



# **Securing ICCP-TASE.2 Communications**

Ralph Mackiewicz – SISCO, Inc.  
David Ambrose - WAPA

EMS Users Group 2003 Meeting  
Sacramento, CA  
16 September 2003



## **Agenda**

- Overview of Technology Used
- Secure ICCP Profile
- ICCP Interoperability Testing Results

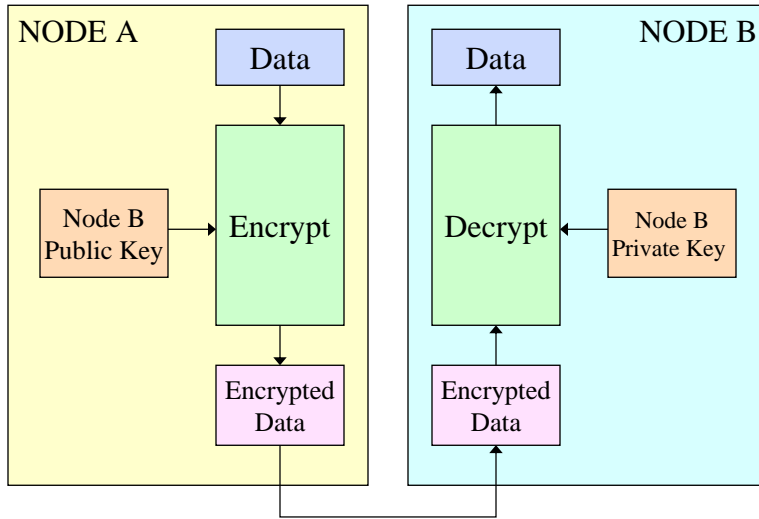
## ICCP Security Objectives

- 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

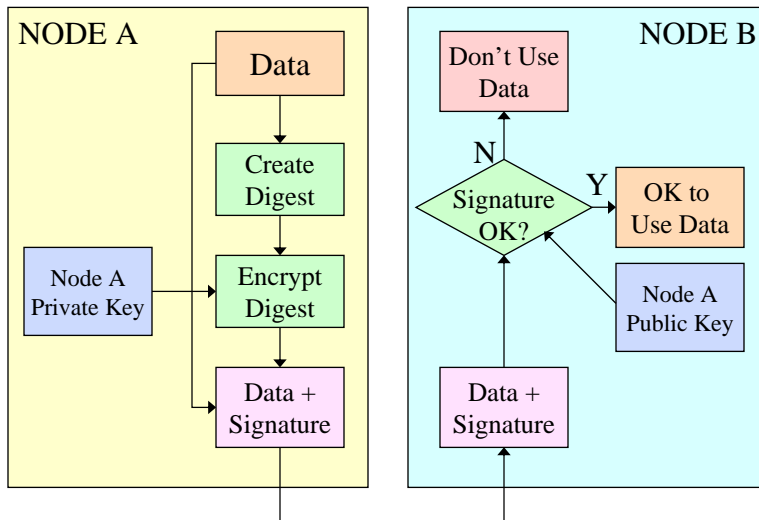
## Security Tools

- 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.

# Public Key Encryption



# Digital Signatures



## Securing ICCP IEC60870-6 TASE.2

- IEC TC57 WG07 (ICCP) adapted recommendations of WG15 (Security).
- Provides both secure and non-secure communications via:
  - Encryption
  - Strong Authentication via Digital Signatures
- EPRI sponsored interoperability testing this summer.

