Defending Energy Utilities from ICS/IoT Attacks

…musings of a 40+ year veteran control system engineer

About Hank

- Control System Engineer – 40+ years experience in electric utility business
- Designed and configured many different DCS and PLC systems
- Performed system startup & commissioning
- Tuned controls & resolved problems
- Implemented medium and low voltage electrical system integration
- Developed 5-year forward corporate ICS planning
- Developed strategy for ICS/IoT Cyber Security
- Implemented CS strategy and fine tuned

Why Care About ICS/IoT Security

- Legislative responsibility for stability of bulk electric system (NERC, FERC, state regulations)
- Potential for risk to population from major power interruption

- Possibility of risk to Nuclear infrastructure
- Potential for damage to the environment
- Damage to national economy
- Company financial risk

$

Why is Monitoring Necessary

Issues…

Strategic…

Functional…

Equipment…

Design…

Leadership…

Maintenance…

Other…

Strategic

- Poor integration choices, like…
  - UPS
  - HVAC
  - Fire Protection
  - Security Cameras
  - Gas Monitors
  - Wireless Devices
- Static Accounts for specialty software
  - Historians
  - Inventory tools
  - Alarm management software
  - Diagnostic Software
- Time servers (firmware, segregation)

Why is Monitoring Necessary

Issues…

Strategic…
Functional…
Equipment…
Design…
Leadership…
Maintenance…
Other…

Functional

- Support for only specific OS versions
- Hardware-specific licensing of OEM software
- Multi-homed network designs
- Weak Domain group policies (or workgroups)
- Simplistic or unmanaged switch configurations
- Unencrypted control communication over publicly known protocols
- Peer-to-peer communication
- Unchangeable default passwords
- Limited security testing of ICS/IoT software
- Very limited support for non-OEM software

Why is Monitoring Necessary

Issues…

Strategic…
Functional…
Equipment…
Design…
Leadership…
Maintenance…
Other…

Equipment

- ICS equipment is always behind the curve
  - Hardware
  - Operating Systems
  - OEM Software

- Systems are often built on commodity hardware
- Physical distribution

Why is Monitoring Necessary

Issues…

Strategic…
Functional…
Equipment…
Design…
Leadership…
Maintenance…
Other…

Design

- – Remote support
- – Connections to third-party systems
- – Enterprise application connections
  - Work order management
  - Cost Tracking
  - Historians
  - Environmental reporting
  - e-mail ?
  - Internet ?

Why is Monitoring Necessary

Issues…

Strategic…
Functional…
Equipment…
Design…
Leadership…
Maintenance…
Other…

Leadership

- Refusal to acknowledge IT-like nature of ICS/IoT
  - General access accounts: tech, oper, maint, admin
  - Admin-level accounts often left logged in
  - Control applications left open
  - Operators running as administrators
  - Commissioning accounts never de-activated
- Loose management of outside (contract) support engineers
  - Hardware
  - Background Checks
  - Supervision
- Weak (or no) transient asset policies
- Incomplete security review/management of OEM ‘spy’ boxes
- Passwords not complex and seldom or ever changed
- Technicians operate as admins with no IT security training
- Unmanaged ecosystem personnel access: HVAC, UPS, Physical Security, Cleaning…

Why is Monitoring Necessary

Issues...

- Strategic...
- Functional...
- Equipment...
- Design...
- Leadership...
- Maintenance...
- Other...

Maintenance

- Risks associated with patching OS
- High costs and risk associated with updating OEM software
- Maintenance burden of updating Antivirus files
- Difficulty of making and testing backups
- Lack of adequate and up-to-date lab environment
- Weak boundary defenses (files coming into environment)
- Potential for ‘Watering Hole’ attacks from OEM sites

Why is Monitoring Necessary

Issues…

Strategic…
Functional…
Equipment…
Design…
Leadership…
Maintenance…
Other…

Other Challenges

- There are no standard pre-hardened (gold standard) machine images
- Most systems were installed without any Security FAT
- Unused switch ports are available, unlocked
- ICS/IoT machine and switch logs are not collected or analyzed
- ICS/IoT system architecture drawings available on Enterprise systems
- Enterprise-edge firewall rules are weak based on poor understanding of ICS/IoT protocols
- No or inadequate penetration testing (Red Teaming)

Operational Benefits of Continuous OT Network Monitoring

- Assist in understanding ICS/IoT network traffic and how systems actually function
- Find undocumented devices on the network
- Identify mis-configured equipment, identifying unnecessary protocols such as DHCP, DNS root hints, IPv6, etc.
- Identify failed backups (failed SMB connections)
- Show protocols that should not be enabled, such as NetBIOS, snmp, ipx, etc.

