Secure ICCP-TASE.2

Ralph Mackiewicz
SISCO, Inc.
6605 19½ Mile Road
Sterling Heights, MI 48314-1408 USA
Tel: +1-586-254-0020 x103
Fax: +1-586-254-0053
Email: ralph@sisconet.com

General Security Concerns

- Appropriate access to information
- Restriction of control and configuration ability.
- Communication Access Control
- Confidentiality

Background

- Security is just not an ICCP issue:
  - » FTP
  - » Telnet
  - » HTTP
  - » Others….
- For confidentiality (e.g. encryption) the above always uses SSL/TLS. So does ICCP.
  - » IEC wanted to use well understood and supported technology for securing the TC57 protocols:

IEC 62351 – Data and Communication Security

Security Objectives for IEC 62351

- Assuring only Authorized Access even within a closed private network
- Preventing Eavesdropping by non-trusted entities
- Preventing Spoofing/Playback of captured data from non-trusted entities
- Secure and non-secure profiles must be able to co-exist and be unambiguous
- One set of identity management policies required
  - » Same mechanism for all IEC TC57 communications profiles (& DNP3)
- Desire to use mainstream IT methodologies.

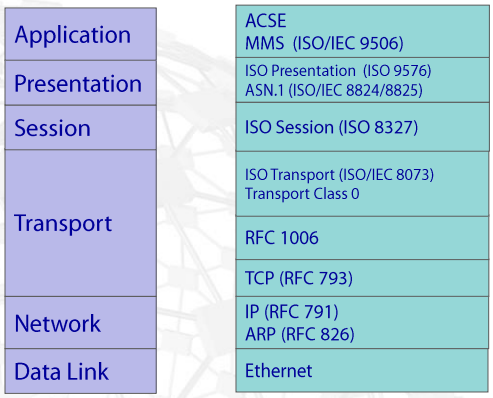
The IEC 62351 Specifications

- IEC 62351-1 Introduction and Overview
- IEC 62351-2 Glossary
- IEC 62351-3 TCP/IP Profile
  - How to use TLS
- IEC 62351-4 Security for MMS based profiles
  - Includes ICCP-TASE.2 annex)
  - References 62351-3
- IEC 62351-5 Security for IEC 60870-5 and derivatives (DNP3)
- IEC 62351-6 Security for 61850
  - References 62351-4
- IEC 62351-7 Mgmt Info. Base (MIB) for end-to-end net. mgmt.
- IEC 62351-8 Role Based Access Control

IEC 62351 – Data and Communications Security

- IEC 62351 specifies only how to use technology to implement security for TC57 protocols.
- It does not specify:
  - What systems need to be secured
  - When to use authentication
  - When to use encryption
  - How to implement role-based access control (coming for IEC 61850)

Profile of concern for ICCP-TASE.2



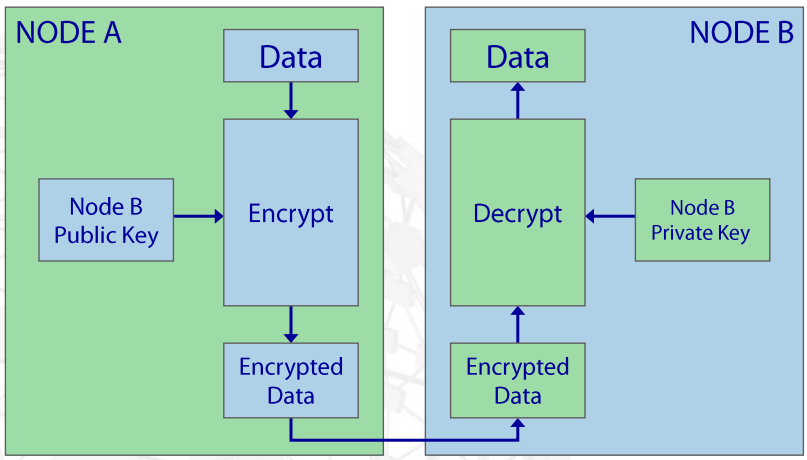
Security Tools

- Encryption
  - » Encrypting data so that only the 2 communicating entities are able to understand the data.
- Authentication
  - » Using digital signatures to ensure that the entity at the other end is known and trusted.