OSI Reference Model

### 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	ISO Transport (ISO/IEC 8073) Transport Class 4
	RFC 1006	SSL/TLS ISO Transport Layer Security (ISO/IEC 10736)
	SSL/TLS	
Network	TCP (RFC 793)	ISO Network (ISO 8473) ES/IS (ISO 9542)
	IP (RFC 791) ARP (RFC 826)	
Data Link	Logical Link Control (ISO 8802)	
	Media Access Control (ISO 8803)	

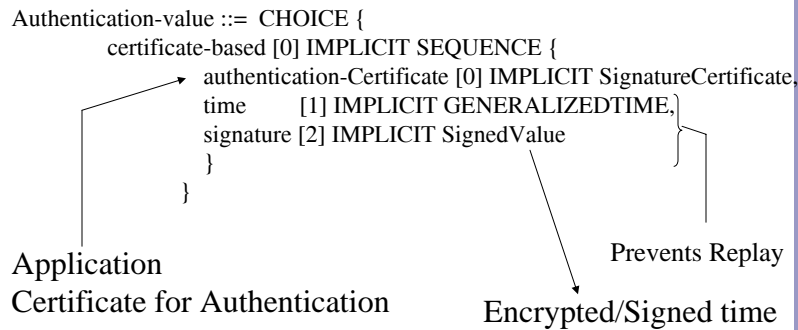
## Specification Theory

- ACSE is used for Application Authentication
- TLS is used to supply encryption

## Different Modes Need to be supported

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

## Application Layer (ACSE) Authentication



Value is sent both ways to authenticate both sides.

## TLS Issues Addressed in Spec

- Deprecation of SSL 1.0 and 2.0 due to known security vulnerabilities.
- Uses TLS 1.0 ::= SSL 3.1
- Deprecation of Cipher Suites that don't do encryptions.
- Transparent key re-negotiation based upon time and number of packets.
- Standardization of support for at least one common Cipher Suite (AES256).
- Specification of TLS Message Authentication

## ICCP 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.

## Cipher Suite

- 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
- Current implementations use OpenSSL

# What does it look like

**-capture- Ethernet**

No.	Time	Source	Destination	Protocol	Info
1	0.000000	192.168.66.30	192.168.66.11	TCP	3790 > 3782 [SYN] Seq=43715322 Ack=0 win=16384 Len=0
2	0.000253	192.168.66.11	192.168.66.30	TCP	3782 > 3790 [SYN, ACK] Seq=1533962997 Ack=43715323 win=17520
3	0.000382	192.168.66.30	192.168.66.11	TCP	3790 > 3782 [ACK] Seq=43715323 Ack=1533962998 win=17520 Len=0
4	0.001111	192.168.66.30	192.168.66.11	SSLV2	Client Hello
5	0.003179	192.168.66.11	192.168.66.30	TLS	Server Hello, Certificate, [Unreassembled Packet]
6	0.003195	192.168.66.11	192.168.66.30	TLS	Continuation data, [Unreassembled Packet]
7	0.003734	192.168.66.30	192.168.66.11	TCP	3790 > 3782 [ACK] Seq=43715393 Ack=1533964901 win=17520 Len=0
8	0.017302	192.168.66.30	192.168.66.11	TLS	Certificate, [Unreassembled Packet]
9	0.017835	192.168.66.30	192.168.66.11	TLS	Continuation data, [Unreassembled Packet]
10	0.017958	192.168.66.30	192.168.66.11	TLS	Continuation data, [Unreassembled Packet]
11	0.018029	192.168.66.11	192.168.66.30	TCP	3782 > 3790 [ACK] Seq=1533964901 Ack=43717441 win=17520 Len=0
12	0.043082	192.168.66.11	192.168.66.30	TLS	Change cipher spec, Encrypted Handshake Message

