DICOM

Digital Imaging and Communications in Medicine

DICOM Educational Conference Brisbane, Australia

SEPTEMBER 27-28, 2018

SECURING DICOM

Lawrence Tarbox, Ph.D.

University of Arkansas for Medical Sciences

User co-chair for WG-14, WG-23, WG-29

UAMS®

Security Requires Planning

- Set policies
- Implement controls
  - Procedural – what people should do
  - Technological – what machines should do
  - Physical – the environment in which people and machines operate
- Educate
- Evaluate

Sources of Guidance - NIST

- National Institute of Standards and Technology (NIST)
  - Cybersecurity Framework (https://www.nist.gov/cyberframework)
    - Points to lots of other documents from multiple sources, not just NIST documents
  - Computer Security Resource Center Publication series (https://csrc.nist.gov/publications/sp)
    - Lots of procedures, probably overkill, but one possible view of 'best practices'. Though focused on government systems, lots of good ideas.
    - SP 800-53 "Security and Privacy Controls for Federal Information Systems and Organizations" is of particular interest (https://csrc.nist.gov/publications/detail/sp/800-53/rev-4/final)

Sources of Guidance

- National Security Agency | Central Security Service
  - Manageable Network Plan Guide (https://www.iad.gov/iad/library/ia-guidance/security-configuration/networks/manageable-network-plan.cfm)
    - A hypothetical project plan for securing networked infrastructure
- Guidelines from other countries, trade organizations
- Joint Security and Privacy Committee (NEMA, COCIR, JIRA)
- Books

Plans Vary

- Different organizations assess and mitigate risks differently
- Responsibilities vary
- Staff size varies
- Typically one person has overall responsibility, for example
  - Chief Information Officer (CIO)
  - Chief Information Security Officer (CISO)
- Security Plans are necessary, but outside the scope of DICOM
- DICOM has features that can be call upon by security

DICOM Security Features

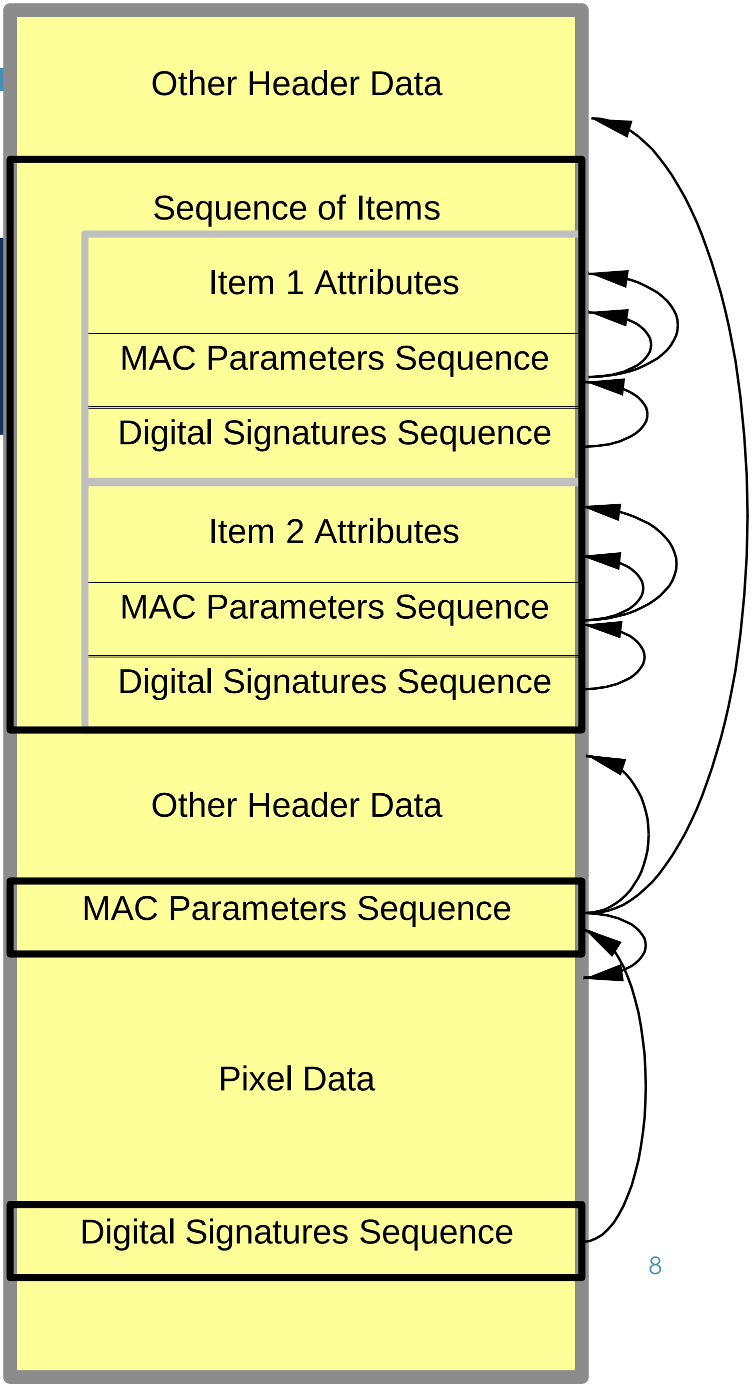
- Protect data at rest
  - Digital Signatures
  - Attribute Confidential, including de-identification
  - Media Storage Security
- Protect data in transit, including node authentication
- User credentialing (optional part of Association Negotiation or session establishment)
- Audit logging

