Keeping It Safe
Securing DICOM

Brad Genereaux, Agfa HealthCare
Product Manager

Industry Co-Chair, DICOM WG-27, Web Technologies
What is security?

- Protecting data security (against unauthorized access)
- Protecting data integrity (against unauthorized changes)
- Protecting data loss (against unauthorized deletions)
- Protecting data availability (against denial of service)
What are the implications if security is compromised?

• Data corruption and loss
• Fraud against those victimized
• Civil penalties (fines and lawsuits)
• Criminal penalties
• Serious harm and death
What is NOT security?

- Changing names of parameters, servers or functions to make it harder to guess
- Including dangerous functions in a release but not including them in documentation
Simple workflow
- Modality transmits images to archive
- Radiologist requests images for reading

: Out to cause security issues
DICOM Security Profiles

- Describes methods to mitigate various security concerns
- Items in red describe solutions that are used in the industry but not explicitly part of the DICOM standard
DICOM in Transit

Who sees this image?

- The modality, who sends the image
- The archive, who receives the image
- Anyone on the network between
• **Transport Level Security** encryption (defined in PS3.15 Section B.1)
• Encryption is negotiated as part of TLS
• Traffic encrypted with public certificate and decrypted by private key
• **Network VPN tunnels** is another mechanism
• **DICOMweb** can leverage **HTTPS (TLS based)**
Who are the actors in transmission?

- The modality, who sends the image
- The archive, who receives the image
- Anyone pretending to be these actors
Node Identity

- **DICOM-TLS certificates** specifies identifying information about the owner.
- Verification of certificates are done against a signing authority.
- **AE titles** are a less secure alternative.
User Authentication

Who can retrieve images?

• Device is validated by DICOM-TLS
• User can retrieve images
• Anyone else using device can, too
User Authentication

- Defined in PS3.15 B.4-7
- Authentication of users can occur via
  - Mutual TLS authentication (each side presents certificates)
  - Authentication during association negotiation (SAML, Kerberos, etc)
- Authenticating users at the application level and making trusted calls to the imaging backend is an alternative approach
Auditing

- Described in PS 3.15 Part A.5
- User should be known
- Events for authentication, query, access, transfer, import/export, and deletion
- This is used in the IHE ITI ATNA profile with Radiology option
Who ensures the images are genuine as the modality provides them?

- The archive accomplishes this task
- Anyone else who can manipulate the archive
Digital Signatures

- DICOM supports digital signatures which provides integrity check and other features
- Defined in PS3.15 Section C
- Individual fields can also be selectively encrypted
- Disk-level encryption can also be used to maintain integrity at rest
Media Storage

- Used when DICOM is transmitted via physical media (CD, DVD, USB key)
- Guarantees confidentiality, integrity, and media origin
- Defined in PS3.15 section D
Anonymization

- Anonymization profiles exist to support masking of data for various purposes
  - Clinical trials
  - Teaching files
- Defined in PS3.15 section E
- Addresses removal and replacement of DICOM attributes that may reveal protected health information
DICOM’s Stance

- DICOM enables a very wide variety of authentication and access control policies, but does not mandate them.
- DICOMweb shares the same position through the use of standard internet technologies.
Suggestions

- Use DICOM-TLS and HTTPS for DICOMweb
- Use appropriate authentication and authorization measures
- Use appropriate at-rest encryption mechanisms
- Control access via managed environments, strong identity management, firewalls
- Consider security throughout your project lifecycle, not at the end
Questions? Thank you!