
ICAO • OACI • ИКАО
国际民航组织 • ايكاو
INTERNATIONAL
CIVIL AVIATION
ORGANIZATION

AFS to SWIM Transition Task Force (AST TF)

SEVENTH MEETING

AMHS SECURITY WORKSHOP

(Dubrovnik, Croatia, 21-24 April 2026)

Leonardo de Vida

Copperchase

Topics

- ✓ The current AMHS Security Environment
- ✓ Use of Wireshark to examine a bind operation
- ✓ X.400 P1 bind operations
- ✓ X.400 P3 bind operations

The current AMHS Security Environment

- ✓ Before we discuss how to improve the current AMHS Security we need to analyse the current situation
- ✓ The phrase “AMHS Security” is too generic
- ✓ We are not taken into consideration things like VPNs
- ✓ We will focus on the establishment of connection used by the X.400 protocols
- ✓ Hopefully, this will highlight the current risks and limitations

P1
Connections

An example of X.400 P1 MTA Binds

- ✓ An X.400 MTA connects to other X.400 MTA using the X.400 P1 protocol
- ✓ To open an X.400 P1 connection, the initiating MTA send an MTA Bind
- ✓ The MTA Bind operation can be Simple or Strong
- ✓ Currently, most (or all?) X.400 MTAs used in AMHS use Simple binds

MTA Bind - Simple

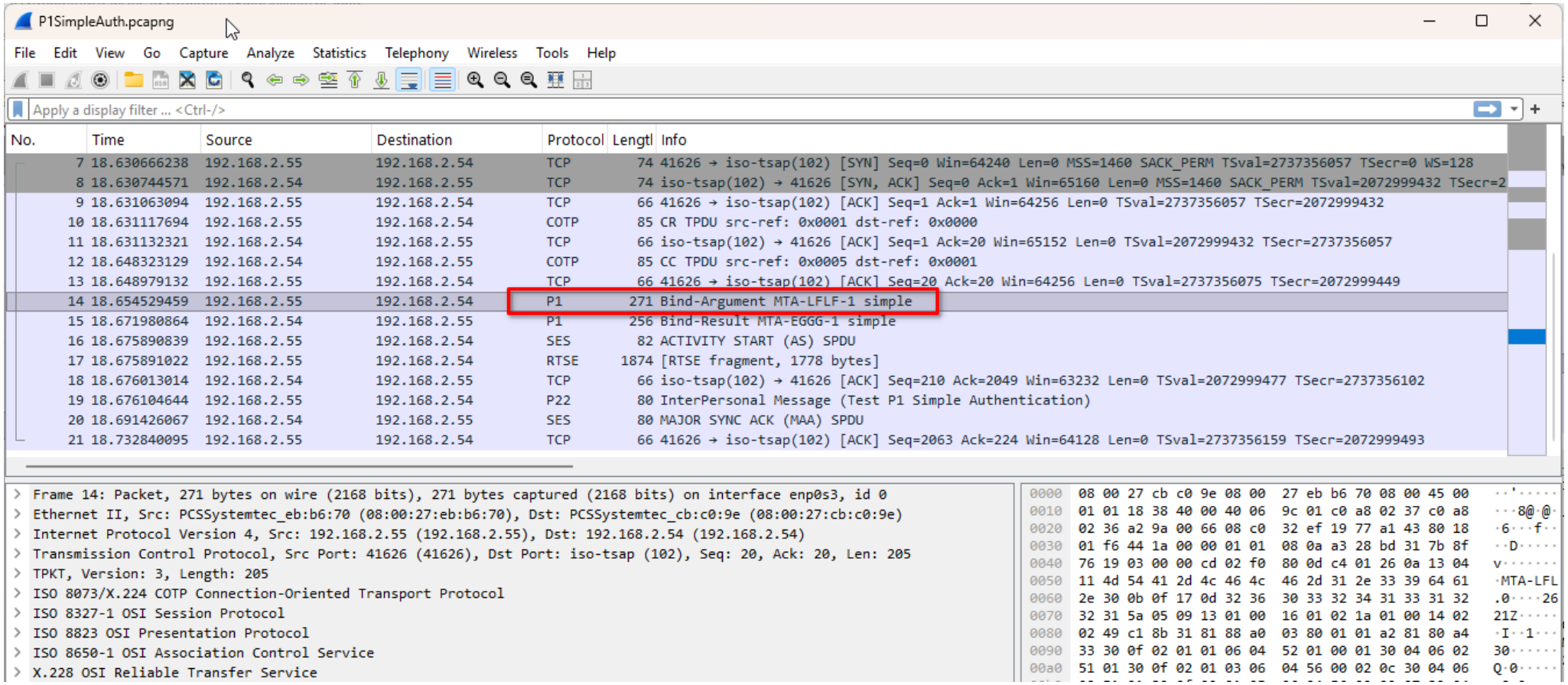
- ✓ A Simple MTA Bind can be considered to consist of a username and password
- ✓ In a following session, the MTA Bind operation will be covered in more detail
- ✓ In the meantime, the MTA Bind operation uses an MTSBindArgument
- ✓ In X.400 terms, the MTSBindArgument contains
  - ✓ The initiator-name, i.e. the MTA Name of the initiating MTA
  - ✓ The initiator-credentials, i.e. a password assigned to the MTA by the administrator