Protecting Data at Rest

- Digital Signatures
  - Persistent integrity check (tamper detection)
  - Identifies users or devices that handled the object, with optional secure timestamp
- Selective Encryption or De-identification
  - Persistent privacy protection
  - Hide sensitive Attributes, except from certain users (optional)
- Whole object encryption
  - Uses a Cryptographic Message Syntax Envelope
  - Retricts access to specific individuals

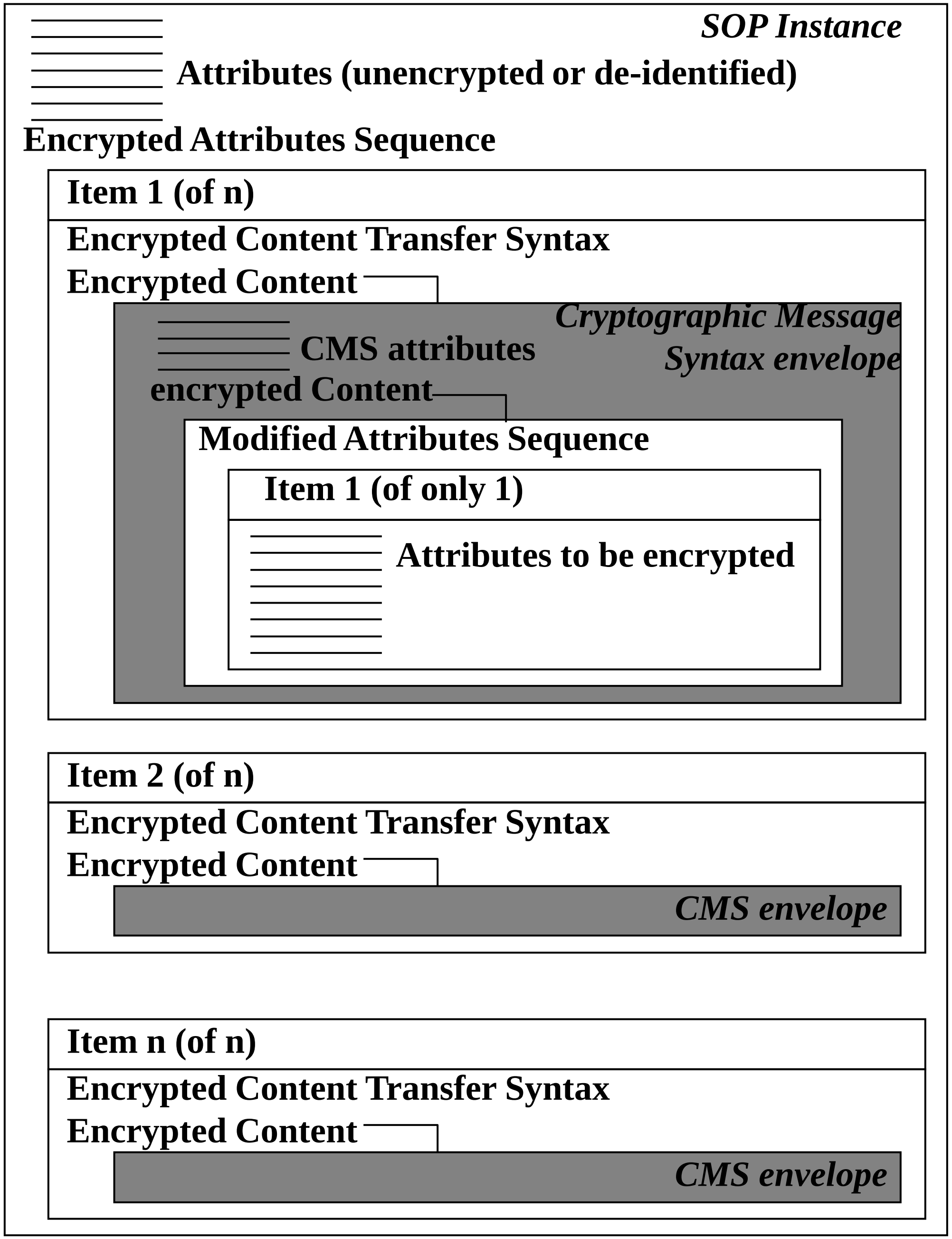
Digital Signatures

- Embedded in SOP Instances
- Can make secure references to unsigned objects
- Multiple Signatures
  - Overlapping subsets
  - Multiple signers
  - Sign individual items
- Signature purposes
- Defined in profiles



Attribute Level Encryption

- Can encrypt all of the SOP Instance, selected Attributes, or even just a single Attribute.
- Security Profiles describe the Attributes to protect
- Local profiles can be used for special needs
  - Only encrypt patient information, not equipment or image
