Securing IEDs against Cyber Threats in Critical Substation Automation and Industrial Control Systems

Eroshan Weerathunga, Anca Cioraca, Mark Adamiak

GE Grid Solutions

MIPSYCON 2017
Introduction

- Threat Landscape
- Tactics in Ukraine Attack and their defense
- Integrating IEDs with security systems
Threat Landscape

Source: The Chertoff Group
Attacks

Copper Theft

Squirrels

PG&E Metcalf substation 2013

Ukraine Cyber Attack 2015, 2016

Stuxnet in 2010
Ukraine Attack

Source: Presentation “Cybersecurity for Energy Delivery Systems” by Michael Assante & Tim Conway
**Tactics in Ukraine Attack**

- Spear Phishing
- Deploy Malware
- Credential Harvesting
- Lateral Movement
- Remote Control
- Malicious firmware uploads

**Defense**

- Spam filtering
- Monthly Phishing test
- Least Privilege
- Malware sandboxing
- Host based Anti Virus
- IDS/IPS system
- Strong Password Policy
- Privileged Identity Management
- Limit admin rights
- Password managers
- Two-factor authentication
- Network segmentation
- SIEM tool
- Device certificates
- Jump Hosts
- Geo-blocking
- Accurate inventories
- Signed firmware & configuration
- Patching
Spear Phishing

WHY PHISHING SCAMS KEEP WORKING

Enter your bank account number.

SCAM.

Source: Dilbert Cartoon
Integrating IEDs with security systems

IED

- SIEM
- RADIUS
- LDAP
- PIM
- Firewall
- IPS/IDS
- KDC
- SYSLOG
- LDAP
- PIM
Intrusion Detection

Change in Bandwidth Usage during Malicious SW Download
Role Based Access Control

- CIP-004-6 R4.3 verify accuracy of all user accounts, user account groups, or user role categories, and associated privileges once every 15 calendar months

- IEC 62351-8 specification defines Role-Based Access Control (RBAC) for enterprise-wide use in power systems, provides a mandatory list of role-to-right mappings

- Role-based access permissions eliminate the need to perform the privilege review on individual user accounts.

- CIP-004-6 R5.2 requires that in the case of reassignments or transfers, the individual’s authorized electronic access is revoked (One implementation is through RADIUS interfacing with Windows Active Directory)
RADIUS server

- Remote Authentication Dial-In User Service (RADIUS)
- Some RADIUS Servers used in utilities
  - Microsoft server 2012 Network Policy Server (MS version of RADIUS)
  - RSA Authentication Manager
  - Juniper Networks Steel-Belted Radius
- RADIUS multiple Authentication methods
### Microsoft Active Directory

#### Active Directory Users and Computers

<table>
<thead>
<tr>
<th>Name</th>
<th>Type</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Administrator</td>
<td>User</td>
<td>Built-in account for administering the computer/domain</td>
</tr>
<tr>
<td>Allowed RODC Passw...</td>
<td>Security Group...</td>
<td>Members in this group can have their passwords replicate...</td>
</tr>
<tr>
<td>Cert Publishers</td>
<td>Security Group...</td>
<td>Members of this group are permitted to publish certificate...</td>
</tr>
<tr>
<td>Cloneable Domain Co...</td>
<td>Security Group...</td>
<td>Members of this group that are domain controllers may be...</td>
</tr>
<tr>
<td>D20MX Administrator</td>
<td>Security Group...</td>
<td>Members of this Group can change security settings</td>
</tr>
<tr>
<td>D20MX Engineer</td>
<td>Security Group...</td>
<td>Members of this Group can change SCADA settings</td>
</tr>
<tr>
<td>D20MX Observer</td>
<td>Security Group...</td>
<td>Members of this Group can only view data</td>
</tr>
<tr>
<td>D20MX Operator</td>
<td>Security Group...</td>
<td>Members of this Group can perform SCADA operations</td>
</tr>
<tr>
<td>Denied RODC Passw...</td>
<td>Security Group...</td>
<td>Members in this group cannot have their passwords replicate...</td>
</tr>
<tr>
<td>DnsAdmins</td>
<td>Security Group...</td>
<td>DNS Administrators Group</td>
</tr>
<tr>
<td>DnsUpdateProxy</td>
<td>Security Group...</td>
<td>DNS clients who are permitted to perform dynamic updat...</td>
</tr>
<tr>
<td>Domain Admins</td>
<td>Security Group...</td>
<td>Designated administrators of the domain</td>
</tr>
<tr>
<td>Domain Computers</td>
<td>Security Group...</td>
<td>All workstations and servers joined to the domain</td>
</tr>
<tr>
<td>Domain Controllers</td>
<td>Security Group...</td>
<td>All domain controllers in the domain</td>
</tr>
<tr>
<td>Domain Guests</td>
<td>Security Group...</td>
<td>All domain guests</td>
</tr>
<tr>
<td>Domain Users</td>
<td>Security Group...</td>
<td>All domain users</td>
</tr>
<tr>
<td>Enterprise Admins</td>
<td>Security Group...</td>
<td>Designated administrators of the enterprise</td>
</tr>
<tr>
<td>Enterprise Read-only Domain</td>
<td>Security Group...</td>
<td>Members of this group are Read-Only Domain Controllers...</td>
</tr>
<tr>
<td>Group Policy Creator</td>
<td>Security Group...</td>
<td>Members in this group can modify group policy for the domain</td>
</tr>
<tr>
<td>Guest</td>
<td>User</td>
<td>Built-in account for guest access to the computer/domain</td>
</tr>
<tr>
<td>RAS and IAS Servers</td>
<td>Security Group...</td>
<td>Servers in this group can access remote access properties ...</td>
</tr>
</tbody>
</table>