Operational Benefits of Continuous OT Network Monitoring

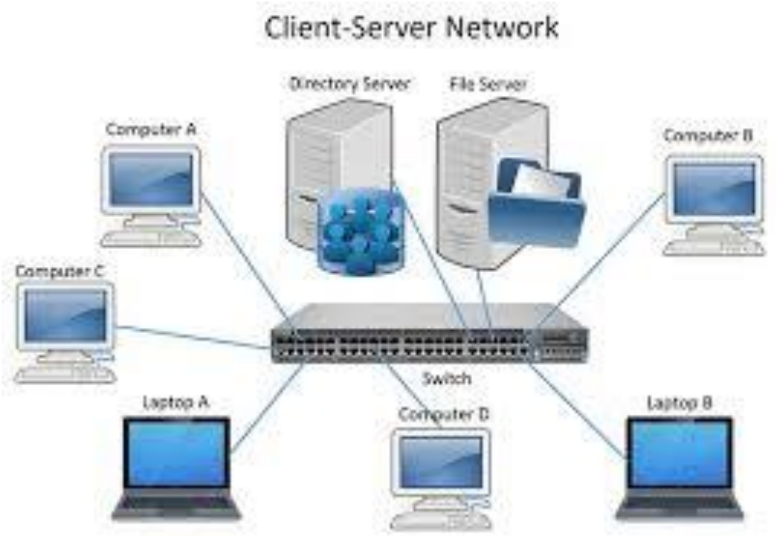
- Show failed connection attempts, bad register addresses, etc. in various industrial protocols, most commonly Modbus, OPC, DNP
- Clean-up traffic to improve speed of updates on HMIs
- Identify switch mis-configurations
- Find plain text passwords in various configurations, for instance snmp, ftp
- Provide awareness of all controller downloads
- ***Learn what 'Normal' looks like***

Developing Multi-Layered Security

- Know Your Network
- Domain Controllers
- Endpoints
- Network Devices
- Remote Access
- Backups
- Transient Assets
- Foreign Devices
- Firewalls
- Miscellaneous

Know Your Network

- Device list
  - IP Address(s)
  - MAC Address(s)
  - OS / Patch Level
  - Hardware Type / Firmware
- Accurate logical and physical maps
- Up-to-date software inventory
- Expected ports and protocols in use



Domain Controllers

- Gold standard image
- Up-to-date firmware
- Secure group policies
- Regular password changes & security requirements
- Separate group policy & creds for domain updates
- Manage network switch creds as domain members
- Event forwarding to SIEM, esp. any changes to admin group
- <u>Severely</u> limit access to DCs
- Domain admin account used only when absolutely required
- Follow principle of least privilege

Endpoints

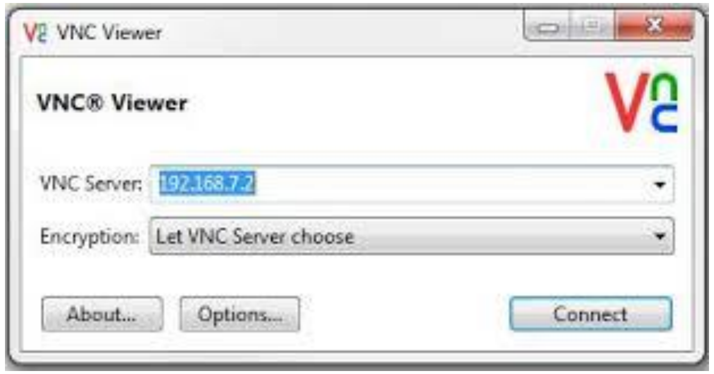
- Whitelisting (where possible)
- Up-to-date firmware / secure boot
- Software/hardware inventory (remove unused apps)
- Event forwarding to SIEM
- Regular Backups
- Use least privilege required for each activity
- Enforce regular password changes
- Remove group access accounts
- Patch as often as possible, OS and apps

Network Devices

- Hardened switch configurations
- Up-to-date (stable) firmware
- Monitor all networks on all switches
- Shut unused ports
- Forward switch events to SIEM
- Use firewalls or routers instead of multi
  possible
- Alert new devices, file transfers and RPCs to SIEM
- Store pcaps for a reasonable time, at least on root switches