  - Only encrypt report contents, not patient ID
- Encrypted Attributes optionally move to inside a Cryptographic Message Syntax envelope inside a sequence, to allow re-identification
- The Attributes to be protected are de-identified


SOP Instance
Attributes (unencrypted or de-identified)
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

Multiple Sequence Items can be used to reveal different subsets of Attributes to different intended recipients. The subsets may overlap.

Keeping the object consistent

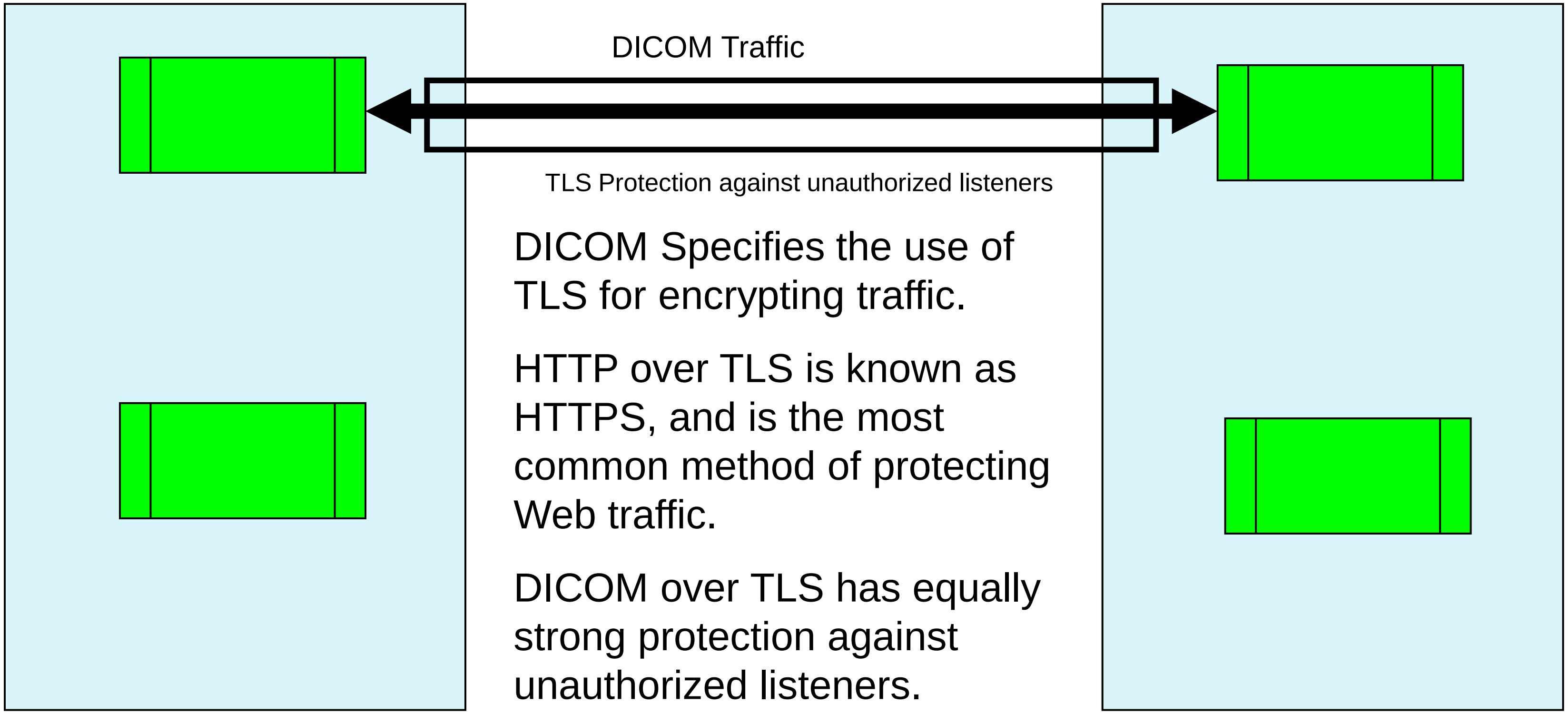
- Attributes being encrypted should be intelligently replaced
  - The Attribute Type and conditions conventions must be honored
    - A Type 1 (Required) Attribute must have a reasonable replacement
      (e.g. Patient IDs, dates, names)
    - A Type 3 (Optional) Attribute could be removed
    - See tables in the profiles for recommendations
  - UIDs should maintain referential consistency – if a UID is replaced, the new UID should replace the old UID in all references

