CIP-005-3 – Electronic Security Perimeter (ESP)

- Dan Mishra
FRCC Compliance Workshop
May 09-13, 2011
Purpose

- Specific NERC CIP-005 Requirements
- Underlying fundamentals of the ESP architecture
- Building ESPs using Security Enclaves and DinD
- Electronic Access Control & Monitoring Systems
- Required Controls for Access Points (R2.1 & R2.2)
Disclaimer

- **CAUTION:** Every environment is different and requires a direct correlation. The material contained in this presentation may not represent your corporate or architectural requirements.

- **ADVISORY:** Education, and compliance is about correctly interpreting and conveying information - a requirement for this content.
Terminologies & Abbreviations

- Cyber Asset – Programmable electronic devices and communication networks including hardware, software, and data.
- CCA – Critical Cyber Assets
- ESP – Electronic Security Perimeter
- EACM – Electronic Access Control & Monitoring
- PACS – Physical Access Control Systems
- DinD – Defense in Depth
- DMZ – Demilitarized Zone
- TFE – Technical Feasibility Exceptions
- ACE – Access Control Engine
- Security Enclave – the collection of computing environments connected by one or more internal networks under the control of a single authority and security policy, including personnel and physical security
• Cyber Security – Electronic Security Perimeters: Requires the identification and protection of an electronic security perimeter and access points. The electronic security perimeter (ESP) is to encompass the critical cyber assets identified pursuant to the requirement of CIP-002-3 R3.
Specific NERC CIP-005 Requirements

• The following are exempt from Standard CIP-005:
  – 4.2.2 Cyber Assets associated with communication networks and data communication links between discrete Electronic Security Perimeters.
Specific NERC CIP-005 Requirements

- Requirement 1 - Electronic Security Perimeter
  - Define an ESP and its access points to protect Critical Cyber Assets
- Requirement 2 - Electronic Access Controls
  - Deny by default, Specify explicit permissions
  - Enable only required ports and services
  - Securing dial-up access (Document needed)
  - Documentation - implement and document the organizational processes and technical and procedural mechanisms for control of electronic access
  - Appropriate Use Banner
- Requirement 3 - Monitoring Electronic Access
- Requirement 4 - Cyber Vulnerability Assessment
- Requirement 5 - Documentation Review and Maintenance

- Monitor FERC Order 706 Activity
Specific NERC CIP-005-3 Requirements focused in this presentation –
- R1, Defining ESP(s)
- R1.5, ESP Access Control & Monitoring
- R2, Electronic Access Control
Specific NERC CIP-005 Requirements

• What do we commonly miss?

**R1.5. Cyber Assets used in the access control and/or monitoring of the Electronic Security Perimeter(s) shall be afforded the protective measures** as specified in Standard CIP-003-3; Standard CIP-004-3 Requirement R3; Standard CIP-005-3 Requirements R2 and R3; Standard CIP-006-3 Requirement R3; Standard CIP-007-3 Requirements R1 and R3 through R9; Standard CIP-008-3; and Standard CIP-009-3.

**R2. Electronic Access Controls — The Responsible Entity shall implement and document the organizational processes and technical and procedural mechanisms for control of electronic access at all electronic access points to the Electronic Security Perimeter(s).**
NERC CIP Compliance

Underlying fundamentals of the ESP architecture
Architecting your ESP

- Design and define the ESP to provide the appropriate operating functionality, access control and monitoring capabilities
- Approach, controls, monitoring, assessment and documentation requirements defined in CIP-005 (R2, R3)
- Challenging to define an electronic perimeter around geographically disperse systems collecting information and performing automated and manual control operations
- Define an **ESP and access point, access control request, review and response process and authorization controls** (CIP-005, R2.5, CIP-004, R4)
- Define an appropriate trust model for your systems (Security Enclaves)
- Ensure the adequacy of protection and continued high availability of authorized access and control
- Do not forget documenting (identifying) **the Non-critical Cyber Assets** and Access Control and Monitoring assets used in the access control and/or monitoring of the Electronic Security Perimeter(s)
Integrating ESP

Assess all CIP-005 Requirements then collectively design the solution -

- Understand your organization’s trust model based upon the enclave approach outlined in the methodology
  - Select your identity type, system and appropriate audit trail (logs) collections approach for each ESP enclave
  - Define the appropriate administrative and operational trusts for system access
  - Separate technical administrative, developers, system operators and general users
  - Correlate your physical and cyber identities as appropriate
  - Ensure identity integrity throughout the ESP
Traditional Isolation of Corporate and Control Domains

Figure 1 – Traditional isolation of corporate and control domains

Overview of Contemporary Control System Architectures

Database Attack Vector

Figure 4 – Common architecture zones

Firewall Deployment for Common Security Zones

Figure 5 – Firewalls protecting architecture zones

Defense in Depth with IDS (R??)

