of system health.

From a security perspective, monitoring allows identification of rogue devices, unauthorized communications, detection of anomalous operation, and violation of access control.

Key Features & Benefits

What are the unique features of this technology?

- Network Monitoring
- Support for event correlation tools
- Securing legacy control protocols

Similar technologies?

- AGA 12 part 2 provides a standard to secure control protocols on legacy serial links.
- Snort rules exist for the examination of Modbus control traffic.
- PKI key management systems are widely deployed for IT solutions.

Why this tool and not the others?

- There is no solution that addresses specifically Modbus and DNP3 protocols over Ethernet links.
- No tools exist to detect malicious Modbus and DNP3 traffic.
- Existing PKI cannot be used for SCADA systems



The Center for Information Security (CIS) at the University of Tulsa supports information security education, research, and service activities. As a National Security Agency Center of Excellence (NSACOE), CIS has the overriding goal of helping establish and execute the national agenda for protecting the networks and information systems our society relies upon.

Functional Description

How is the tool operated?

- The tool passively monitors MODBUS traffic in a DCS system on a TCP/IP network.
- An active scanner can report nodes on a network and map supported functions and register space.
- Active and passive system alerts can be sent to an intrusion detection system for event correlation.
- Passive and active scanning initiated by operator. Event detection operates as a service or daemon. Middleware solutions planned as embedded solutions.

System Requirements

- Java based solution allows for cross platform use. Runs on the majority of operating systems including UNIX, Microsoft Windows, Linux and Mac OS X
- Supports dual network interfaces for passive scanning of control network while sending alerts over a management LAN

Summary of Costs

	Low	Medium	High
Component	<\$1,000	\$1,000-\$10,000	>\$10,000
Engineering	Drop-in	Moderate modification	Complete System Design Lifecycle
Bandwidth/Network Burden	None-Passive Only	Moderate Traffic, Medium Overhead	Heavy Traffic, Large Overhead
Training	No training required	Moderate training	Intensive training. Additional staffing may be required.
Maintenance and Operation	< 1 hour per week	< 5 hours per week	> 5 hours per week

Technical Description

An oil pipeline uses a process control system to manage and operate all control elements in real time. Being part of a comprehensive approach to PCS security, SecSS tools are designed to complement other technical solutions and assist in the implementation of a defense in depth posture. A distributed network scanner provides increased situational awareness by placing sensors on strategic communication points in the process control network.

Architecture

- Client/server model
- Master scanner is the central control point for all scanning activities Initiates scanning activities on sensors and provides reports by querying database
- Remote sensors implement active and passive scanning. These incorporate some intelligence to minimize impact on process control network

Active Scanning

Queries devices in the process control network obtaining:

- Unit configuration (ID and IP)
- Supported operations
- Memory mappings
- Diagnostics
- Scheduled over time to minimize traffic

Passive Scanning

Passively analyzes messages flowing through the process control network:

- Provides Modbus topology information
- Identifies masters and slaves
- Reports requested operations, and its details (reads, writes, memory addresses, etc.)
- Anomaly detection including rogue masters and abnormal operations
- Limits the amount of traffic generated to minimize impact on network

Technology Transfer and Readiness:

- Under development

For more information about the Survivability and Recovery of Process Control Systems project, visit:

<http://www.thei3p.org/research/srpcs.html>

This material is based upon work supported by the U.S. Department of Homeland Security under Grant Award Numbers 2006-CS-001-000001 and 2003-TK-TX-0003, under the auspices of the Institute for Information Infrastructure Protection (I3P) research program. The I3P is managed by Dartmouth College. The views and conclusions contained in this document are those of the authors and should not be interpreted as necessarily representing the official policies, either expressed or implied, of the U.S. Department of Homeland Security, the I3P, or Dartmouth College.



The I3P is managed by Dartmouth College.

Researcher Contact Information

Sujeet Sheno sujeet@utulsa.edu
 Mauricio Papa mauricio-papa@utulsa.edu
 Rodrigo Chandia rodrigo-chandia@utulsa.edu