THE DICOM 2013 INTERNATIONAL CONFERENCE & SEMINAR
March 14-16 Bangalore, India

DICOM℠
Digital Imaging and Communications in Medicine

Keeping It Safe: Securing DICOM

Lawrence Tarbox, Ph.D.

Mallinckrodt Institute of Radiology
Washington University in St. Louis

Research Assistant Professor of Radiology
St. Louis, Missouri, USA

WG-5, WG-10, WG-14 (Chair),
WG-18, WG-23 (chair), WG-27

Washington University in St. Louis
School of Medicine

MIR Mallinckrodt Institute of Radiology

Audience Participation

DICOM
Digital Imaging and Communications in Medicine

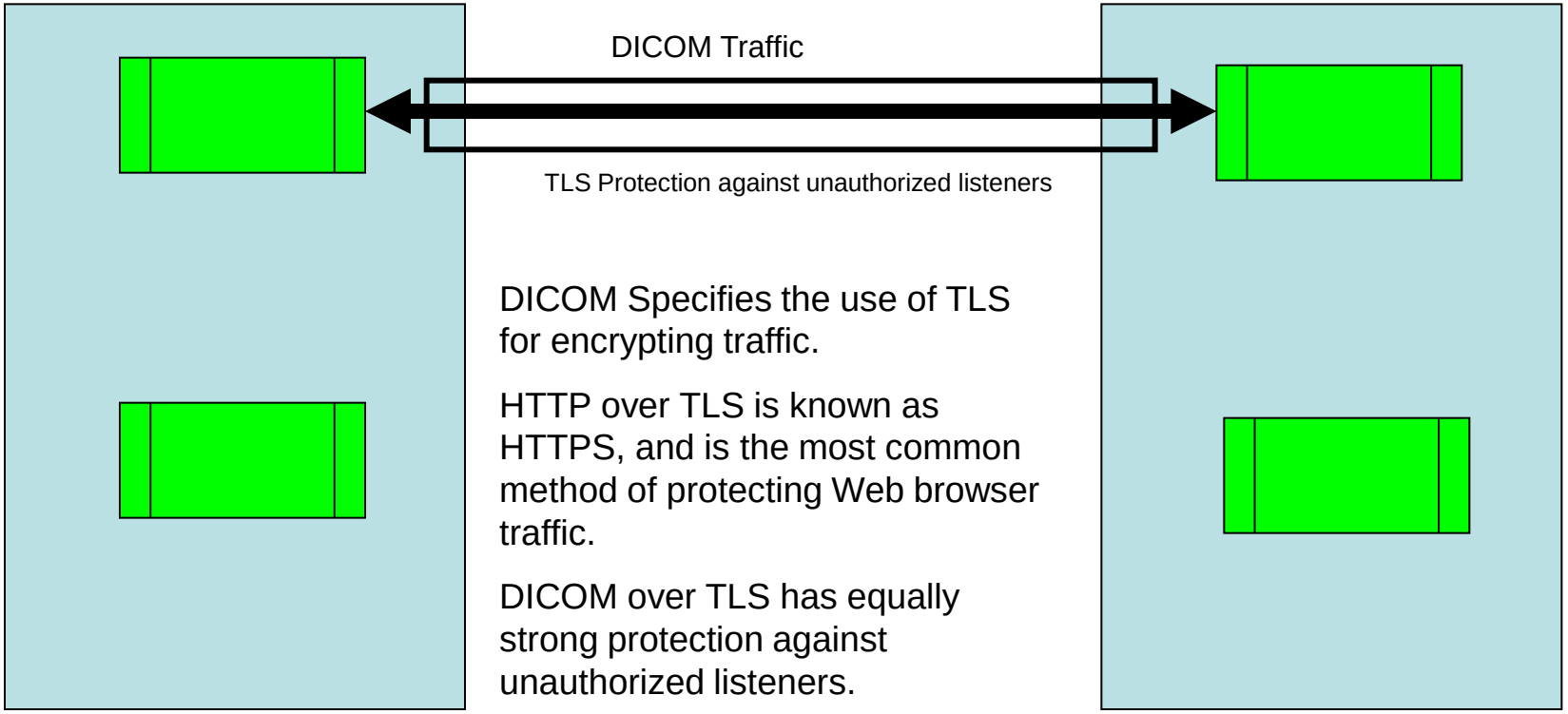
Time For A Quiz!