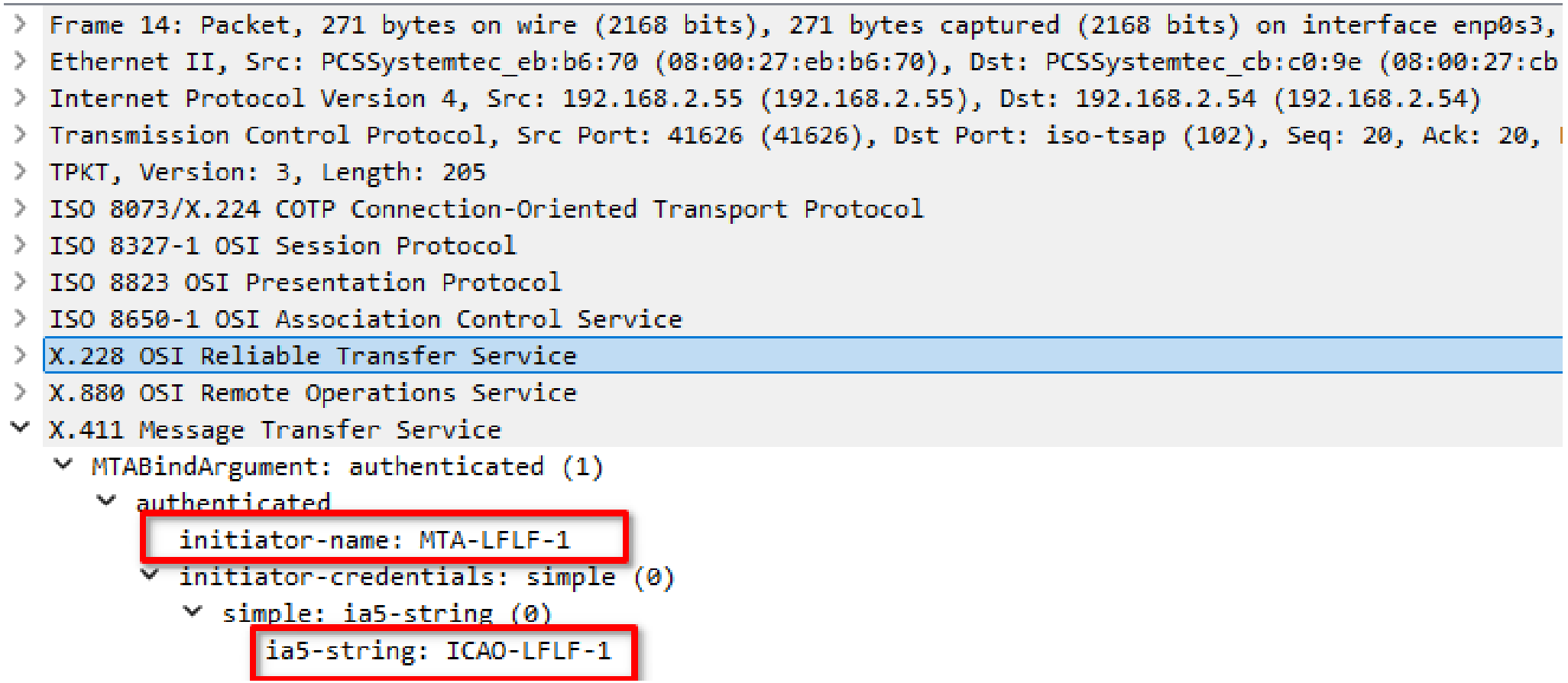
Issues with MTA Bind – Simple

- ✓ The information in the MTSBindArgument is transmitted over the network **without encryption**
- ✓ Anyone who can monitor a network, can therefore see the credentials
- ✓ We will examine a couple of X.400 connection examples using Wireshark

Wireshark

- ✓ Wireshark is a free and open-source packet analyser
- ✓ The next screen shots are taken from Wireshark
- ✓ They contain an X.400 P1 and P3 MTA Bind operations and the corresponding results