**-capture- Ethernet**

No.	Time	Source	Destination	Protocol	Info
1	0.000000	192.168.66.30	192.168.66.11	TCP	3790 > 3782 [SYN] Seq=43715322 Ack=0 win=16384 Len=0
2	0.000253	192.168.66.11	192.168.66.30	TCP	3782 > 3790 [SYN, ACK] Seq=1533962997 Ack=43715323 win=17520
3	0.000382	192.168.66.30	192.168.66.11	TCP	3790 > 3782 [ACK] Seq=43715323 Ack=1533962998 win=17520 Len=0
4	0.001111	192.168.66.30	192.168.66.11	SSLV2	Client Hello
5	0.003179	192.168.66.11	192.168.66.30	TLS	Server Hello, Certificate, [Unreassembled Packet]
6	0.003195	192.168.66.11	192.168.66.30	TLS	Continuation data, [Unreassembled Packet]
7	0.003734	192.168.66.30	192.168.66.11	TCP	3790 > 3782 [ACK] Seq=43715393 Ack=1533964901 win=17520 Len=0
8	0.017302	192.168.66.30	192.168.66.11	TLS	Certificate, [Unreassembled Packet]
9	0.017835	192.168.66.30	192.168.66.11	TLS	Continuation data, [Unreassembled Packet]
10	0.017958	192.168.66.30	192.168.66.11	TLS	Continuation data, [Unreassembled Packet]
11	0.018029	192.168.66.11	192.168.66.30	TCP	3782 > 3790 [ACK] Seq=1533964901 Ack=43717441 win=17520 Len=0
12	0.043082	192.168.66.11	192.168.66.30	TLS	Change cipher spec, Encrypted Handshake Message

Frame 5 (1514 bytes on wire, 1514 bytes captured)  
 Ethernet II, Src: 00:0b:db:0a:13:35, Dst: 00:40:f4:70  
 Internet Protocol, Src Addr: 192.168.66.11 (192.168.66.11), Dst Addr: 192.168.66.30  
 Transmission Control Protocol, Src Port: 3782 (3782), Dst Port: 3782 (3782)  
 Secure socket Layer
 

- TLS Record Layer: Server Hello
  - Content Type: Handshake (22)
  - Version: TLS 1.0 (0x0301)
  - Length: 74
- Handshake Protocol: Server Hello
  - Content Type: Handshake (22)
  - Version: TLS 1.0 (0x0301)
  - Length: 1801
- Handshake Protocol: Certificate
  - Handshake Type: Certificate (11)
  - Length: 1797
    - Certificates Length: 1794
    - Certificates (1794 bytes)
      - Certificate Length: 864
      - Certificate (864 bytes)
      - Certificate Length: 924

```

0000 00 00 00 52 0d 0e 09 2a 89 48 89 77 0d 01 01  ..RO...H....
0001 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00  ..G...G...G...
0002 55 53 31 11 30 0f 06 09 55 04 08 13 08 4d 66  US..O...U...M
0003 02 48 69 05 0e 3a 49 29 17 05 01 53 04 07 51  ..H...G...h...
0004 53 74 65 75 0e 3a 49 29 17 05 01 53 04 07 51  ..S...E...M...
0005 7f 21 09 30 0c 06 02 55 04 0a 13 01 53 49 53 49  ..O...U...S...
0006 31 0f 30 04 06 03 55 04 0b 13 50 49 4f 50 55  ..S...E...S...
0007 41 31 13 13 13 0e 03 55 04 03 13 0c 48 63 72  ..A..O...U...M...
0008 02 02 02 02 02 02 02 02 02 02 02 02 02 02 02  ..M...P...R...
0009 86 48 68 17 04 01 00 01 16 11 68 65 75 62 40 78  ..R...e...h...a...
0010 89 75 63 0f 68 63 74 36 63 6f 6d 30 12 17 00 54  ..S...c...o...m...
0011 13 36 37 35 32 30 33 38 31 31 54 17 0d 30 34  ..O...T...S...I...T...
0012 10 37 32 30 32 30 33 38 21 31 54 30 78 31 28 30  ..O...T...S...I...T...
0013 06 05 35 01 31 24 87 43 48 43 53 2c 4c 43  ..E...S...G...E...N...E...R...I...C...C...O...R...P...O...R...A...T...I...O...N...
0014 4c 45 43 54 52 49 43 20 43 4f 52 59 4f 52 41  ..E...L...E...C...T...R...I...C...C...O...R...P...O...R...A...T...I...O...N...
0015 45 4f 46 20 28 87 68 62 68 20 20 82 0e 31  ..F...O...N...C...o...m...p...a...n...y...
0016 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00  ..
    
```