DICOM
Digital Imaging and Communications in Medicine

DICOM does not have any provisions for secure communication of images

FALSE

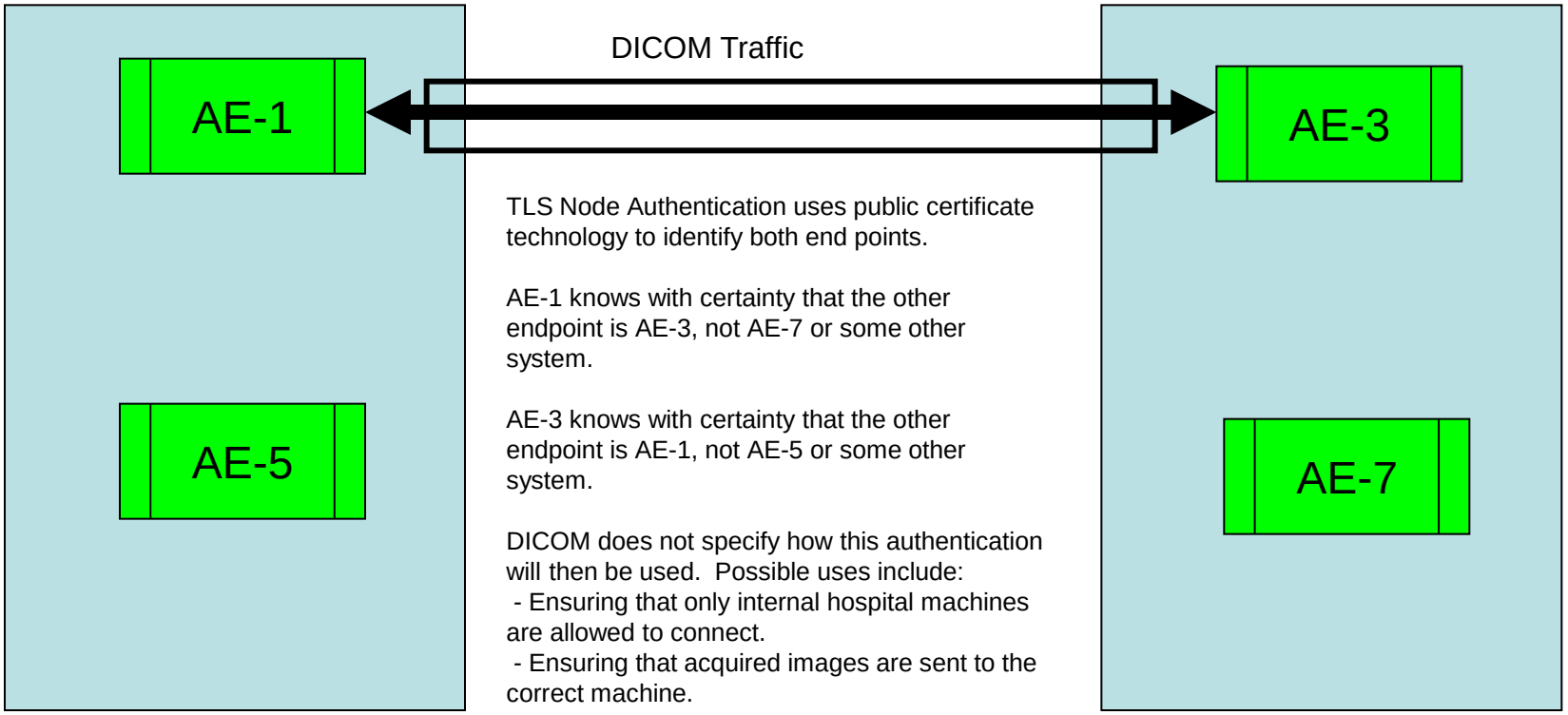
Traffic on the Network



Protection against unauthorized network listeners by means of encryption

Slide Provided by Eric Pan, Agfa HealthCare

Traffic on the Network



Identifying the other system

Slide Provided by Eric Pan, Agfa HealthCare

Traffic on the Network

TLS encryption makes use of public internet connections safe.