Leave out the Encrypted Attributes Sequence

Media Security

- Applies to all DICOM specified media, e.g., CD-R, DVD-R, E-mail, USB device
- The media's file system remains unencrypted
  - No special drivers or file system software needed
  - Easy to process and copy
- Object are enclosed within Cryptographic Message Syntax (CMS) Envelopes placed inside regular files
  - CMS is often used to secure e-mail
  - Optional encryption to protect against unauthorized disclosure
  - Optional integrity check to protect against tampering

Protecting Data in Transit



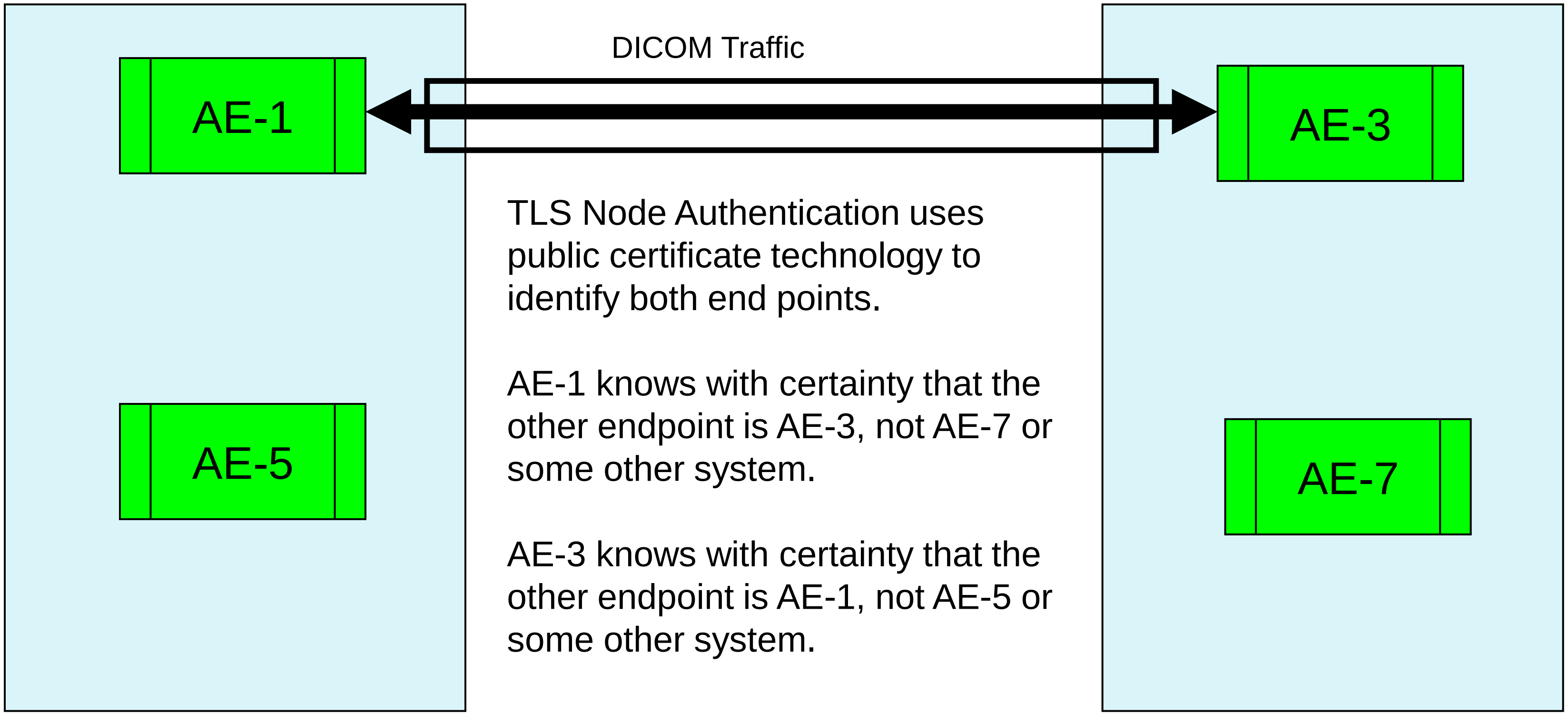
DICOM Specifies the use of TLS for encrypting traffic.