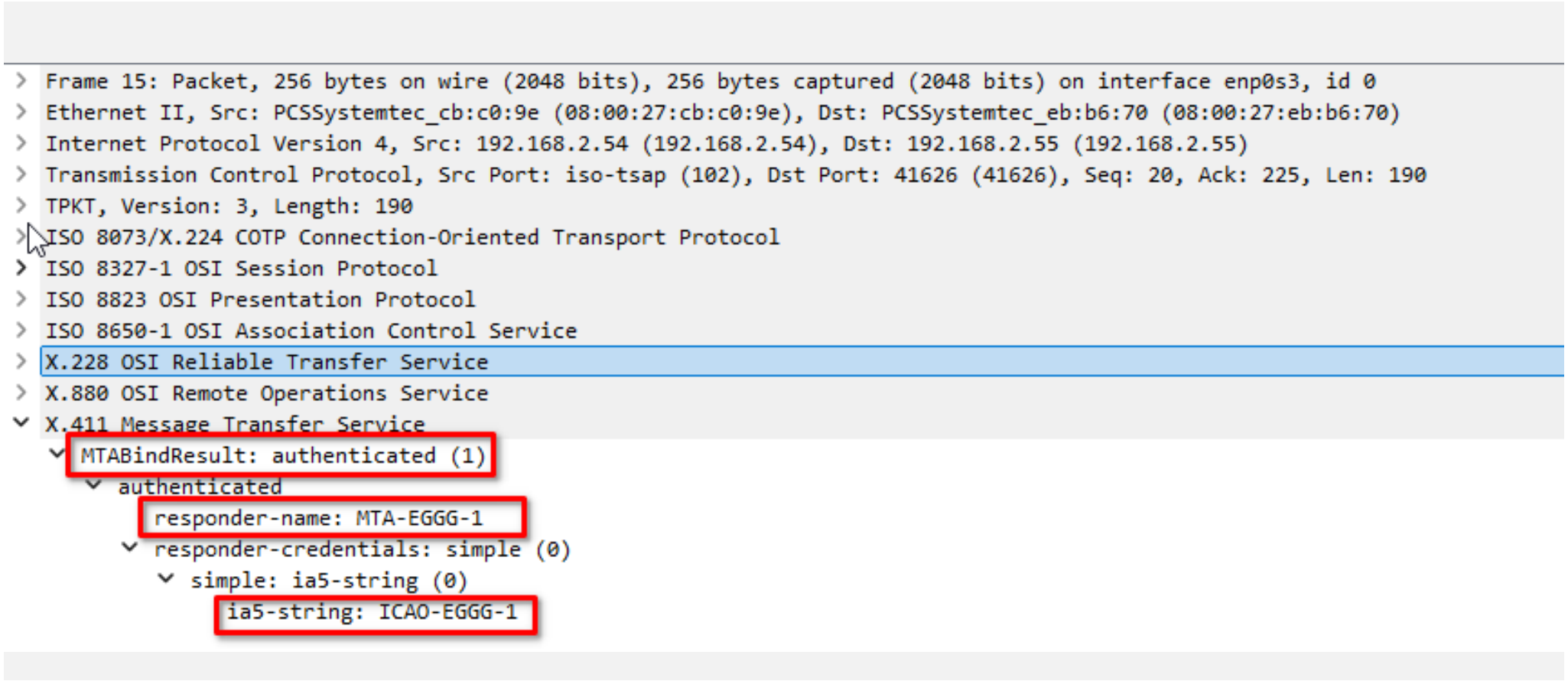

P1SimpleAuth.pcapng
File Edit View Go Capture Analyze Statistics Telephony Wireless Tools Help
Apply a display filter ... <Ctrl-/>
No. Time Source Destination Protocol Lengtl Info
7 18.630666238 192.168.2.55 192.168.2.54 TCP 74 41626 → iso-tsap(102) [SYN] Seq=0 Win=64240 Len=0 MSS=1460 SACK_PERM TSval=2737356057 TSecr=0 WS=128
8 18.630744571 192.168.2.54 192.168.2.55 TCP 74 iso-tsap(102) → 41626 [SYN, ACK] Seq=0 Ack=1 Win=65160 Len=0 MSS=1460 SACK_PERM TSval=2072999432 TSecr=2
9 18.631063094 192.168.2.55 192.168.2.54 TCP 66 41626 → iso-tsap(102) [ACK] Seq=1 Ack=1 Win=64256 Len=0 TSval=2737356057 TSecr=2072999432
10 18.631117694 192.168.2.55 192.168.2.54 COTP 85 CR TPDU src-ref: 0x0001 dst-ref: 0x0000
11 18.631132321 192.168.2.54 192.168.2.55 TCP 66 iso-tsap(102) → 41626 [ACK] Seq=1 Ack=20 Win=65152 Len=0 TSval=2072999432 TSecr=2737356057
12 18.648323129 192.168.2.54 192.168.2.55 COTP 85 CC TPDU src-ref: 0x0005 dst-ref: 0x0001
13 18.648979132 192.168.2.55 192.168.2.54 TCP 66 41626 → iso-tsap(102) [ACK] Seq=20 Ack=20 Win=64256 Len=0 TSval=2737356075 TSecr=2072999449
14 18.654529459 192.168.2.55 192.168.2.54 P1 271 Bind-Argument MTA-LFLF-1 simple
15 18.671980864 192.168.2.54 192.168.2.55 P1 256 Bind-Result MTA-EGGG-1 simple
16 18.675890839 192.168.2.55 192.168.2.54 SES 82 ACTIVITY START (AS) SPDU
17 18.675891022 192.168.2.55 192.168.2.54 RTSE 1874 [RTSE fragment, 1778 bytes]
18 18.676013014 192.168.2.54 192.168.2.55 TCP 66 iso-tsap(102) → 41626 [ACK] Seq=210 Ack=2049 Win=63232 Len=0 TSval=2072999477 TSecr=2737356102