- **This will need to be explained to security staff.**
- **DICOM over TLS is like HTTPS and should be allowed.**

Node Authentication uses can be extensively customized.

- **Each connection can be verified in detail, or connections just checked to ensure that they are all within facility connections.**
- **DICOM enables a very wide variety of authentication and access control policies.**
- **DICOM does not mandate any particular policies.**

Slide Provided by Eric Pan, Agfa HealthCare

DICOM
Digital Imaging and Communications in Medicine

DICOM does not have any provisions for securely communicating user credentials

FALSE

User Credentialing

- **Option 1: Trust the sender**
  - **Mutual TLS authentication**
- **Option 2: Assertions during association negotiation**
  - **SAML**
  - **Kerberos**

User Credentials

DICOM
Digital Imaging and Communications in Medicine

Facilitates audit logging

Step toward cross-system authorization and access controls

- **DICOM still leaves access control in the hands of the application**

Query Filtering

- **For productivity as well as security**

Design Goals

DICOM
Digital Imaging and Communications in Medicine

Independent of other security mechanisms

- **No changes to other DICOM security mechanisms**

Avoid incompatibility with the installed base

- **Minimum of changes to existing implementation libraries**

Extensible for future credential types

Established during association negotiation

- **before any regular DIMSE transactions take place**
- **Allows SCP to reject associations based on ID**