HTTP over TLS is known as HTTPS, and is the most common method of protecting Web traffic.

DICOM over TLS has equally strong protection against unauthorized listeners.

Protection against unauthorized network listeners by means of encryption

Node Authentication



TLS Node Authentication uses public certificate technology to identify both end points.

AE-1 knows with certainty that the other endpoint is AE-3, not AE-7 or some other system.

AE-3 knows with certainty that the other endpoint is AE-1, not AE-5 or some other system.

Identifying communication partners

Node Authentication

- DICOM does not specify how this authentication will then be used. Possible uses include:
  - Ensuring that only internal hospital machines are allowed to connect.
  - Ensuring that acquired images are sent to the correct machine.
- Though not commonly turned on, most web infrastructure does support bi-directional mutual authentication

Advantages to using TLS

- TLS encryption protects public internet connections.
  - 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

TLS Configuration

- Very configurable
- Best practices captured in BCP195 from IETF
- Referenced by the DICOM Standard
  - BCP195 TLS Profile (downgradable)
  - Non-downgrading BCP195 Profile (restricts negotiation to more secure TLS versions and cipher suites)
  - (coming) The CRYPTREC TLS Profile (restricts negotiation and cipher suites even further, with additional baseline ciphersuite support – a Japanese recommendation)

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)
  - Certificates for facility authorities. Certificates signed by these authorities are recognized as authorized
- The SPC paper "Managing Certificates" describes this in more detail
- The Automatic Certificate Management Environment (ACME) protocol, being standardized by IETF may be useful

User Credentialling

- Option 1: Trust the sender
  - Mutual TLS Authentication
- Option 2a: Assertions during Association Negotiation (traditional DICOM)
  - SAML
  - Kerberos
- Option 2b: Leverage Web mechanisms (DICOMweb™)
  - SAML
  - OpenID Connect

