

Lessons Learned from NERC CIP Applied to the Industrial World

Matt Proctor, Terrence Smith – GE Grid Solutions

2017 Texas A&M Protective Relay Conference

Industrial facilities and the status quo

- Traditionally, there are minimal cyber assets at the plant level.
- DCS Systems, Power Management Systems only occasionally tie into corporate-level networks.
- Sense of security achieved through obscurity and isolation.

NERC – Critical Infrastructure Protection

- NERC develops, implements and enforces mandatory Reliability Standards
- Section 215 of the Federal Power Act
- CIP – addresses cyber assets that are critical to the bulk electrical system.
- **NERC CIP DOES NOT APPLY TO MOST INDUSTRIAL PLANTS!**
- **I AM NOT ADVOCATING TO EXTEND NERC JURISDICTION!**
- **PLEASE PUT AWAY YOUR PITCHFORKS AND TORCHES. I AM NOT ADVOCATING MORE REGULATION!**

Why bring up NERC-CIP at all?

- Bad actors do exist .
 - State-sponsored
 - Organized crime syndicates
 - Activists (both well-intentioned and ill-intentioned)
- They have ways and means to do harm.
 - There are several known threat vectors.
 - As technology is adopted to make life easier, it inevitably increases vulnerabilities.
- They have motivation to do harm.
 - Profit
 - Social upheaval
 - Chaos
- It makes sense to have a plan of action.
- NERC-CIP provides a reference.

NERC-CIP provides a framework.

- **Physical Security of Cyber Systems**
 - CIP-006 – Control, Monitor & Log Physical Access
- **Electronic Security of Cyber Systems**
 - CIP-002 - Identification of Cyber Assets
 - CIP-003 - Documentation of Cyber Security Policies
 - CIP-005 - Electronic Security Perimeter
 - CIP-007 – Ports & Services
 - CIP-009 – Recovery Plan Specifications
- **Personnel Management & Procedures**
 - CIP-004 Cyber Security Training Program
 - CIP-008 Incident Reporting & Response Planning

Who are these Threat Actors?

- State-Sponsored Threats
 - North Korea (Sony)
 - Russia (Ukraine – BlackEnergy)
- Hacktivists
 - Anonymous (Amazon, Paypal, Mastercard, Visa, Power Corporation of Canada, etc. etc. etc..)
 - WikiLeaks (Afghanistan War Logs, DNC)
- Organized Crime
 - Ransomware
 - Corporate espionage
- Agents of Chaos
 - Jason Woodring, convicted Arkansas grid saboteur
- The most dangerous of all, employees (of both disgruntled and happily oblivious varieties).

What are the Threat Vectors?

- Physical Damage
- Cyber Assets
 - “..that if rendered unavailable, degraded, or misused would, with 15 minutes adversely impact [electrical reliability].”
 - Routable Protocols
- People can be Threat Vectors
 - Social Engineering is a technique to manipulate decision making.

Identify Critical Assets

- Can the device directly trip/close critical breakers?
- Can the device start/stop a motor improperly that may cause cascading damage?
- Is this device capable of sending a transfer trip to a different breaker?
- Can a device create unwanted data on a network?

NERC CIP-006 – Physical Security

NERC CIP-006 Addresses Physical Security Perimeter (PSP)

- Key Card Readers
- Motion Sensors
- Security Cameras

NERC CIP-005 – Electronic Secure Perimeter (ESP)

- Equipment communicating with a routable protocol including:
Modbus TCP/IP, DNP/IP, IEC61850 MMS
- Basically, any equipment with an Ethernet port.

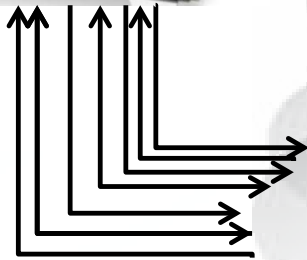
NERC CIP-005 – Electronic Access Point (EAP)

- EAP is a physical device that controls traffic in and out of the ESP.
- EAP can filter data and allow only data that fits the accepted packet structure.
- EAP can whitelist certain MAC addresses, IP addresses.
- EAP can segment data traffic to contain unwanted data.