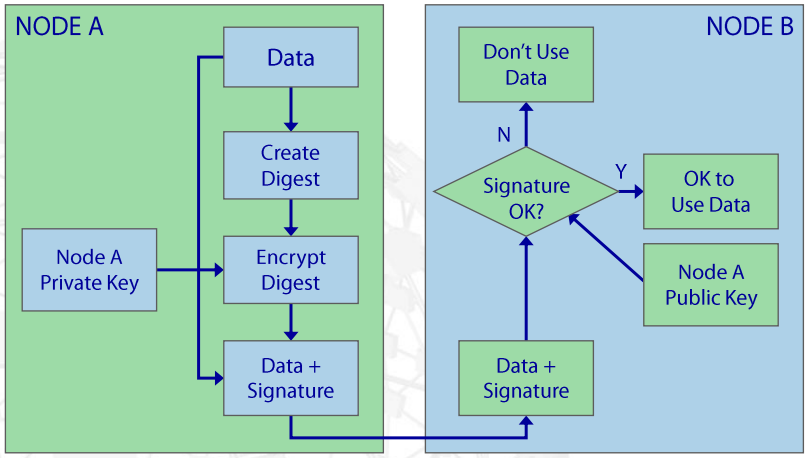
Security Technologies Used

- Public/Private Key Encryption
  - » Transport Layer Security (TLS)
  - » Needed for Confidentiality
- Digital Signatures
  - » Needed to verify authenticity of identification
- X.509 Digital Certificate Technology
  - » Public / Private Key

Public Key Encryption



Digital Signatures



What is a Digital Certificate?

- A digital certificate is a standardized file format that can be exchanged with communications partners that identifies an entity and contains:
  - A public key for encrypting data that can only be decrypted by the private key
  - A unique serial number assigned by the certificate authority
  - Certificate Authority Signature of the Certificate and algorithm used
  - The name of the certificate authority
  - Version of the certificate
  - Validity dates
  - Certificate thumbprint/digest and algorithm used
  - usage, etc.
  - A private key is included for your own certificate that you install on your own machine. **You do not distribute certificates with private keys to others**

What is a Certificate Authority?

- A certificate authority is an entity that issues certificates.
- There is a digital certificate for the CA that includes all the usual certificate information including the CA's public key
- TRUST is a critical element of the CA:
  - » Accepting a CA certificate means that you trust them to verify that the information in certificates issued by them is valid
- **Don't install certificates from CAs into your system you don't trust**

Use of Certificate Authority

- Calculate Digest/thumbprint/fingerprint of the digital certificate
- Compare this to the signature generated by the certificate authority
- If they MATCH AND ***you trust the CA***: the certificate was issued to the entity identified in the certificate by that CA and the public key can be trusted
- If they DON'T MATCH: then something is wrong and you can't trust the certificate or any information in it including the public key.

Certificate Authorities

- Verisign
- Thawte
- Certisign
- Deutche Telecom
- EquiFax
- ANYONE can be a CA

- Important to Utilities
  - » Power Pools
  - » ISOs
  - » RTOs
  - » Your own company

Secure Profile for ICCP-TASE.2

Application	ACSE (ISO/IEC 8650) + **ACSE Authentication Definitions** MMS (ISO/IEC 9506)
Presentation	ISO Presentation (ISO 9576) ASN.1 (ISO/IEC 8824/8825)
Session	ISO Session (ISO 8327)
Transport	ISO Transport (ISO/IEC 8073) Transport Class 0
	RFC 1006
	SSL/TLS
Network	TCP (RFC 793)
	IP (RFC 791) ARP (RFC 826)
Data Link	Logical Link Control (ISO 8802)
	Media Access Control (ISO 8803)

Specification Theory

- TLS is used to supply encryption and node authentication.
  - » Authenticates the identity of the computer running the transport stack, not the applications accessing that stack.
- ACSE is used for Application Authentication.
  - » Authenticates individual applications residing on a given computer.

Security Modes

TLS Encryption	Application Authentication	Use
None	None	Backward Compatible with current implementations
None	Yes	For use over VPN connections or internal to control centers
Yes	No	Provides encryption and node level authentication only.
Yes	Yes	Full security

TLS Encryption

- Asymmetrical Public Key exchange is used to negotiate a secure encrypted connection at the transport level.
  - » Usually relatively high strength keys are used (>256 bit key length)
- In order to minimize overhead, a symmetrical key (both sides use the same encryption key) of a smaller size is then exchanged for continuing communications.