Example Applications of User Credentials

- 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

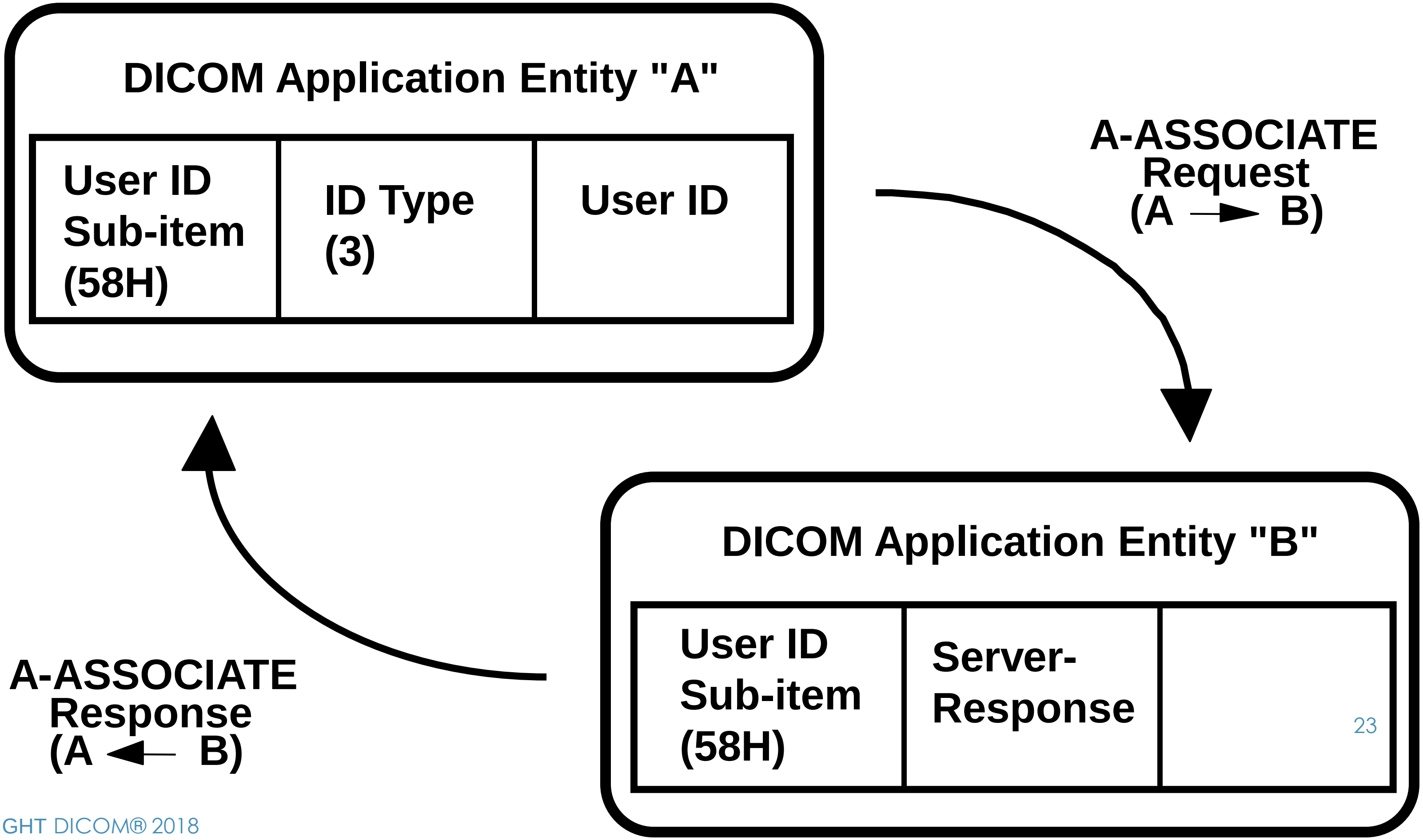
DICOM User Credentialling Design Goals

- Independent of other security mechanisms
  - No changes to other DICOM security mechanisms
- Avoid incompatibility with the installed base
  - Minimum changes to existing implementation libraries
- Extensible for future credential types
- Established during association negation
  - Before any regular DIMSE transactions take place
  - Allows SCP to reject associationos based on ID

User Credential Type Profiles

- Un-authenticated identity assertion
  - Systems trust each other
- Username plus passcode
  - Systems in a secure network
- Kerberos-based authentication
  - Strong security, more involved implementation and deployment
- Generic SAML assertion
  - Nice mix of simplicity and security

Extended Negotiation – Response Expected



DICOM Application Entity "A"

