Secure ICCP

Secure ICCP adds Confidentiality, Integrity, and strong authentication to a common protocol

Prepared by LiveData
Secure ICCP Topics

- ICCP Overview
- Non-Secure ICCP Vulnerabilities
- Secure ICCP Overview
- Anatomy of Secure ICCP
- Secure ICCP Setup
- Maintaining Secure ICCP
ICCP Overview

ICCP Network

Utility Control Centers

Power Pools

Regional Control Centers

Non-Utility Generators

Internal Utility Systems

Substations

ICCP is used to exchange data over WANS or LANS between utility control centers and other systems.

The data exchange consists of Real time controls, measurements, scheduling data, energy account data, historical trends and operator messages.

Standard protocol for real-time data exchange within the electric power utilities industry
ICCP Overview

- ICCP, Inter-Control Center Communication Protocol, is also known as TASE.2, Telecontrol Application Service Element 2
- The ICCP standard is defined in IEC documents 60870-6-503, 60870-6-503, and 60870-6-702
- ICCP is an implementation of the Manufacturing Messaging Specification (MMS), ISO 9506.
- MMS resides on layer 7 of the OSI networking model.
- TCP/IP is used as the Network and Transport layers.

<table>
<thead>
<tr>
<th>ISO Layer 7</th>
<th>ICCP TASE.2</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td>MMS</td>
</tr>
<tr>
<td></td>
<td>ACSE</td>
</tr>
<tr>
<td>6</td>
<td>Presentation</td>
</tr>
<tr>
<td>5</td>
<td>Session</td>
</tr>
<tr>
<td>4</td>
<td>Transport</td>
</tr>
<tr>
<td></td>
<td>TCP/IP</td>
</tr>
<tr>
<td>3</td>
<td>Network</td>
</tr>
<tr>
<td>2</td>
<td>Data Link</td>
</tr>
<tr>
<td>1</td>
<td>Physical</td>
</tr>
</tbody>
</table>
Non-Secure ICCP Vulnerabilities

Non-Secure ICCP is an unprotected binary protocol over TCP/IP. As a result it has the typical vulnerabilities including:

- Bypassing Controls
- Integrity Violation
- Intercept/Alter (Man-in-the-middle)
- Spoof
- Masquerade
- Eavesdropping
Secure ICCP Overview

Secure ICCP addresses these typical vulnerabilities:

- SSL/TLS Counter **Bypassing Controls** through strong node to node authentication.

- SSL/TLS’s hashing that is encrypted with the message address protects against **Integrity Violation**, **Intercept/Alter (Man-in-the-middle)**, **Spoof**, and **Masquerade** attacks.

- SSL/TLS encryption provides **Eavesdropping** protection.

- Secure ICCP’s application level certificate provides a counter to **Masquerade** attacks.
Secure ICCP Overview

- Secures ICCP over WANs and Un-Trusted LANs
- Uses SSL/TLS
- Uses Digital Certificates for strong application level authentication

Secure ICCP adds Confidentiality, Integrity, and strong authentication
### Anatomy of Secure ICCP

<table>
<thead>
<tr>
<th>ISO Layer 7</th>
<th>ICCP TASE.2</th>
</tr>
</thead>
<tbody>
<tr>
<td>MMS</td>
<td>ACSE With Certificates</td>
</tr>
<tr>
<td>6</td>
<td>Presentation</td>
</tr>
<tr>
<td>5</td>
<td>Session</td>
</tr>
<tr>
<td>4</td>
<td>Transport</td>
</tr>
<tr>
<td>3</td>
<td>Network</td>
</tr>
<tr>
<td>2</td>
<td>Data Link</td>
</tr>
<tr>
<td>1</td>
<td>Physical</td>
</tr>
</tbody>
</table>

Certificates provide strong authentication

Web Pages that use SSL authenticate user through secret user name and password. Since ICCP is software service, the ACSE certificate provides the end application level authentication

SSL/TLS provides a secure communication channel
Asymmetric Encryption

- Asymmetric Encryption is a key technology used for both Certificates and SSL
- Asymmetric Encryption using a pair of keys, one public and one private.
- Public keys are generally distributed in public key certificates

Items encrypted with the Private key can only be decrypted with the Public key

Items encrypted with the Public key can only be decrypted with the Private key
Certificates

- **Certificates function as digital identification**
  - This is analogous to a passport

- **Certificates are provided by or signed by Certificate Authorities (CA)**
  - To continue the analogy, CAs are like the government issuers of passports

- **Certificates are stored and delivered in files**
  - Established in 1988, most recent version, 3, established in 2002

- **Certificates include the digital signature of the CA**
  - This functions as the water mark on a passport
  - It is signed with the CA’s private key, which can be verified the CA’s public key from CA’s certificate

- **Certificates come in two parts, private and public**
  - The public part contains a public key and is provided to anyone who needs to authenticate you or to decrypt messages from you
  - The private part is kept private and used to encrypted and/or sign messages.
Certificate Trust

Both parties obtain a copy of the CA Certificate, generally through their web site
Both parties obtain Certificates from a Certificate Authority
Each sends their own Certificate to the other party,
Generally through e-mail
Each party validates the other party’s certificate through the CA Certificate
SSL/TLS

- SSL: Secure Sockets layer
- TLS: Transport Layer Security protocol, essentially SSL version 4, January 1999
- Provides a secure communication channel across networks
- Most widely known and used for HTTPS
- Provides for Server and optionally client authentication through X.509 Certificates
- Initiate communication through asymmetric encryption and then continues communication through faster a shared key encryption.
  - The shared key is established during the start up under asymmetric encryption.
Secure ICCP Setup

1. Secure ICCP setup starts with same steps as non-secure ICCP
   a) Plan list of data objects to exchange
   b) Complete ICCP information exchange form which includes the IP Address, OSI, MMS, and ICCP connection parameters
   c) Set up network
   d) Install and configure ICCP node

2. Obtain SSL and ACSE Certificates
   1. Generate a Public Certificate and matching private key
   2. Send Public Certificate to Certificate authority for signing

3. Install Certificates
Maintaining Secure ICCP Connections

- Certificates expire one to three years after they are issued, depending on the certificate. So new certificates must be obtained and installed every one to three years.

- Certificate authorities maintain Certificate Revocation List (CRL) to list certificates that have been compromised. If the certificate in an ICCP connection is compromised it must be replaced.

- General secure ICCP maintenance, adding and removing data objects, is the same as non-secure ICCP
Secure ICCP adds Confidentiality, Integrity, and strong authentication to a common protocol

Questions?