19 18.676104644 192.168.2.55 192.168.2.54 P22 80 InterPersonal Message (Test P1 Simple Authentication)
20 18.691426067 192.168.2.54 192.168.2.55 SES 80 MAJOR SYNC ACK (MAA) SPDU
21 18.732840095 192.168.2.55 192.168.2.54 TCP 66 41626 → iso-tsap(102) [ACK] Seq=2063 Ack=224 Win=64128 Len=0 TSval=2737356159 TSecr=2072999493
Frame 14: Packet, 271 bytes on wire (2168 bits), 271 bytes captured (2168 bits) on interface enp0s3, id 0
Ethernet II, Src: PCSSystemtec_eb:b6:70 (08:00:27:eb:b6:70), Dst: PCSSystemtec_cb:c0:9e (08:00:27:cb:c0:9e)
Internet Protocol Version 4, Src: 192.168.2.55 (192.168.2.55), Dst: 192.168.2.54 (192.168.2.54)
Transmission Control Protocol, Src Port: 41626 (41626), Dst Port: iso-tsap (102), Seq: 20, Ack: 20, Len: 205
TPKT, Version: 3, Length: 205
ISO 8073/X.224 COTP Connection-Oriented Transport Protocol
ISO 8327-1 OSI Session Protocol
ISO 8823 OSI Presentation Protocol
ISO 8650-1 OSI Association Control Service
X.228 OSI Reliable Transfer Service
0000 08 00 27 cb c0 9e 08 00 27 eb b6 70 08 00 45 00
0010 01 01 18 38 40 00 40 06 9c 01 c0 a8 02 37 c0 a8
0020 02 36 a2 9a 00 66 08 c0 32 ef 19 77 a1 43 80 18
0030 01 f6 44 1a 00 00 01 01 08 0a a3 28 bd 31 7b 8f
0040 76 19 03 00 00 cd 02 f0 80 0d c4 01 26 0a 13 04
0050 11 4d 54 41 2d 4c 46 4c 46 2d 31 2e 33 39 64 61
0060 2e 30 0b 0f 17 0d 32 36 30 33 32 34 31 33 31 32
0070 32 31 5a 05 09 13 01 00 16 01 02 1a 01 00 14 02
0080 02 49 c1 8b 31 81 88 a0 03 80 01 01 a2 81 80 a4
0090 33 30 0f 02 01 01 06 04 52 01 00 01 30 04 06 02
00a0 51 01 30 0f 02 01 03 06 04 56 00 02 0c 30 04 06