Symmetrical Key Renegotiation

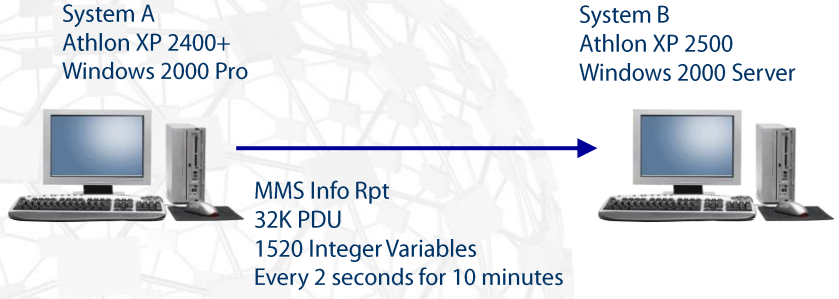
- Maximum of every 5,000 packets (configurable).
- 10 minute time limit (configurable)
- Entity that was connected to (called) responsible for key negotiation.
  - Avoids protocol deadlocking.
- Eliminates possibility of long-term eavesdropping to break the weaker symmetrical keys.

TLS Cipher Suite

- OpenSSL from http://www.openssl.org
- Approximately 40 suites are available in OpenSSL
- Picked a single suite as mandatory to enable interoperability:
  - » TLS_DH_DSS_WITH_AES_256_SHA
- Several don't encrypt and are deprecated

CPU Performance Impact of Encryption

- Implementation specific
- CPU performance related.



Measure Average CPU Utilization

TLS Suite	System A	System B
None	0.425	0.537
AES 256	0.577 (+35%)	0.758 (+41%)
3DES	0.708 (+66%)	0.931 (+73%)
DES	0.597 (+40%)	0.884 (+65%)

Data Transfer Bandwidth Impact of Encryption

- Implementation not expected to have a major impact.

System A
Athlon XP 2400+
Windows 2000 Pro

MMS Reads of 100 Vars
1000 Iterations
Observed with Ethereal

System B
Athlon XP 2500
Windows 2000 Server

Data Transfer Bandwidth Results

	Number of Bytes observed	Percentage Increase
No Encryption	2,693,846	
SSL AES-256	2,742,774	+ 1.18%

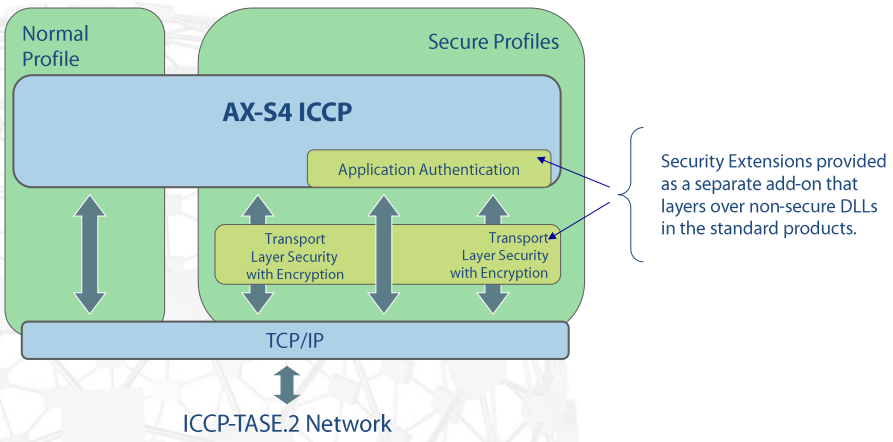
Impact of Application Authentication

- Application Authentication only takes place during association establishment.
- ICCP-TASE.2 consists of long-lived associations
  - » Infrequent application association initiation
- No significant impact on application perfromance or bandwidth for application authentication.
- Minimal impact on application association initiation processing.

SISCO Products Supporting Secure Profiles

- MMS-EASE
  - » Used by large SCADA/EMS OEMs for ICCP-TASE.2
- AX-S4 ICCP
  - » OPC Server for ICCP-TASE.2
- ICCP Lite PLUS+
  - » Source code for ICCP-TASE.2
- MMS Lite
  - » IEC 61850 Source Code

AX-S4 ICCP Security Profile




SISCO
SYSTEMS
INTEGRATION
SPECIALISTS
Thank You
Ralph Mackiewicz
SISCO, Inc.
6605 19½ Mile Road
Sterling Heights, MI 48314-1408 USA
Tel: +1-586-254-0020 x103
Fax: +1-586-254-0053
Email: ralph@sisconet.com
© Copyright 2014 SISCO, Inc.