Credential Type Profiles

DICOM
Digital Imaging and Communications in Medicine

Un-authenticated identity assertion

- Systems in a trusted environment

Username plus passcode

- Systems in a secure network

Kerberos-based authentication

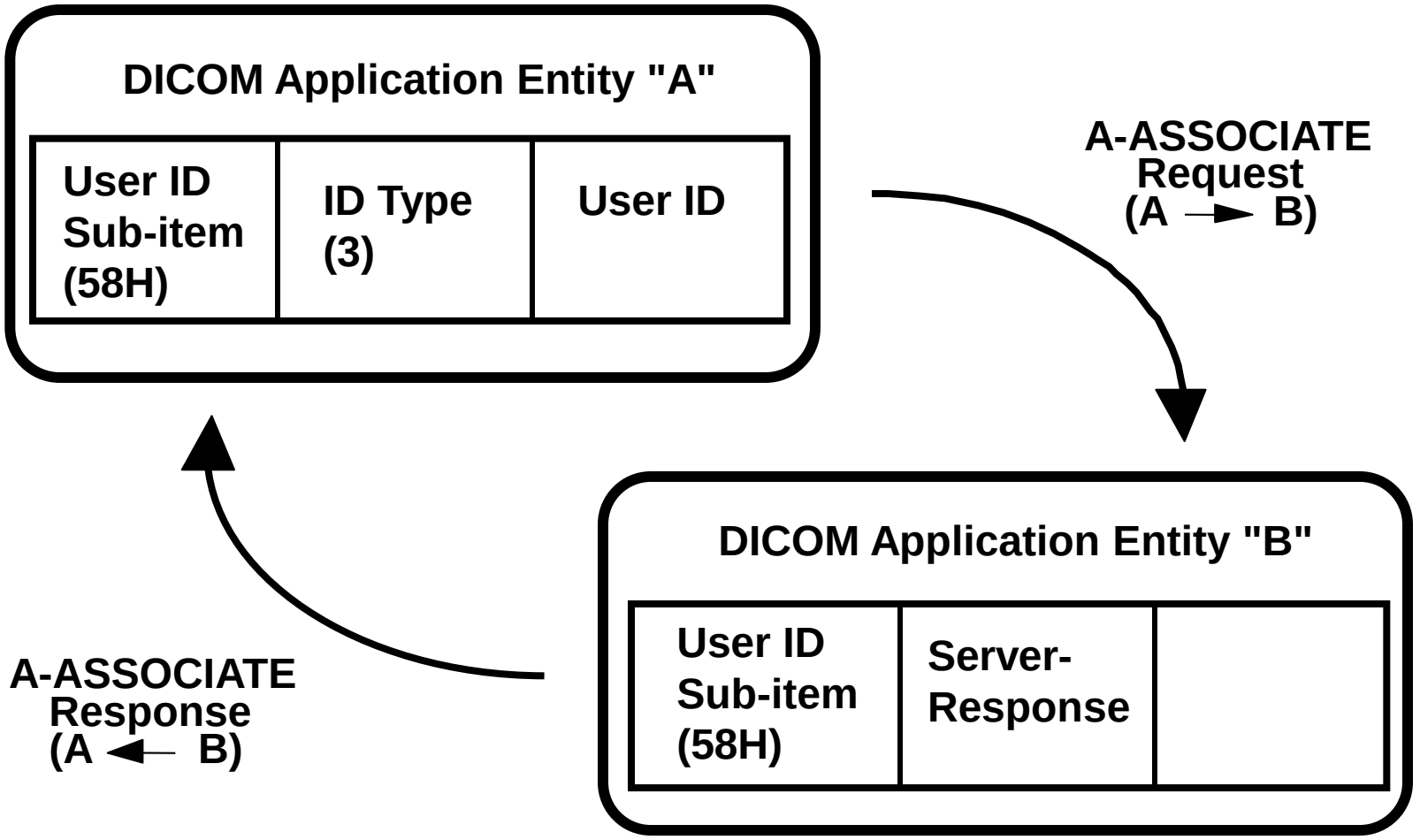
- Strongest security

Generic SAML assertion

- Nice mix of simplicity and security

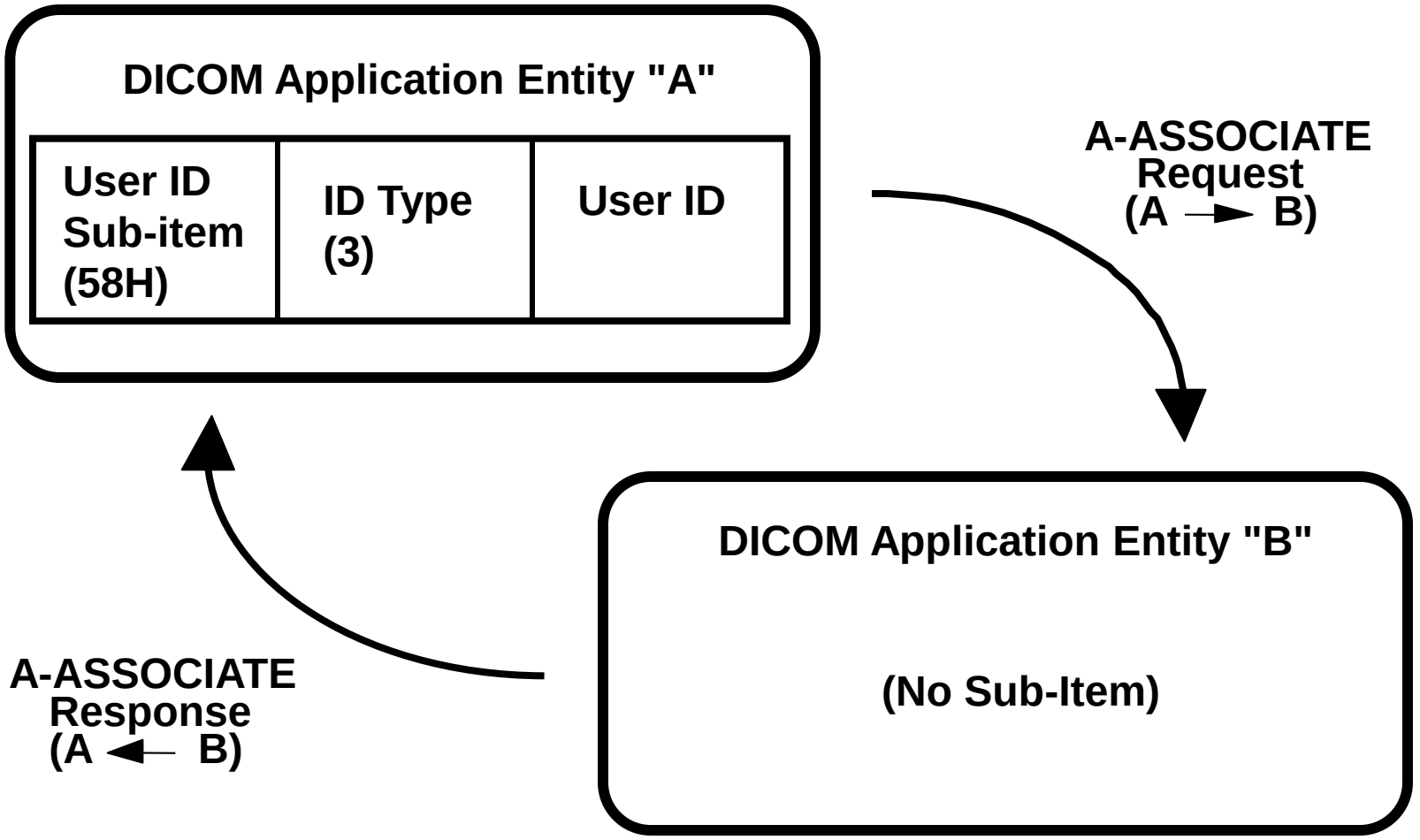
Extended Negotiation

Response Expected



Extended Negotiation

No Response Expected



Prepared for the Future

DICOM
Digital Imaging and Communications in Medicine

Could support any mechanism that supports uni-directional assertion mechanism (e.g. using PKI and Digital Signatures)

Does not support identity mechanisms that require bi-directional negotiation (e.g. Liberty Alliance proposals)

Several Options

- **User identity alone, with no other security mechanisms**
- **User identity plus the current DICOM TLS mechanism**
- **User identity plus future lower level transport mechanisms (e.g. IPv6 with security option)**
- **User identity plus VPN**