Frame 14: Packet, 271 bytes on wire (2168 bits), 271 bytes captured (2168 bits) on interface enp0s3,
Ethernet II, Src: PCSSystemtec_eb:b6:70 (08:00:27:eb:b6:70), Dst: PCSSystemtec_cb:c0:9e (08:00:27:cb
Internet Protocol Version 4, Src: 192.168.2.55 (192.168.2.55), Dst: 192.168.2.54 (192.168.2.54)
Transmission Control Protocol, Src Port: 41626 (41626), Dst Port: iso-tsap (102), Seq: 20, Ack: 20,
TPKT, Version: 3, Length: 205
ISO 8073/X.224 COTP Connection-Oriented Transport Protocol
ISO 8327-1 OSI Session Protocol
ISO 8823 OSI Presentation Protocol
ISO 8650-1 OSI Association Control Service
X.228 OSI Reliable Transfer Service
X.880 OSI Remote Operations Service
X.411 Message Transfer Service
MTABindArgument: authenticated (1)
authenticated
initiator-name: MTA-LFLF-1
initiator-credentials: simple (0)
simple: ia5-string (0)
ia5-string: ICAO-LFLF-1

```
 7 18.630666238  192.168.2.55  192.168.2.54  TCP      74 41626 → iso-tsap(102) [SYN] Seq=0 Win=64240 Len=0 MSS=1460 SACK_PERM TSval=2737356057 TSecr=0 WS=128
 8 18.630744571  192.168.2.54  192.168.2.55  TCP      74 iso-tsap(102) → 41626 [SYN, ACK] Seq=0 Ack=1 Win=65160 Len=0 MSS=1460 SACK_PERM TSval=2072999432 TSecr=2
 9 18.631063094  192.168.2.55  192.168.2.54  TCP      66 41626 → iso-tsap(102) [ACK] Seq=1 Ack=1 Win=64256 Len=0 TSval=2737356057 TSecr=2072999432
10 18.631117694  192.168.2.55  192.168.2.54  COTP     85 CR TPDU src-ref: 0x0001 dst-ref: 0x0000
11 18.631132321  192.168.2.54  192.168.2.55  TCP      66 iso-tsap(102) → 41626 [ACK] Seq=1 Ack=20 Win=65152 Len=0 TSval=2072999432 TSecr=2737356057
12 18.648323129  192.168.2.54  192.168.2.55  COTP     85 CC TPDU src-ref: 0x0005 dst-ref: 0x0001
13 18.648979132  192.168.2.55  192.168.2.54  TCP      66 41626 → iso-tsap(102) [ACK] Seq=20 Ack=20 Win=64256 Len=0 TSval=2737356075 TSecr=2072999449
14 18.654529459  192.168.2.55  192.168.2.54  P1      271 Bind-Argument MTA-LFLF-1 simple
15 18.671980864  192.168.2.54  192.168.2.55  P1      256 Bind-Result MTA-EGGG-1 simple
16 18.675890839  192.168.2.55  192.168.2.54  SES      82 ACTIVITY START (AS) SPDU
17 18.675891022  192.168.2.55  192.168.2.54  RTSE   1874 [RTSE fragment, 1778 bytes]
18 18.676013014  192.168.2.54  192.168.2.55  TCP      66 iso-tsap(102) → 41626 [ACK] Seq=210 Ack=2049 Win=63232 Len=0 TSval=2072999477 TSecr=2737356102
19 18.676104644  192.168.2.55  192.168.2.54  P22      80 InterPersonal Message (Test P1 Simple Authentication)
```

```
> Frame 15: Packet, 256 bytes on wire (2048 bits), 256 bytes captured (2048 bits) on interface enp0s3, id 0
> Ethernet II, Src: PCSSystemtec_cb:c0:9e (08:00:27:cb:c0:9e), Dst: PCSSystemtec_eb:b6:70 (08:00:27:eb:b6:70)
> Internet Protocol Version 4, Src: 192.168.2.54 (192.168.2.54), Dst: 192.168.2.55 (192.168.2.55)
> Transmission Control Protocol, Src Port: iso-tsap (102), Dst Port: 41626 (41626), Seq: 20, Ack: 225, Len: 190
> TPKT, Version: 3, Length: 190
> ISO 8073/X.224 COTP Connection-Oriented Transport Protocol
> ISO 8327-1 OSI Session Protocol
> ISO 8823 OSI Presentation Protocol
> ISO 8650-1 OSI Association Control Service
> X.228 OSI Reliable Transfer Service
> X.880 OSI Remote Operations Service
v X.411 Message Transfer Service
  v MTABindResult: authenticated (1)
    v authenticated
        responder-name: MTA-EGGG-1
      v responder-credentials: simple (0)
        v simple: ia5-string (0)
            ia5-string: ICAO-EGGG-1
```

```
0000  08 00 27 eb b6 70 08 00  27 cb c0 9e 08 00 45 00   ··'··p··  '·····E·
0010  00 f2 f0 43 40 00 40 06  c4 04 c0 a8 02 36 c0 a8   ···C@·@·  ·····6··
0020  02 37 00 66 a2 9a 19 77  a1 43 08 c0 33 bc 80 18   ·7·f···w  ·C··3···
0030  01 fc 86 a2 00 00 01 01  08 0a 7b 8f 76 31 a3 28   ········  ··{·v1·(
0040  bd 31 03 00 00 be 02 f0  80 0e b5 01 26 09 13 04   ·1······  ····&···
0050  11 4d 54 41 2d 4c 46 4c  46 2d 31 2e 33 39 64 61   ·MTA-LFL  F-1.39da
0060  2e 30 0b 0f 17 0d 32 36  30 33 32 34 31 33 31 32   .0····26  0324131312
0070  32 31 5a 05 09 13 01 00  16 01 03 1a 01 00 14 02   21Z·····  ········
0080  02 49 34 00 c1 7a 31 78  a0 03 80 01 01 a2 71 a5   ·I4··z1x  ····q·
0090  1b 30 07 80 01 00 81 02  51 01 30 07 80 01 00 81   ·0·····  Q·0·····
00a0  02 51 01 30 07 80 01 00  81 02 51 01 61 52 30 50   ·Q·0····  ··Q·aR0P
00b0  02 01 01 a0 4b 61 49 a1  06 06 04 56 00 01 06 a2   ····KaI·  ···V····
00c0  03 02 01 00 a3 05 a1 03  02 01 00 be 33 28 31 06   ········  ····3(1·
00d0  02 51 01 02 01 03 a0 28  b1 26 80 01 3f a2 21 a0   ·Q·····(  ·&··?·!·
00e0  1f b1 1d a1 1b 80 0a 4d  54 41 2d 45 47 47 47 2d   ·······M  TA-EGGG-
00f0  31 a1 0d 16 0b 49 43 41  4f 2d 45 47 47 47 2d 31   1····ICA  O-EGGG-1
```