Cybersecurity Tools - RADIUS

“RADIUS Client”

IP Addr: 192.168.1.200



Establish SSH Connection

Share “secret” (Diffie-Hellman)

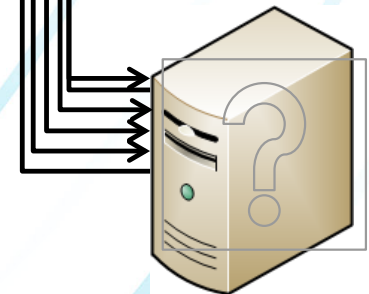
Network

1. Establish SSH Connection & Issue Access Request (includes User Name, Password & Secret).
2. Client Initiates Key Exchange Req.
3. Share secret (Diffie-Hellman exchange)
4. Access Request from Client

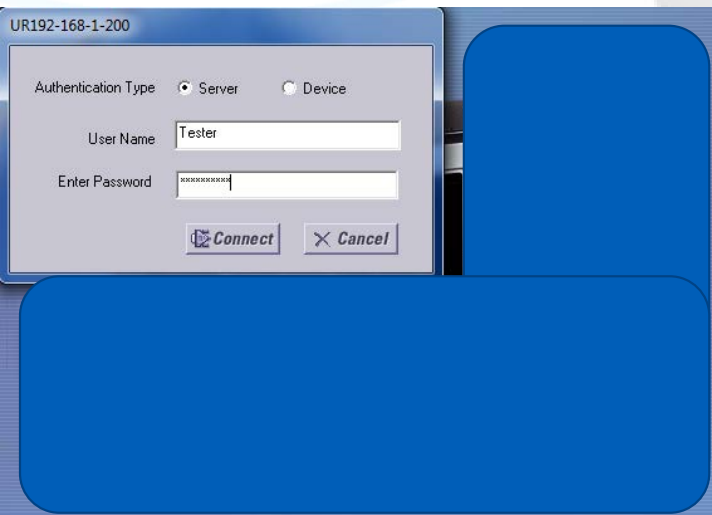
5. Server Issues Access-Challenge
6. Another Access Request from Client
7. Server Checks Authentication Manager
8. Server Responds with Accept or Reject
9. If Accepted, User Continues to Communicate Through SSH.

“RADIUS Server”

IP Addr: 192.168.1.167



Provide Authentication Info to Client

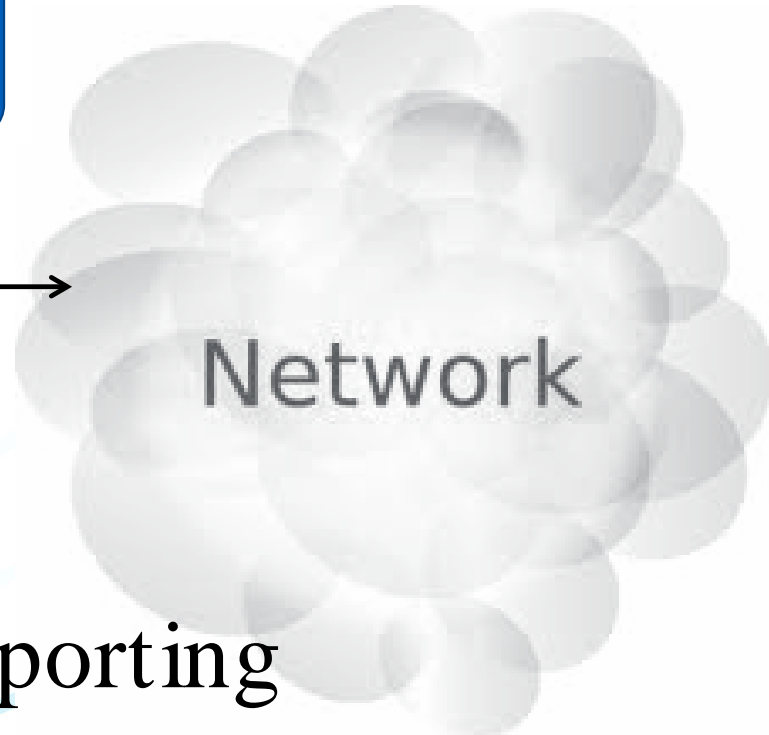
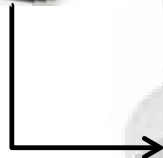


Cybersecurity Tools – Role Based Access

- Administrator – Complete access to settings, commands
- Engineer – Can change settings but not firmware or security settings
- Operator – Can only issue commands but not change other settings
- Observer – Can only read/retrieve info.
- Supervisor – Access role to allow Admin, Engineer privileges.