- ***Practically any combination needed***

DICOM
Digital Imaging and Communications in Medicine

DICOM does not have any provisions for guaranteeing the integrity of data.

FALSE

Embedded Security Features

DICOM
Digital Imaging and Communications in Medicine

Digital Signatures

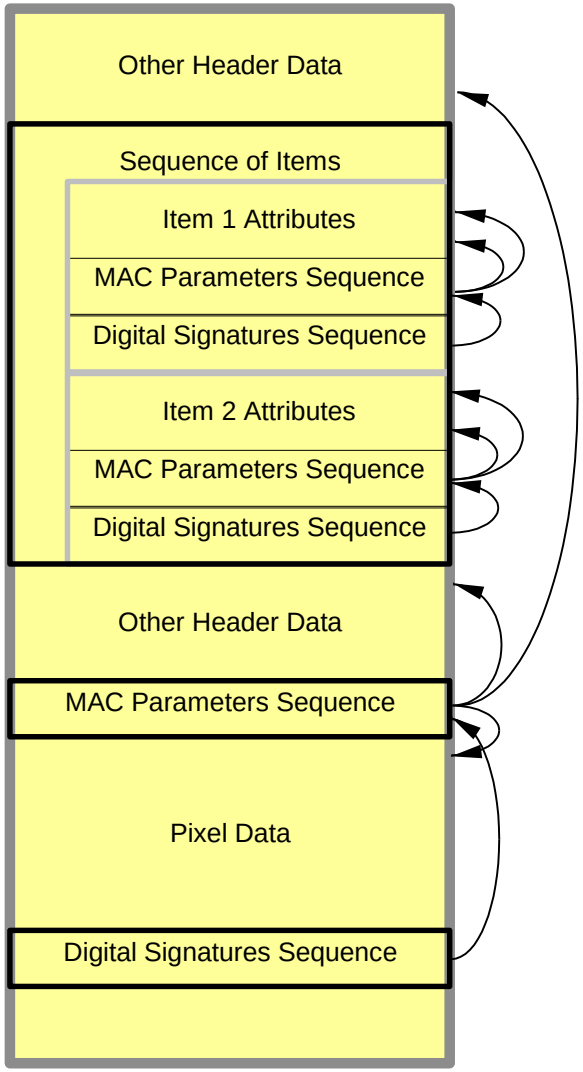
- Persistent integrity check
- Identifies users or devices that handled the object, with optional secure timestamp

Selective Encryption

- Persistent privacy protection
- Hide sensitive Attributes from certain users

Digital Signatures

- **Embedded in SOP Instance**
- **Can make secure references to unsigned objects**
- **Multiple signatures**
  - **Overlapping subsets**
  - **Multiple signers**
  - **Signatures on individual items**
- **Signature purposes**
- **Defined in profiles**



DICOM
Digital Imaging and Communications in Medicine

DICOM does not have standardized digital watermarking of images

TRUE, but …

DICOM does not preclude its use

DICOM
Digital Imaging and Communications in Medicine

There is no embedded encryption defined by DICOM.