Complete defense-in-depth strategy with IDS

Definition: Security Enclaves

• An enclave is, as defined in the Department of Defense Directive (DoDD) 8500.1 E2.1.16.2, “the collection of computing environments connected by one or more internal networks under the control of a single authority and security policy, including personnel and physical security.”

• Terminology Potpourri
  – Security Zones
  – DeMilitarized Zones (DMZ)
  – Transactional Zones

• Determine security controls and define system interactions

• Review NIST SP 800-53 r2; 800-82
Security Enclave Creation

• Security enclaves provide the layers of trusted systems which limit untrusted interactions
• Enclaves creation can be based upon:
  – Mission criticality
  – Dependent Risks
  – Operational requirements
  – Type of application
  – System users
  – Trusted versus untrusted interactions
Enclave Split - Services

• Services are separated among enclaves
• Separation of duties
  – External DNS / Internal DNS
  – External Mail / Internal Mail
  – External Web / Internal Web
  – External Authentication / Internal Authentication
    • Split Active Directory Domains
  – Out Of Band Management Network
  – Application Proxy
Building Security Enclaves

- Defined logical ESP access points with enterprise identity management and network integrated firewalls and IDS.

Legend

- Site-to-Site VPN
- Firewall
- ESP

Restricted WAN

Remote VPN, Contractor, Identity Mgmt, Uncontrolled ISO Enclaves
Office Desktop Systems
ISO, Identity & Event Mgmt Enclaves
Testing Enclaves
Control Enclave
High Availability Virtualized Architecture

IDS/EDS
Cyber Assets used in the access control and/or monitoring of the Electronic Security Perimeter(s) (EACMs) shall be afforded the protective measures as a specified in –
– Standard CIP-003-3;
– Standard CIP-004-3 Requirement R3;
– Standard CIP-005-3 Requirements R2 and R3;
– Standard CIP-006-3 Requirement R3;
– Standard CIP-007-3 Requirements R1 & R3 – R9;
– Standard CIP-008-3;
What is considered as Cyber Assets used in the access control and/or monitoring of the Electronic Security Perimeter(s)?

EACMs are Cyber Assets that can –
1. Controls Access (authenticates / sets privileges) of the ESP
2. Used in monitoring the ESP (logging/recording/alerting)
CIP-005 – R 1.5, Access Control & Monitoring

Protection of Electronic Access Control Systems (EACMs) — Cyber Assets used in the access control and/or monitoring of the Electronic Security Perimeter(s) shall reside within an identified Physical Security Perimeter.

Sister Requirement – Physical Access Control Systems (PACS)
CIP-005 – R2, Access Control & Monitoring

R2. Electronic Access Controls — The Responsible Entity shall **implement and document** the organizational processes and technical and procedural mechanisms for control of electronic access at all electronic access points to the Electronic Security Perimeter(s).

R2.1. These processes and mechanisms shall **use an access control model that denies access by default**, such that **explicit access permissions** must be specified.

R2.2. At all access points to the Electronic Security Perimeter(s), the Responsible Entity shall **enable only ports and services required for operations and for monitoring Cyber Assets within the Electronic Security Perimeter**, and **shall document, individually or by specified grouping, the configuration of those ports and services**.

R2.3. The Responsible Entity **shall implement and maintain a procedure** for securing dial-up access to the Electronic Security Perimeter(s).
R2.4. Where external interactive access into the Electronic Security Perimeter has been enabled, the Responsible Entity shall implement **strong procedural or technical controls at the access points** to ensure **authenticity of the accessing party**, where technically feasible.

R2.5. The required documentation shall, at least, identify and describe:

- The processes for access request and authorization.
- The authentication methods.
- The review process for authorization rights, in accordance with Standard CIP-004-3 Requirement R4.
- The controls used to secure dial-up accessible connections.