User ID Sub-item (58H)	ID Type (3)	User ID

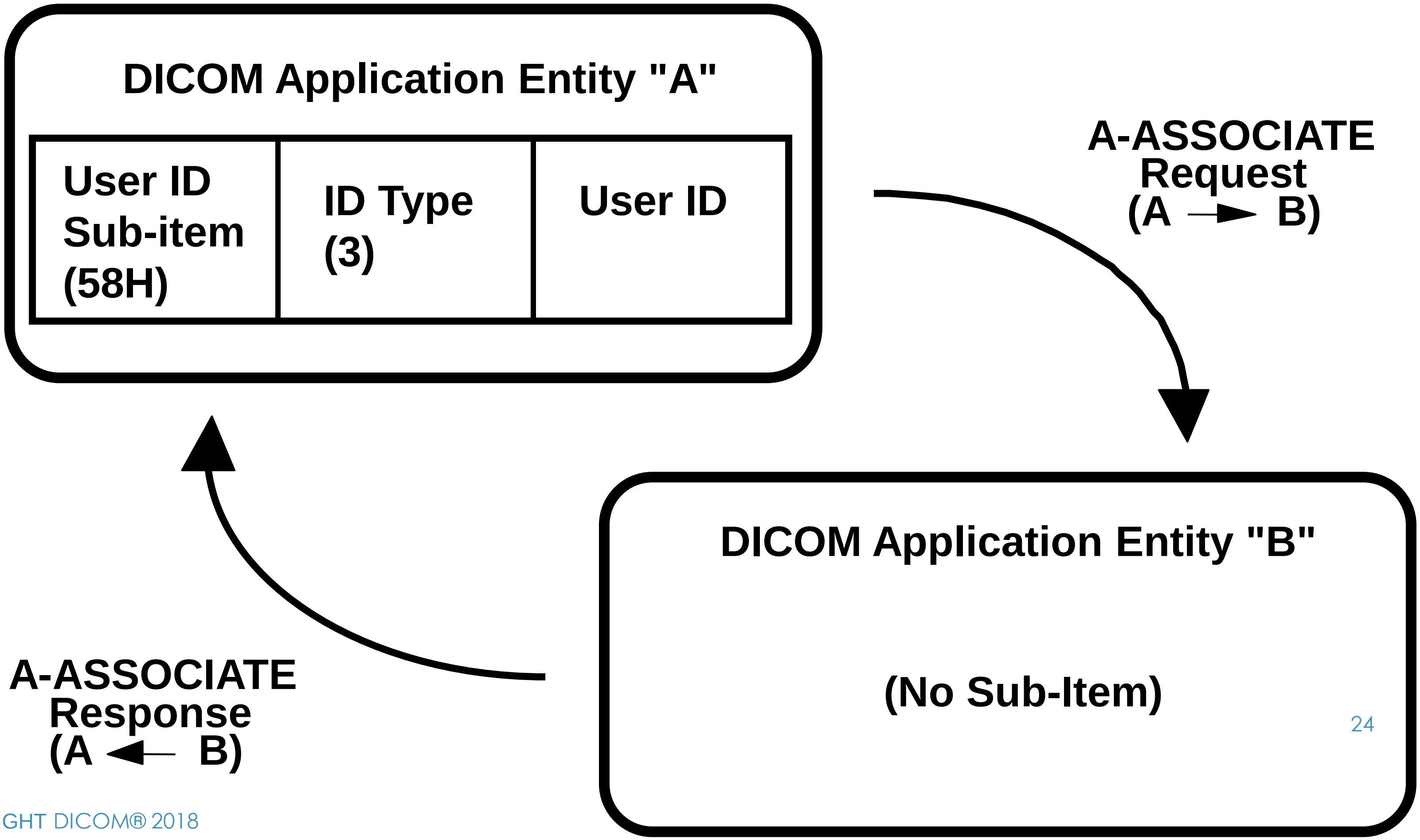
A-ASSOCIATE Request (A → B)

DICOM Application Entity "B"

User ID Sub-item (58H)	Server-Response	

A-ASSOCIATE Response (A ← B)

Extended Negotiation – No Response Expected



DICOM Application Entity "A"

User ID Sub-item (58H)	ID Type (3)	User ID

A-ASSOCIATE Request (A → B)

DICOM Application Entity "B"

(No Sub-Item)

A-ASSOCIATE Response (A ← B)

Prepared for the Future

- Could support any mechanism that supports uni-directional assertion mechanisms (e.g. using PKI and Digital Signatures)
- Does not support identity mechanisms that require bi-directional negotiation (e.g. Liberty Alliance proposals

Several Options

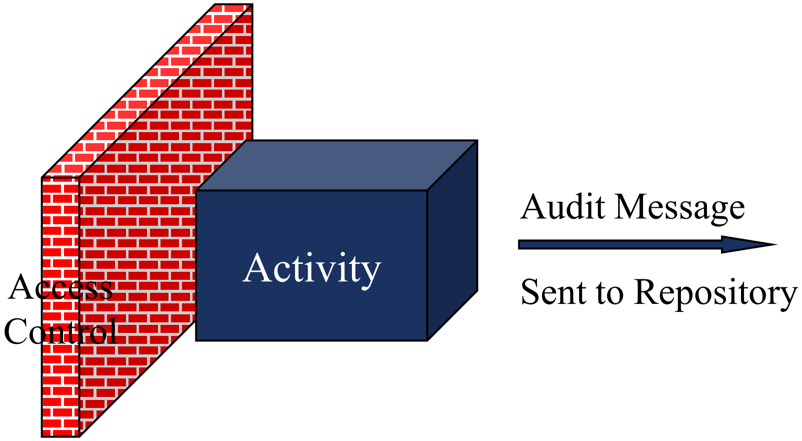
- User identity alone, with no other security mechanisms
- User identity plus DICOM TLS
- User identity plus future lower level transport mechanisms (e.g. IPv6 with security option)
- User identity plus VPN