FALSE

Selective Encryption

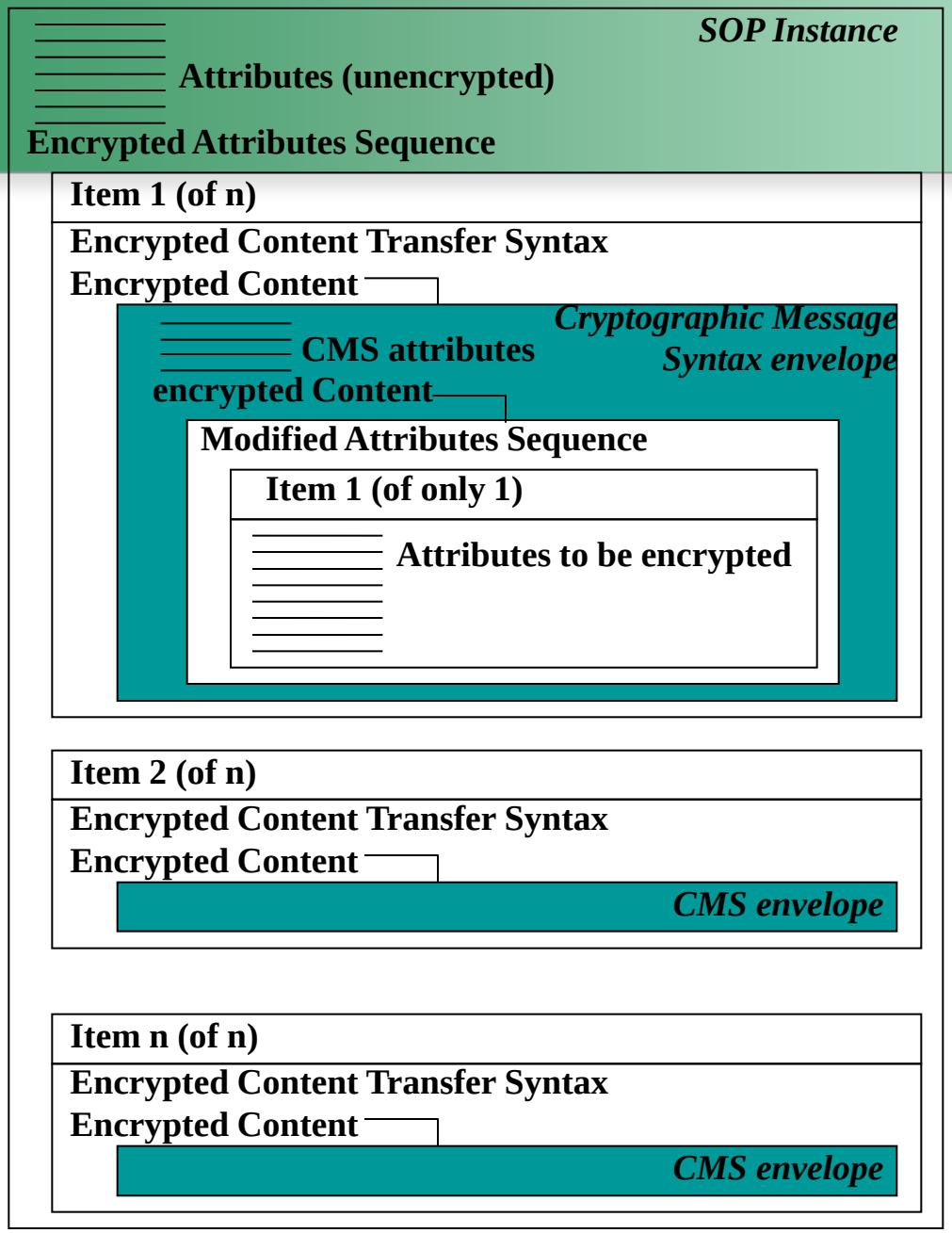
Can encrypt all of the SOP Instance, selected attributes, or even just a single attribute