Cybersecurity Tools - Syslog

IP Addr: 192.168.1.200

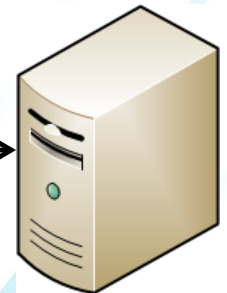


Network



“Syslog Server”

IP Addr: 192.168.1.167



Constant Reporting
Security Audit Trail

NERC CIP – Recovery Plan

- Keep a running log of all cyber assets.
- Keep a copy of all firmware files, settings files.
- Assign people to this function and train them to be capable of performing a complete system “reset”.

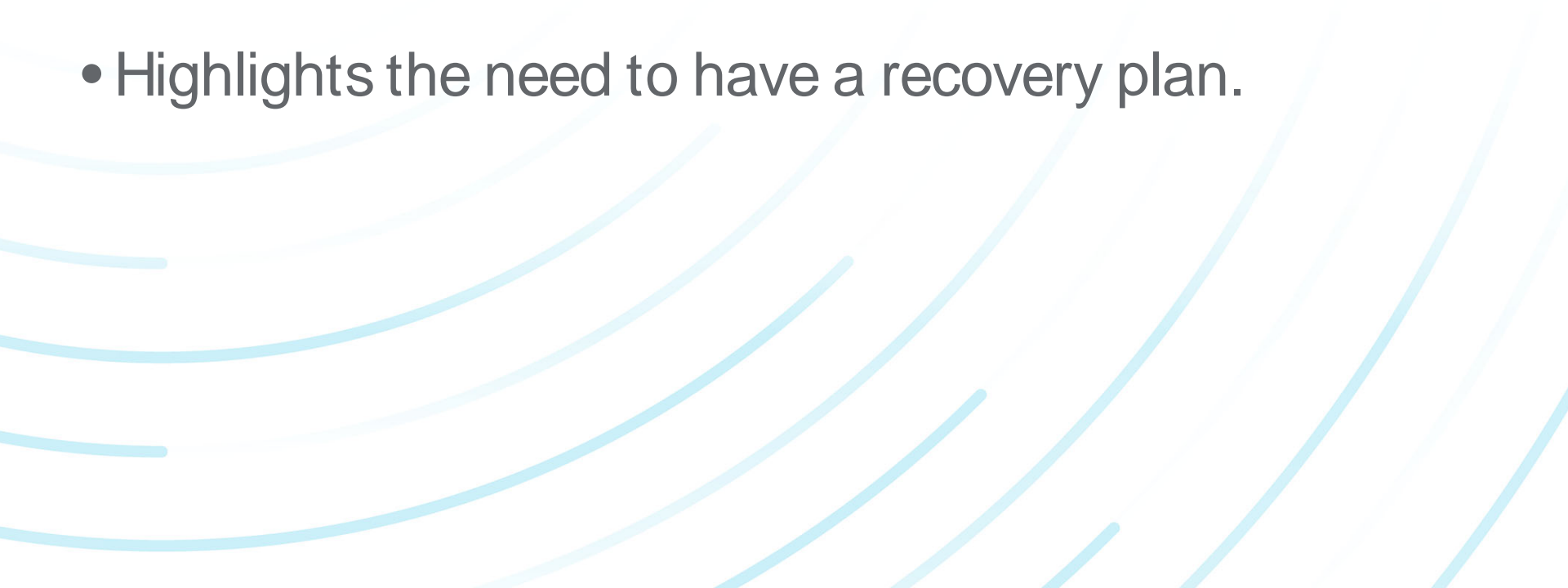
Cautionary Tale #1 - Stuxnet

- First cyber-attack that created physical damage.
- Highlights that “air gapping” is not effective.
- Contractors suspected bogus firmware months prior to the attack. Highlights the value of training personnel to look for signs of attack.

Cautionary Tale #2 – German Steel Mill

- Highlights that “Obscurity” is not a defense.
- Access was gained through “spear-phishing” (official looking attachment).
- Reconnaissance was performed for months prior to attacking. EAP packet sniffing could have helped.

Cautionary Tale #3 – Ukraine Power Grid

- Thirty substations, 225,000 customers affected.
 - Again, phishing and months of reconnaissance.
 - Highlights the need to address known security vulnerabilities.
 - Highlights the need to have a recovery plan.
- 

Conclusions

- If they are not already, networked systems will be used in your plant.
- Obscurity & Isolation are not effective strategies.
- NERC CIP provides a useful reference.
- IED technology developed for NERC CIP compliance can be used to secure cyber-assets, even though you're not legally compelled to use it.

Thank You

Questions?