No.	Time	Source	Destination	Protocol	Application
13	0.043921	192.168.66.30	192.168.66.11	TLS	Application
14	0.045116	192.168.66.11	192.168.66.30	TLS	Application
15	0.046148	192.168.66.30	192.168.66.11	TLS	Application

Frame 13 (144 bytes on wire, 144 bytes captured)  
 Ethernet II, Src: 00:40:f4:70:71:cc, Dst: 00:0b:db:0a:13:35  
 Internet Protocol, Src Addr: 192.168.66.30 (192.168.66.30), Dst Addr: 192.168.66.11  
 Transmission Control Protocol, Src Port: 3790 (3790), Dst Port: 3782 (3782), Seq: 11111111, Win: 0, Len: 0  
 Secure Socket Layer

- TLS Record Layer: Application Data
  - Content Type: Application Data (23)
  - Version: TLS 1.0 (0x0301)
  - Length: 32
  - Application Data
- TLS Record Layer: Application Data
  - Content Type: Application Data (23)
  - Version: TLS 1.0 (0x0301)
  - Length: 48

```

0000  00 0b db 0a 13 35 00 40 f4 70 71 cc 08 00 45 00  ....5.@ .pq...E.
0010  00 82 69 9b 40 00 80 06 8b 60 c0 a8 42 1e c0 a8  ..i.@... ..B...
0020  42 0b 0e ce 0e c6 02 9b 13 8e 5b 6e 72 a0 50 18  B..... ..[nr.P.
0030  44 35 3b e7 00 00 17 03 01 00 20 d8 fd a3 8a 37  D5;..... ..7
0040  3c ab 2b 1c 1a 3a cc bb e2 2d ed e8 d1 e5 46 8b  <.+... ..F.
0050  3f ff 90 b8 86 41 e4 6d ca 26 99 17 03 01 00 30  ?....A.m .&....0
0060  6d 0f 02 eb 95 74 4c 83 07 cf 21 64 f3 12 58 f5  m....tL. ..!d.X.
0070  49 37 c6 2d 9d 26 19 82 2f be 38 54 9f dd a8 32  I7;-.&.. /.8T...2
0080  16 50 7d 9e dd 00 3f 76 53 ba 8b 25 45 46 7c 53  .P)...?v S..%EF|S
  
```

# EPRI Interoperability Test

## Description and Results

## IOP Test for ICCP-TASE.2

- Date: 8/12/2003 – Five Participants, 3 observers
  - Participants
    - Alstom
    - GE
    - LiveData
    - Siemens
    - SISCO
  - Observers
    - WAPA
    - SPP
    - NYISO
- Hosted by WAPA
- Sponsored and funded by EPRI

## Tests for TLS IOP

- Client, Server, Combo certificate acceptance.
- Acceptance of Certs from a known CA
- Acceptance of only configured Certs
- Rejection of Certs/connection of unknown CA.
- Rejection of non-configured Certs.
- Key renegotiation
- Cipher-suite negotiation

All test run between pairs where both act as  
Calling and called (18 tests total).

## Tests for ACSE IOP

- Proper certificate acceptance.
- Seal testing (forward and backward time skew)
- Acceptance of only configured Certs
- Invalid calling/called certificates
- Non-configured certificate tests (calling/called)

All test run between pairs where both act as Calling and called (14 tests total).

## Combined Tests

- No security (backward compatibility)
- TLS and ACSE Security enabled.
- Simultaneous Secure/Non-Secure associations.
- Don't Care configuration (accepts any combination).
- ISO/OSI exchange unaffected.

10 tests involved at a minimum.

## Time Estimate for Testing

- Initial estimate was 4-6 hours per pair.
- 10 different test pairs given 5 participating vendors.
- Could not complete all pairs testing due to lack of time.