R2.6. Appropriate Use Banner — Where technically feasible, **electronic access control devices** shall **display** an **appropriate use banner** on the user screen upon all **interactive access** attempts. The Responsible Entity shall **maintain a document identifying the content of the banner**.
CIP-005 – R 2, Electronic Access Controls

Entity perspective –
1. High Risk Control - It is in Entity’s best interest to secure this control
2. Implementation can be complex

Auditor perspective –
1. Requirement is the level 1/ front-Line defense for the ESP
2. Highest Risk impact if controls are ineffective
3. Takes very long to review these controls as it is time and resources intensive and can vary based on configuration and device technology.
R2.1 – Deny by default Model for Access Control

• CISCO ACE Configuration – Required steps may include

  • Known Communication Between Systems
    – Review levels of system trust for need of isolation station / proxy
    – Define appropriate access rules
    – Identify Source & Destination
    – Identify IP Subnets (IP, Mask)
    – Identify Ports (ranges, gt, lt)

  • Unknown Communication Between Systems
    – Review levels of system trust for need of isolation station / proxy
    – Work with application vendor to identify requirements
    – If necessary, enable connectivity in learning mode

• Do you know who, how, why, where, and when the system communicates across the ESP?
R2.1 – Deny by default Model for Access Control

• CISCO ACE Example

• Good
  - access-list 101 permit tcp host 10.1.1.189 host 172.26.150.205 eq 102
  - access-list 101 permit tcp EMS_Net host 172.26.150.205 object-group EMS_Ports

• Bad (not always wrong)
  - access-list 101 permit tcp host 10.1.1.189 host 172.26.150.205
  - access-list 101 permit tcp host 10.1.1.189 host 172.26.150.0/24 eq 102
  - deny tcp any any

• Ugly
  - Permit tcp any any
R2.2 - Defining Ports and Services Access Rules

R2.2 Requires to enable only ports and services required for operations and for monitoring Cyber Assets within the Electronic Security Perimeter, and shall document, individually or by specified grouping, the configuration of those ports and services.

• Beyond the configuration, Entity documentation to include –
  – Ports or range of ports required for normal or emergency operation (Service/Application, Normal or emergency)
  – Device / Cyber Asset where these application or services are enabled.
  – Since requirement state “only ports”, all other ports communication must be explicitly/implicitly denied.
  – Caution – Routers (Implicit Deny – R3.2)
  – How is CIP-007 R2 different?
R2.2 – Resultant product in Cisco Environment

• What’s the difference?

Network Object Model
hostname (config)# object-group network eng
hostname (config-network)# network-object host 10.1.1.5
hostname (config-network)# network-object host 10.1.1.89
hostname (config)# object-group network Trans
hostname (config-network)# network-object host 10.1.2.8
hostname (config-network)# network-object host 10.1.2.12
hostname (config)# object-group network SysControl
hostname (config-network)# network-object host 10.1.4.89
hostname (config-network)# network-object host 10.1.4.100
hostname (config)# object-group network EMS_Net
hostname (config-network)# group-object eng
hostname (config-network)# group-object Trans
hostname (config-network)# group-object SysControl

object-group service EMS_Ports tcp
port-object eq 102
port-object eq 389
port-object eq 88
port-object eq 543
port-object eq domain
port-object eq 123
port-object eq time
port-object eq 443
port-object eq 22

access-list 101 permit tcp EMS_Net host 172.26.150.205

object-group service EMS_Ports (similar for udp)

Direct ACL Entry
access-list 101 permit tcp host 10.1.1.5 host 172.26.150.205 eq 102
access-list 101 permit tcp host 10.1.1.5 host 172.26.150.205 eq 389
access-list 101 permit tcp host 10.1.1.5 host 172.26.150.205 eq 88
access-list 101 permit tcp host 10.1.1.5 host 172.26.150.205 eq 543
access-list 101 permit tcp host 10.1.1.5 host 172.26.150.205 eq domain
access-list 101 permit tcp host 10.1.1.5 host 172.26.150.205 eq 123
access-list 101 permit tcp host 10.1.1.5 host 172.26.150.205 eq 443
access-list 101 permit tcp host 10.1.1.189 host 172.26.150.205 eq 102
access-list 101 permit tcp host 10.1.1.189 host 172.26.150.205 eq 389
access-list 101 permit tcp host 10.1.1.189 host 172.26.150.205 eq 88
access-list 101 permit tcp host 10.1.1.189 host 172.26.150.205 eq 543
access-list 101 permit tcp host 10.1.1.189 host 172.26.150.205 eq domain
access-list 101 permit tcp host 10.1.1.189 host 172.26.150.205 eq 123
access-list 101 permit tcp host 10.1.1.189 host 172.26.150.205 eq time
access-list 101 permit tcp host 10.1.1.189 host 172.26.150.205 eq 443
access-list 101 permit tcp host 10.1.1.189 host 172.26.150.205 eq 22
• Questions / Discussions