Frame 15: Packet, 256 bytes on wire (2048 bits), 256 bytes captured (2048 bits) on interface enp0s3, id 0
Ethernet II, Src: PCSSystemtec_cb:c0:9e (08:00:27:cb:c0:9e), Dst: PCSSystemtec_eb:b6:70 (08:00:27:eb:b6:70)
Internet Protocol Version 4, Src: 192.168.2.54 (192.168.2.54), Dst: 192.168.2.55 (192.168.2.55)
Transmission Control Protocol, Src Port: iso-tsap (102), Dst Port: 41626 (41626), Seq: 20, Ack: 225, Len: 190
TPKT, Version: 3, Length: 190
ISO 8073/X.224 COTP Connection-Oriented Transport Protocol
ISO 8327-1 OSI Session Protocol
ISO 8823 OSI Presentation Protocol
ISO 8650-1 OSI Association Control Service
X.228 OSI Reliable Transfer Service
X.880 OSI Remote Operations Service
X.411 Message Transfer Service
MTABindResult: authenticated (1)
authenticated
responder-name: MTA-EGGG-1
responder-credentials: simple (0)
simple: ia5-string (0)
ia5-string: ICAO-EGGG-1

Potential risks of the current procedures

- ✓ The example shown corresponds to an MTA connecting to another MTA using P1
- ✓ The problem will be the similar for X.400 P3 and X.400 P7 connections
- ✓ If a potential attacker got hold of the connection information, it could impersonate an AMHS MTA
- ✓ So, an attacker could impersonate an AMHS Com Centre and therefore it could:
  - ✓ Receive messages that will not be delivered to the real AMHS Com Centre
  - ✓ Send false messages to the other AMHS Com Centre

P3
Connections

An example of X.400 P3 MTA Binds

- ✓ An AMHS User Agent that uses X.400 P3 connects to the MTA using an MTA Bind operation
- ✓ The MTA Bind operation can be Simple or Strong
- ✓ Currently, most (or all?) AMHS User Agents use Simple binds