Practically any combination needed

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

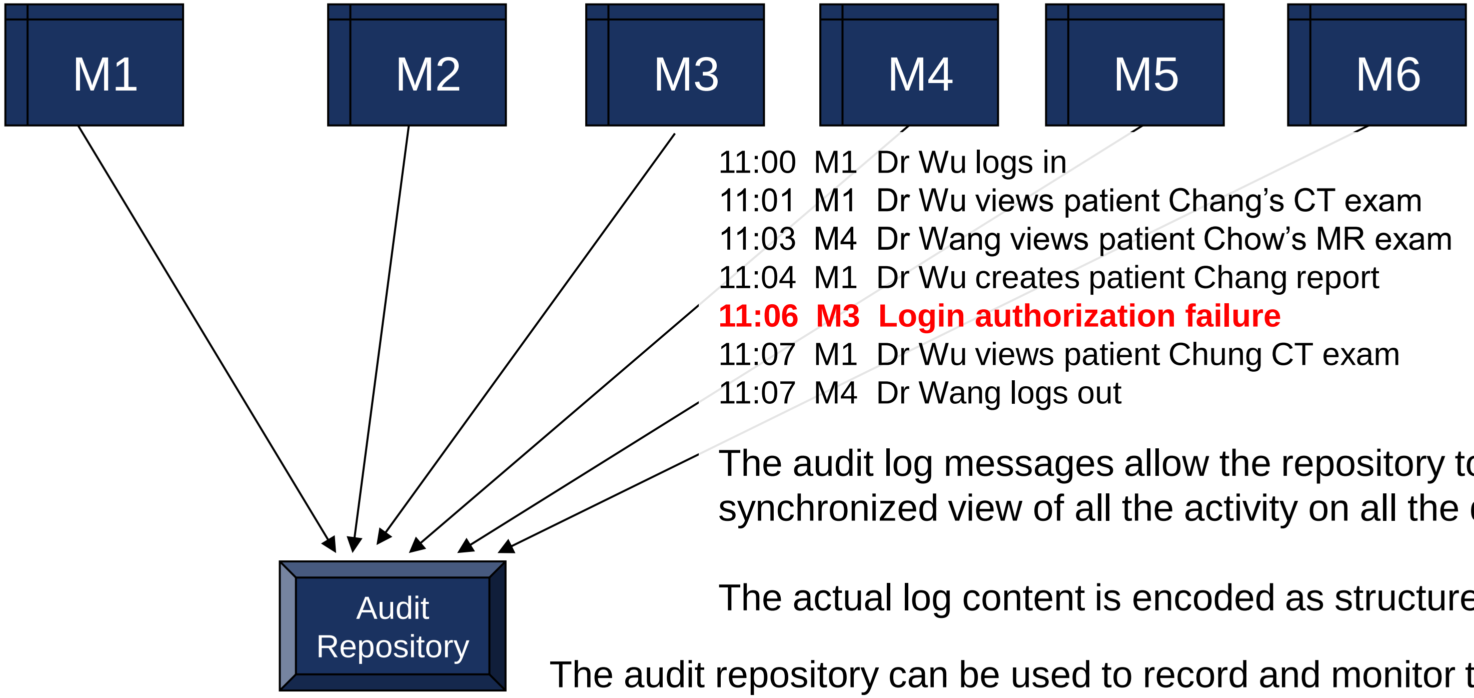
- Allow action without interference, trusting the judgment of the staff.
- Monitor behavior to detect and correct errors.

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

DICOM's Contribution to Access Control

- DICOM does not specify computer access control
  - These are subject to local policy
  - These are very application specific
  - These are very implementation specific
- DICOM can convey user credentialing
- 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

Audit Repository



```
11:00  M1  Dr Wu logs in
11:01  M1  Dr Wu views patient Chang’s CT exam
11:03  M4  Dr Wang views patient Chow’s MR exam
11:04  M1  Dr Wu creates patient Chang report
11:06  M3  Login authorization failure
11:07  M1  Dr Wu views patient Chung CT exam
11:07  M4  Dr Wang logs out
```

The audit log messages allow the repository to record a synchronized view of all the activity on all the different systems.

The actual log content is encoded as structured XML messages.

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.

Presenter’s contact information

Lawrence Tarbox
LTarbox@uams.edu

Department of Biomedical Informatics
University of Arkansas for Medical Sciences
4301 W. Markham, Slot 782
Little Rock, Arkansas 72205, USA

Thank you for your attention.

And thanks to Eric Pan for providing material for slides, Rob Horn for his brilliance, and the other participants of DICOM WG-14 Security who put forth the effort to make this happen.