## IOP Information

ICCP Implementations Tested	MMS, Stack, and Security Implementation Used
Alstom	SISCO
GE	SISCO
LiveData	LiveData
Siemens	SISCO
SISCO	SISCO

## Observers

Dave Ambrose  
(WAPA)

Glenn Sheffer  
(NYISO)

Kevin Perry  
(SPP)



## Test Coordinators

- Herbert Falk (SISCO)
- Dave Becker (EPRI)
  - EPRI funded the specification development and sponsored the IOP.

## Security Isn't Only a Stack Issue

- Applications (e.g. ICCP) interact and make decisions on security.
  - Found IOP issues with ICCP (non-secure/secure)
    - Database issues
    - Bi-directional vs. Single direction associations
- Found:
  - Database issues
    - Same VCC Data Values (DVs) being sourced by both ends of the testing.
    - Non-configuration of extended type DVs.
    - Access control configuration issues for VCC level DVs accessed by multiple remotes.

## Critical Issues Found

- ACSE
  - Malformed encodings of ACSE Authentication values (corrected).
  - Specification issue in regards to specification of digital signature (corrected).

## Critical Issues Found

- Use of ACSE certificates exposed a conformance issue in the session layer (corrected).
  - This would have been almost impossible to find in the field (took 6 hours during IOP test).

## Problem Resolution

- Problems were diagnosed
- Corrected
- Consumed 11-14 hours of IOP time.
- Caused other vendors to re-execute some tests.

## General Test Results

	Alstom	GE	LiveData	Siemens	SISCO
Alstom <sup>(1)</sup>		Passed	Passed	Passed	Passed
GE	Passed		Passed	Passed	Passed
LiveData <sup>(2)</sup>	Passed	Passed		TLS only <sup>(3)</sup>	Passed
Siemens <sup>(1)</sup>	Passed	Passed	TLS only <sup>(3)</sup>		Passed
SISCO	Passed	Passed	Passed	Passed	

(1) - ICCP DB configuration issue (did not affect interoperability)

(2) - Some TLS test cases skipped

(3) - Complete suite not executed due to lack of time

## Other lessons learned

- Tool set needs to be augmented
- Participants gained an understanding of how to configure and debug secure implementations.
- Determined need to take IOP tests and construct a guide for deployment/FAT.

## Lessons Learned

- Attempt to perform testing in advance (over Internet) failed.
  - IT staffs would not open up required ports.
- Calling and called testing was critical to finding certain issues.

## Observer Tools

- Kema UniCA analyzer
  - Provided MMS/ICCP decoding and association setup/dataset transfer validation
  - Did not display SSL/TLS exchanges.
  - Gave inaccurate decodes when decoding the ACSE Authentication and certificates. (has been updated since testing occurred)
- Ethereal
  - Able to observe/display SSL/TLS exchanges.
  - Does not decode above transport (e.g. no MMS/ICCP decoding).
  - Became an integral tool for the observers.
  - Available from [www.ethereal.com](http://www.ethereal.com)

## Summary

- IOP was successful
- Problems with implementations were found and corrected.
- Specification was enhanced to be more precise.
- Observers were satisfied with the overall test, test methodology, and results.

## What's Next

- EPRI specification is being used as the basis for three (3) IEC New Work Item Proposals (NWIP) within IEC TC57 WG15.
- NERC DEWG will address deployment requirements at its November meeting.

# Thank You

Ralph Mackiewicz  
SISCO, Inc.  
6605 19½ Mile Road  
Sterling Heights, MI 48314 USA  
Tel: +586-254-0020  
Fax: +586-254-0053  
E-Mail: ralph@siskonet.com

David Ambrose  
WAPA  
5555 E. Crossroads Blvd.  
Mail Code: J4010  
Loveland, CO 80538-8986  
Phone: 970-461-7354  
Fax: 970-490-7213  
E-Mail: ambrose@wapa.gov