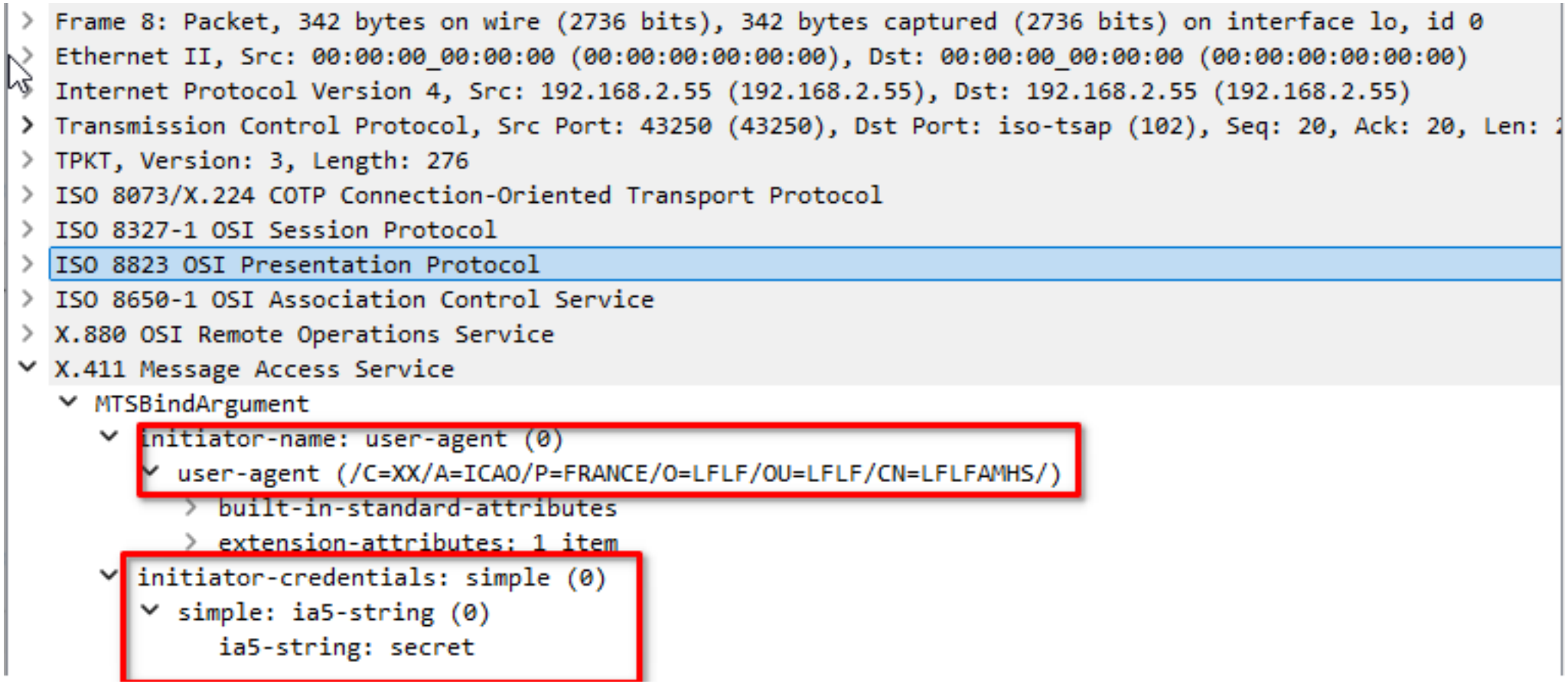
MTA Bind - Simple

- ✓ A Simple MTA Bind can be considered to consist of a username and password
- ✓ An MTA Bind operation requires the authentication information to be in an MTSBindArgument
- ✓ In X.400 terms, the MTSBindArguments contains
  - ✓ The initiator-name, i.e. the X.400 O/R address of the user agent
  - ✓ The initiator-credentials, i.e. a password assigned to the user by the administrator
- ✓ The information in the MTSBindArguments is transmitted over the network without encryption
- ✓ Anyone who can monitor a network, can therefore see the credentials

