Securing Supervisory Control and Data Acquisition (SCADA) and Control Systems (CS)

What are SCADA and CS?

Supervisory Control and Data Acquisition, or SCADA, is a term that refers to systems and networks that monitor, manage, and control automation, production and distribution. In industrial applications, similar systems are also known as Distributed Control Systems (DCS), Process Control Systems (PCS), Safety Instrumented Systems (SIS) and Energy Management Systems (EMS). Collectively they are referred to as Control Systems (CS).

Why Secure SCADA and CS?

Historically, CS were physically isolated and relied upon point-to-point communications. In order to gain improvements in efficiency, CS began to migrate to network-based communications and grow external connections. Many were designed prior to the wide scale adoption of network security products and practices and unfortunately, most CS lacked adequate consideration of and protection from network attack. This trend has evolved to the point where today, for a myriad of reasons, CS are often connected to the global Internet.

Connecting a CS to the Internet, whether directly or indirectly through a corporate LAN and its firewalls, makes it vulnerable to network attack. Security measures are necessary to mitigate and manage these vulnerabilities, but often cannot totally eliminate them. Along with this connectivity, some level of risk must be accepted. Total isolation from non-CS networks is the only means of making a CS impervious to network attack. Admittedly, such isolation comes with a high price and may be unworkable. Therefore, the SNAC offers the following network security recommendations for SCADA and CS.

Security Recommendations

Develop a Security Policy

A Security Policy defines the controls, behaviors, and expectations of users and processes, and lays the groundwork for securing CS assets. Since the acceptable use of CS is narrower, and they have more demanding operational requirements than IT systems, they also demand their own Security Policy. See the Sandia National Labs, *Framework for SCADA Security Policy* for a good starting point.

Establish Physical Security

Establish good physical security (Guards, Gates, & Guns) to protect CS equipment from physical damage and unauthorized access.

Lockdown Perimeter Security

Eliminate all external connections to the perimeter of the CS which are not absolutely necessary. For necessary connections, authenticate, authorize, and monitor any use over those connections.

- Understand, document, and periodically review the necessity for each external connection.
- Consider the use of security products for perimeter protection that meet the NIST FIPS standards.
- Allow only known users of known devices to reach known destinations during known time periods and log the details of the activity.

Enable Existing Security Features

Effectively utilize security features of current CS and infrastructure devices.

- Configure any available user access controls.
- Change the defaults and use strong passwords.
- Eliminate or protect any paths over which plaintext access control can't be avoided.
- Do not reuse or share User IDs or passwords between systems or personnel.
- Practice good OPSEC; don't reveal information jewels through banners, device names, etc.
- Configure router access control lists (ACLs) to restrict network protocols and connectivity.
- Use switch Virtual LANs (VLANs) to isolate like traffic, making ACLs easier to apply and manage.
- Use MAC filtering to block out unknown devices.

See www.nsa.gov for guides on routers, switches, wireless LANs, and port security, etc.

Secure Operational Traffic

Eliminate any unnecessary operational traffic.

- Disable non-essential features on CS devices.
- Put like devices on the same VLAN, then use router and switch security features to only allow known devices, their required protocols, and their specific network connectivity on those VLANs.

Secure Management Traffic

Use dedicated hosts for device management. Don't use them for any other purpose. Use router and switch security features to only allow these hosts, using specific management protocols, to access infrastructure and CS devices. Isolate and protect management traffic from operational traffic in any of the following ways:

- Manage devices through direct local connection.
- Manage devices using an out-of-band network or serial connection. This requires both dedicated communications bandwidth and a dedicated management interface on each device.
- Manage devices using a protected in-band remote connection. Use VLANs for in-band isolation, ACLs for traffic control, and VPNs, where available, for integrity.

Manage the CS Configuration

Good configuration management starts with good documentation.

- Map out and document the entire CS network, including CS and infrastructure device configurations.
- Prepare and configure new equipment off-line.
- Sanitize old equipment before disposal.
- Keep CS infrastructure security features current with device moves, additions, and decommissions.
- Enable auditing features and periodically examine the resulting logs for signs of unusual activity.
- Synchronize to a common time reference, so audit logs become more useful during incident response.
- Develop a Disaster Recovery Plan (DRP) for the CS, and if possible test it!

Eliminate Security Shortfalls

Identify security shortfalls (using established CS Security Policy) and develop a plan to proactively eliminate them.

Continuous Security Training

Involve all CS personnel with security. Make it relevant. Provide comprehensive security training with refreshers on a periodic basis.

Perform Security Audits

Verify effectiveness of security measures by performing frequent, irregularly scheduled, security audits.

SCADA and CS Security Checklist:

- ☐ Develop a Security Policy
- ☐ Establish Physical Security
- ☐ Lockdown Perimeter Security
- ☐ Enable Existing Security Features
- ☐ Secure Operational Traffic
- ☐ Secure Management Traffic
- ☐ Manage the CS Configuration
- ☐ Eliminate Security Shortfalls
- ☐ Continuous Security Training
- ☐ Perform Security Audits

Systems & Network Analysis Center (SNAC)
410-854-6632 / DSN 244-6632
www.nsa.gov/snac
snac@radium.ncsc.mil

NSA Creative Imaging 32735VRL