- Images and diagrams are used to illustrate the Active Directory configuration and user privileges.
Microsoft Active Directory

![Screenshot of Jim Smith Properties window in Microsoft Active Directory](image)

### Member Of

<table>
<thead>
<tr>
<th>Name</th>
<th>Group Name</th>
</tr>
</thead>
<tbody>
<tr>
<td>D20MX Operator</td>
<td>Active Directory Domain Services Folder</td>
</tr>
<tr>
<td>Domain Users</td>
<td>myutility.com/Users</td>
</tr>
</tbody>
</table>

**Primary group:** Domain Users

There is no need to change Primary group unless you have Macintosh clients or POSIX-compliant applications.
• Extensible Authentication Protocol (EAP)
• RADIUS secure Authentication methods
  EAP-TLS, EAP-TTLS, EAP-PEAP
Lightweight Directory Access Protocol (LDAP) is an application protocol that provides mechanism to connect, search and modify directory.

Using Transport Layer Security (TLS), LDAP can encrypt user sessions between the client and server.
Two-factor authentication

- CIP-005-5 R2.3 requires multi-factor authentication for all Interactive Remote Access sessions
- Multi-factor authentication (MFA): knowledge (something they know), possession (something they have), and inherence (something they are)
- Two-factor authentication: possession (secret token) and knowledge (PIN, Password)
Security Information & Event Logging

- CIP-007-6 R4.1, utilities should Log events at the BES Cyber System level or at the Cyber Asset level (IED level) for identification of, and after-the-fact investigations of, Cyber Security Incidents.

- CIP-007-6 R4.2 requires to generate alerts for security events.

- CIP-007-6 R4.3 requirement, retain applicable event logs for at least the last 90 consecutive calendar days
Syslog

- Syslog protocol is used to transport IED events to a remote Syslog server
- The Priority value = Facility number * 8 + Severity number
- Severity number
  - Informal - 6
  - Warning - 4
  - Error - 3
  - Critical - 2
Privilege Identity Management

• CIP-007-6 R5.6 requires utilities to enforce password changes or an obligation to change the password at least once every 15 calendar months

• PIM focuses solely on managing privileged accounts
• CIP-007-6 R3.1, utilities should deploy method(s) to deter, detect, or prevent malicious code.

• CIP-007-6 R3.2 requires utilities to mitigate threats from detected malicious code.

• CIP-005-5 R1.1 requires to place all applicable Cyber Assets connected to a network via a routable protocol within a defined Electronic Security Perimeter (ESP)

• CIP-005-5 R1.2 requires all External Routable Connectivity through an identified Electronic Access Point (EAP)

• CIP-005-5 R1.3 requires to enforce inbound and outbound access permissions, including the reason for granting access, and deny all other access by default

• CIP-005-5 R1.5 requires utilities to have one or more methods for detecting known or suspected malicious communications for both inbound and outbound communications
Secure Messaging

- Defined in IEC 62351
- Implemented in the IEC Routable GOOSE and Routable Sample Value profiles
- Security Mechanisms:
  - Message Authentication via SHA 256
  - Message Encryption via AES 128
  - "Locked" via Shared Key to a Security Group
R-GOOSE SPDU Signature

SPDU: Session Protocol Data Unit

Signature: “keyed” hash of all items in the SPDU
• In secure R-GOOSE, key management is based upon Group Domain of Interpretation (GDOI).

• GDOI implements the Key Distribution Center function.
• Can we prevent an attack such as Ukraine cyber attack in North America?

• Successful cyber security of a system is a combined effect of technology, procedures, policies, users, monitoring, standard compliance and diligent enforcement

• To secure IEDs, their security features should be enabled and configured properly

• IACS and SAS can achieve required IED cyber security by proper integration of third party security systems with IEDs
Thank You

Questions?