Security Profiles are used to describe the attributes that are protected

Local profiles can be used if selective encryption is wanted for special needs, e.g.,

- **Only encrypt patient information, not equipment or image**
- **Only encrypt report contents, not patient identification**

Slide Provided by Eric Pan, Agfa HealthCare


SOP Instance
Attributes (unencrypted)
Encrypted Attributes Sequence
Item 1 (of n)
Encrypted Content Transfer Syntax
Encrypted Content
Cryptographic Message Syntax envelope
CMS attributes
encrypted Content
Modified Attributes Sequence
Item 1 (of only 1)
Attributes to be encrypted
Item 2 (of n)
Encrypted Content Transfer Syntax
Encrypted Content
CMS envelope
Item n (of n)
Encrypted Content Transfer Syntax
Encrypted Content
CMS envelope

Media Security

DICOM Digital Imaging and Communications in Medicine

DICOM Media Security applies to all DICOM specified media, e.g., CD-R, DVD-R, E-Mail, USB Device

The media's file system remain unencrypted, so the media can be processed and copied without special operating system driver

The individual objects are held in CMS (Cryptographic Message Syntax) envelopes inside files on the media

- **CMS is often used in secure e-mail**
- **Optional encryption to protect against unauthorized disclosure.**
- **Optional integrity check to protect against tampering**

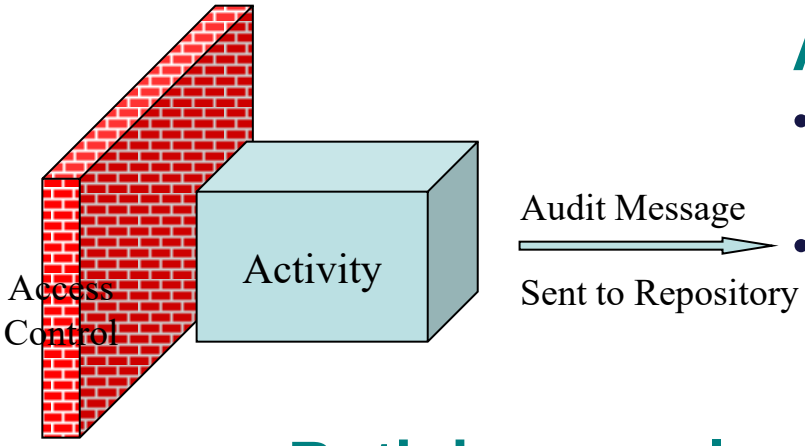
DICOM
Digital Imaging and Communications in Medicine

DICOM itself provides no mechanisms for controlling access to data

TRUE

Securing Access to Data

- **Access Control**
  - Get permission before allowing action
  - Suitable for certain situations, e.g. restricting access to authorized medical staff



Audit Control

- **Allow action without interference, trusting the judgment of the staff.**
- **Monitor behavior to detect and correct errors.**

- **Both have a place in security systems**
- **Local security policies determine what is handled by access control, and what is handled by audit controls.**

On the computer

DICOM does not specify computer access control or other computer security measures.