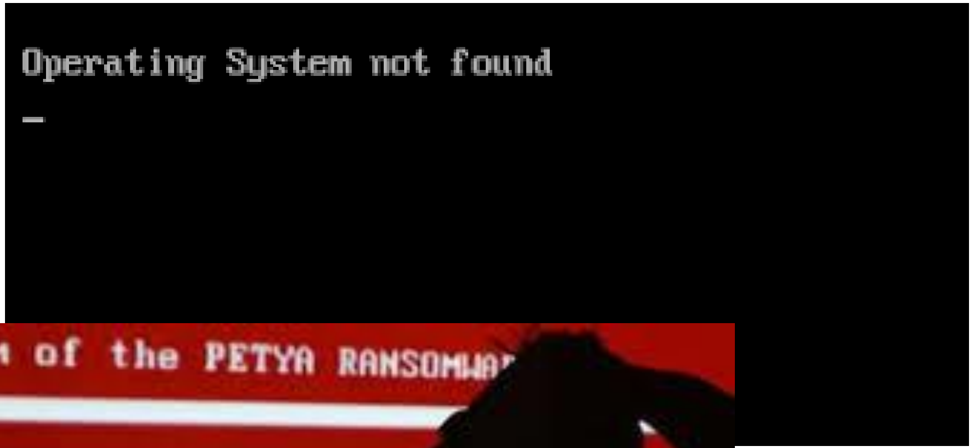
Remote Access

- – Limit Remote Access to specific machines per policy
- – Control traffic with firewall
- – Alert to SIEM on any remote access traffic in the network
- – Use multi-factor authentication
- – Eliminate all dial-up access



Backups

- Regular full backups of all ICS computers stored locally and off site
- Test backup restoration at least annually
- Alert SIEM on failed backups
- Alert on Backup disk full



Transient Assets

– Secure configuration
– Domain group policy enforced
– Minimize third-party software
– Update regularly, then scan with up-to-date antivirus
– Encrypted files are a problem, avoid them
– Physically remove wireless
– Replace regularly

‘Outside’ Vendor Transient Assets

- – Avoid at all reasonable costs
- – Remove HDD and scan with offline tool or use non-Windows bootable disk scan
- – Validate ‘clean’ by multiple methods
- – Once certified, keep in secured area

‘Foreign’ Devices

IEC 61850 Goose

– Isolate by protocol-specific firewalls
– Allow only designed control traffic and no other
– Evaluate and potentially hard-wire connections to critical support equipment
– Firewall any wireless communication
– Monitor all this traffic
– Forward firewall alerts to SIEM
– Alert any periods of lost communication
– Alert any bad (mis-configured) points

Firewalls

- Implement two-layer Next Gen firewalls between ICS and business enterprise networks.
- Use protocol-specific firewalls between ‘foreign’ devices and ICS
- Firewall communication links between disparate ICSs
- Make sure time server is not a common compromise point
- Get an independent peer review of firewall rules
- Perform ‘Red Team’ penetration tests against perimeter firewalls
- Remove icmp (ping) rules once system is stable

Miscellaneous…

- Encrypt system-related data, logic, configurations
- Control access to this data
- Control access to copies of network drawings
- Use controlled encrypted USB devices only
- Wireless devices only connect to a separate ‘untrusted’ network
- Cellular phones (charging…)
- Printers

NOC/SOC Integration

- Enterprise Network Operations teams already have their hands full and generally don’t understand OT
- There is a benefit in tuning a local site SIEM and passing specific crafted alerts on to NOC/SOC
- Test and validate the full circuit for each type of alert. Follow information from source, through monitoring tool, SIEM, intervening firewalls to NOC/SOC
- Decide on and coordinate recommended actions for each type of alert
- Retain the <u>ability</u> to pass all events if necessary

NOC/SOC Integration

- Realize that sending more data puts more information about private networks in the Enterprise realm
- Consider storing packet metadata or full pcaps if possible for analysis in the event of an attack
- Use relay servers so that the data flow path is not a compromise path through Enterprise edge firewalls

Educating OT Personnel

- Administrator account is not your friend
- No free lunch - easy is not usually best
- Understand ‘clean’ and ‘dirty’ with respect to USB devices, laptops and other networking tools.
- Monitor ‘foreigners’ (not a racist statement)
- Uncontrolled trash leads to accidents
- Idle applications are the devils workshop
- The old car wasn’t really better
- If it isn’t physically secure, it isn’t secure at all

Eliminating IT/OT Security Silos

- Approaches are different but objectives are the same.
  - IT, more invasive, multiple discrete apps on each endpoint, performance hits not all important
  - OT, minimal invasion, performance is crucial, only ICS vendor approved apps on endpoints
  - IT, functionality is desirable, but security is supreme
  - OT, safety is supreme, functionality equates to production, security after that
- Shared Goals: Safety, reliability, security, production, open data flow, minimal failures.
- Look for and leverage common concerns
- Learn from IT systems (and people) that are more advanced
- Get CISO sponsorship
- Cross-train individuals

Key Take Aways

- Take action!
- Strong Domain Controllers
- Network Monitoring
- Passwords… Least Privilege
- Up-to-date →2019
- Tested Backups
- Secure Transient Assets
- Buy Secure

"John1234"

Questions?