No.	Time	Source	Destination	Protocol	Length	Info
6	0.015257591	192.168.2.55	192.168.2.55	COTP	85	CC TPDU src-ref: 0x0002 dst-ref: 0x0001
7	0.015276962	192.168.2.55	192.168.2.55	TCP	66	43250 → iso-tsap(102) [ACK] Seq=20 Ack=20 Win=65536 Len=0 TSval=1205622147 TSecr=
8	0.015356155	192.168.2.55	192.168.2.55	P3	342	mts_bind_argument simple
9	0.032010736	192.168.2.55	192.168.2.55	P3	436	mts_bind_result MTA-LFLF-1;/C=XX/ADMD=ICAO/PRMD=FRANCE simple
10	0.073554035	192.168.2.55	192.168.2.55	TCP	66	43250 → iso-tsap(102) [ACK] Seq=296 Ack=390 Win=65536 Len=0 TSval=1205622205 TSec
11	8.965021946	192.168.2.55	192.168.2.55	ACSE	94	Release-Request (normal)
12	8.965138746	192.168.2.55	192.168.2.55	ACSE	91	Release-Response (normal)
13	8.965153024	192.168.2.55	192.168.2.55	TCP	66	43250 → iso-tsap(102) [ACK] Seq=324 Ack=415 Win=65536 Len=0 TSval=1205631096 TSec
14	8.965207814	192.168.2.55	192.168.2.55	TCP	66	43250 → iso-tsap(102) [FIN, ACK] Seq=324 Ack=415 Win=65536 Len=0 TSval=1205631096
15	8.969247224	192.168.2.55	192.168.2.55	TCP	66	iso-tsap(102) → 43250 [FIN, ACK] Seq=415 Ack=325 Win=65536 Len=0 TSval=1205631101

```
> Frame 8: Packet, 342 bytes on wire (2736 bits), 342 bytes captured (2736 bits) on interface lo, id 0
> Ethernet II, Src: 00:00:00_00:00:00 (00:00:00:00:00:00), Dst: 00:00:00_00:00:00 (00:00:00:00:00:00)
> Internet Protocol Version 4, Src: 192.168.2.55 (192.168.2.55), Dst: 192.168.2.55 (192.168.2.55)
> Transmission Control Protocol, Src Port: 43250 (43250), Dst Port: iso-tsap (102), Seq: 20, Ack: 20, Len:
> TPKT, Version: 3, Length: 276
> ISO 8073/X.224 COTP Connection-Oriented Transport Protocol
> ISO 8327-1 OSI Session Protocol
> ISO 8823 OSI Presentation Protocol
> ISO 8650-1 OSI Association Control Service
> X.880 OSI Remote Operations Service
> X.411 Message Access Service
```

```
0000  00 00 00 00 00 00 00 00  00 00 00 00 08 00 45 00
0010  01 48 68 89 40 00 40 06  4b 68 c0 a8 02 37 c0 a8
0020  02 37 a8 f2 00 66 49 1c  1a 63 ec 1a a3 3b 80 18
0030  02 00 86 f9 00 00 01 01  08 0a 47 dc 55 83 47 dc
0040  55 83 03 00 01 14 02 f0  80 0d ff 01 09 01 26 0a
0050  13 04 11 4d 54 41 2d 4c  46 4c 46 2d 31 2e 33 61
0060  64 36 2e 30 0b 0f 17 0d  32 36 30 33 32 34 31 33
0070  33 35 32 32 5a 05 0c 13  01 00 15 04 07 fd 07 fd
0080  16 01 01 14 02 00 02 c1  cd 31 81 ca a0 03 80 01
0090  01 a2 81 c2 a4 55 30 0f  02 01 01 06 04 52 01 00
00a0  01 30 04 06 02 51 01 30  0f 02 01 03 06 04 56 00
00b0  02 01 30 04 06 02 51 01  30 0f 02 01 05 06 04 56
00c0  00 02 02 30 04 06 02 51  01 30 0f 02 01 07 06 04
00d0  56 00 02 06 30 04 06 02  51 01 30 0f 02 01 09 06
00e0  04 56 00 02 0b 30 04 06  02 51 01 61 69 30 67 02
00f0  01 01 a0 62 60 60 a1 06  06 04 56 00 01 00 be 56
0100  28 54 06 02 51 01 02 01  09 a0 4b b0 49 31 47 60
0110  3b 30 26 61 04 13 02 58  58 62 06 13 04 49 43 41
0120  4f a2 08 13 06 46 52 41  4e 43 45 83 04 4c 46 4c
```


Frame 8: Packet, 342 bytes on wire (2736 bits), 342 bytes captured (2736 bits) on interface lo, id 0
Ethernet II, Src: 00:00:00_00:00:00 (00:00:00:00:00:00), Dst: 00:00:00_00:00:00 (00:00:00:00:00:00)
Internet Protocol Version 4, Src: 192.168.2.55 (192.168.2.55), Dst: 192.168.2.55 (192.168.2.55)
Transmission Control Protocol, Src Port: 43250 (43250), Dst Port: iso-tsap (102), Seq: 20, Ack: 20, Len:
TPKT, Version: 3, Length: 276
ISO 8073/X.224 COTP Connection-Oriented Transport Protocol
ISO 8327-1 OSI Session Protocol
ISO 8823 OSI Presentation Protocol
ISO 8650-1 OSI Association Control Service
X.880 OSI Remote Operations Service
X.411 Message Access Service
MTSBindArgument
initiator-name: user-agent (0)
user-agent (/C=XX/A=ICAO/P=FRANCE/O=LFLF/OU=LFLF/CN=LFLFAMHS/)
built-in-standard-attributes
extension-attributes: 1 item
initiator-credentials: simple (0)
simple: ia5-string (0)
ia5-string: secret

Potential risks of the current procedures

- ✓ The example shown corresponds to a User Agent using X.400 P3
- ✓ If a potential attacker got hold of the connection information, it could impersonate an AMHS user
- ✓ So, an attacker could impersonate an AMHS user and therefore it could:
  - ✓ Receive messages that will not be delivered to the real AMHS user
  - ✓ Send false messages to the other AMHS users

Message corruption

- ✓ So far, we have concentrated only on the security of X.400 connections
- ✓ However, there is another problem with the current setup: message corruption
- ✓ An AMHS message that is on transit could be potentially modified
- ✓ If the modification is done carefully, the recipient would not know that the message was not the one sent by the originator
- ✓ This is due to the lack of message signatures
- ✓ This potential problem could occur because of an attacker or a bug in the software

In Summary

- ✓ The current AMHS Security environment is quite weak and can be improved
- ✓ ICAO Doc 9880 Edition 3 specifies how to improve it

Thank You

ICAO