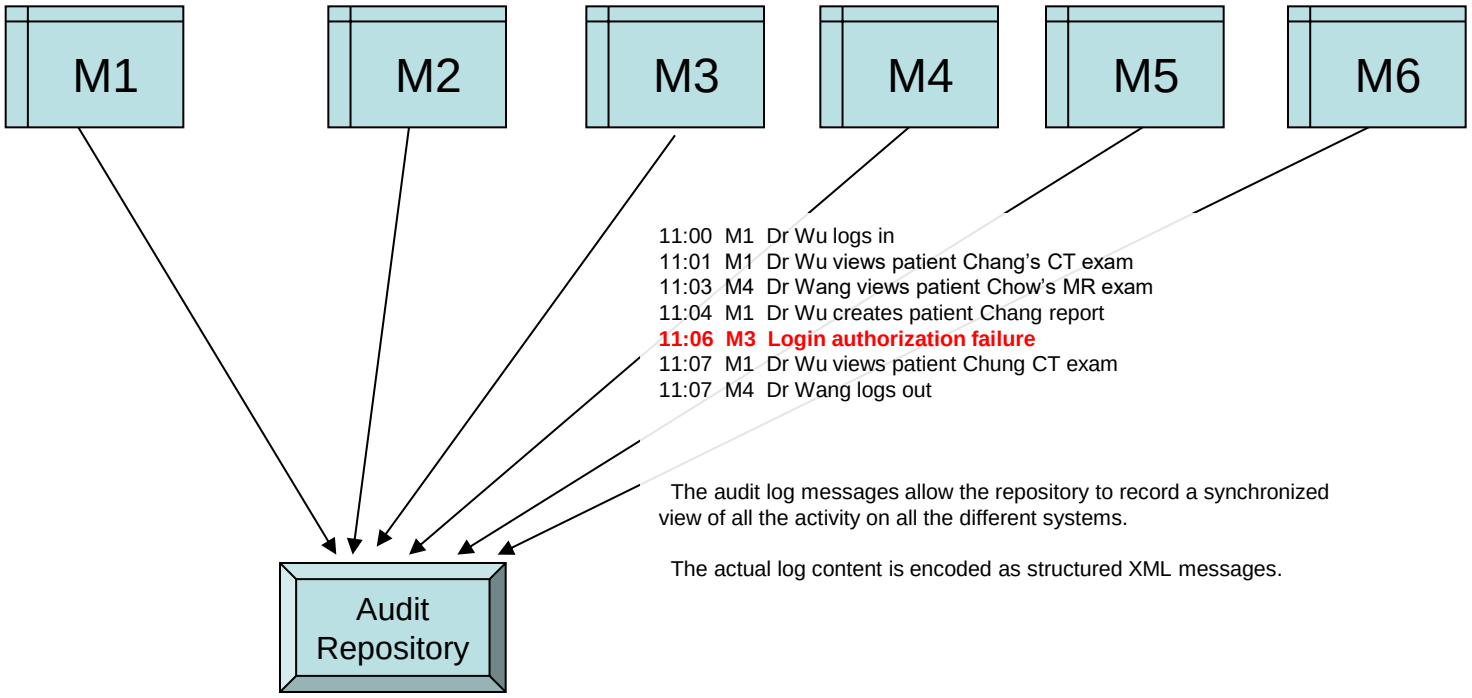
- **These are subject to local policy**
- **These are very application specific**
- **These are very implementation specific**

DICOM does expect that the use of audit trails and activity monitoring will be part of the local security system.

DICOM defines a standard interface for reporting user and computer activity to a centralized audit repository.

Slide Provided by Eric Pan, Agfa HealthCare

On the Computer



The audit repository can be used to record and monitor the entire network.

The security detection mechanisms may be as simple as flagging a login failure, or be highly complex behavior pattern recognition. DICOM enables these mechanisms. DICOM does not specify them.

Slide Provided by Eric Pan, Agfa HealthCare

Configuring Network Security

Certificate Management

- Certificates are used to identify systems (and perhaps Application Entities)
- Certificates can be self-generated, facility signed, or signed by internationally recognized authorities.

Most equipment supports

- Individually provided certificates per system (self-signed or otherwise), and
- Certificates for facility authorities. Certificates signed by these authorities are recognized as authorized.

Management reference

- The SPC paper “Managing Certificates” describes this in more detail.

Slide Provided by Eric Pan, Agfa HealthCare

Configuring Network Security

Firewall rules

- **Firewalls may need to be configured to permit DICOM over TLS traffic (in and out).**
  - The DICOM over TLS port defaults to the same port as HTTPS, but it is often changed.
  - Using a different port permits the same system to be both an HTTPS server and a DICOM over TLS system.

Audit Policies

- **DICOM makes no specific recommendations on how the DICOM audit logs should be analyzed.**
- **The audit logs are designed to support surveillance for unauthorized activity. Other more detailed system specific logs are expected to provide forensic detail.**

Slide Provided by Eric Pan, Agfa HealthCare

References

http://dicom.nema.org/

http://www.HL7.org/

http://www.IHE.net/

Author Contacts

Lawrence Tarbox, Ph.D.

- tarboxl@mir.wustl.edu
- 510 South Kingshighway Boulevard
  St. Louis, MO 63110 USA

Thank you for your attention !