DICOMwebTM 2015 Conference &
Hands-on Workshop
University of Pennsylvania, Philadelphia, PA
September 10-11, 2015

DICOM℠
Digital Imaging and Communications in Medicine

Keeping it Safe – Securing DICOM

Robert Horn, Interoperability Architect, Agfa Healthcare

Chair, DICOM Working Group 6, Base Standard

AGFA HealthCare

What is security?

- **Protecting data access (against unauthorized access)**
- **Protecting data integrity (against unauthorized changes)**
- **Protecting data loss (against unauthorized deletions)**
- **Protecting data availability (against denial of service)**
- **Protecting other systems (against indirect attacks)**

The threat environment is changing

- **Healthcare applications are now on the front line for malicious attackers.**
  - **Old attitude of “they won’t attack us” is wrong.**
  - **Hiding behind firewalls is becoming insufficient.**

What are the implications if security is compromised?

- **Data corruption and loss**
- **Fraud against those victimized**
  - **Approximate median cost to a patient from stolen medical identity: $14,000 (2014)**
- **Civil penalties (fines and lawsuits)**
  - **Some fines over $1,000,000 in 2014 (US)**
- **Criminal penalties**
  - **Multiple felony convictions (over 1 yr) in 2014, (US)**
- **Serious harm and death**

Simple workflow

- Modality transmits images to archive
- Radiologist requests images for reading

 : Out to cause security issues

DICOM Security Profiles

- **Defined in PS3.15, “Security and System Management Profiles”**
- **Describes methods to mitigate various security concerns**
- **Items in red describe solutions that are used in the industry but not explicity part of the DICOM standard**

DICOM in Transit (unprotected)

Who sees this image?

- The modality, who sends the image
- The archive, who receives the image
- Anyone on the network between

DICOM-TLS

- Transport Level Security encryption (defined in PS3.15 Section B.1)
- Encryption algorithm and temporary key is negotiated using public certificates as part of TLS
- Traffic is encrypted using temporary private key
- DICOMweb should use TLS (aka HTTPS)
- Network VPN tunnels and VLAN are other network protection mechanisms

DICOM in Transit (Authentication)

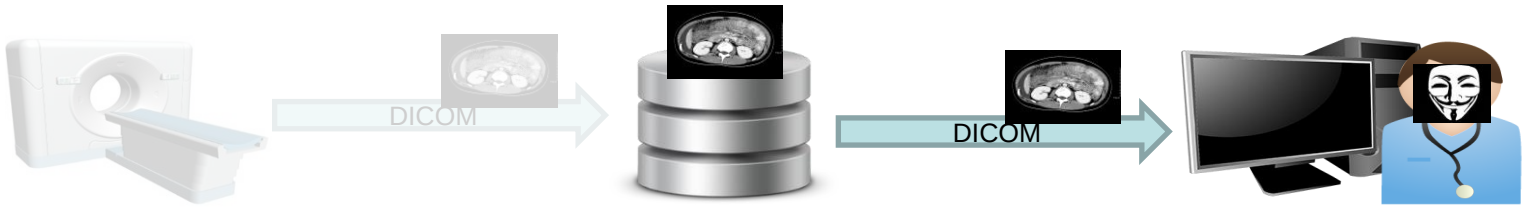
Who are the actors in transmission?

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

Node Identity (Authentication)

- **DICOM-TLS certificates provide identifying information about the end point machines**
- **Certificates may be self-signed, private CA signed, or public CA signed. Private CA and self-signed are more appropriate for healthcare.**
- **AE title verification is a weak authentication alternative if TLS is used**

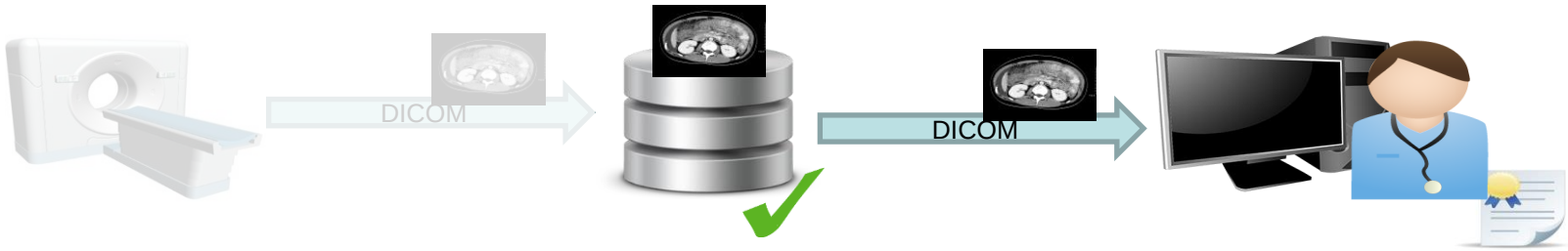
User Authentication



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 plus local authentication (trust a known counterparty)
  - Authentication during association negotiation (SAML, Kerberos, etc)
  - OAuth when using DICOMWeb
- 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**
- **Logs must be analyzed, not just gathered.**

DICOM at Rest

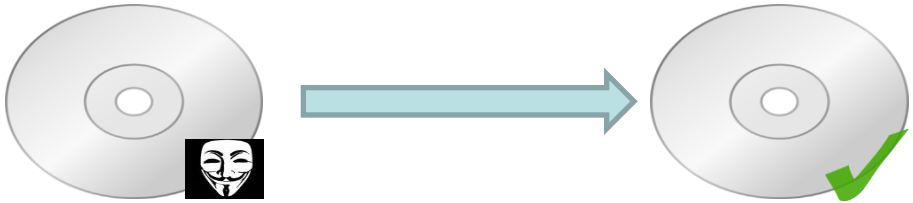
Who ensures the images are genuine as the modality provides them?

- **The creating device**
- **Anyone 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**

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**
- **Disk-level encryption can also be used to maintain protection for both removable media and built-in media.**

Anonymization

- **Anonymization profiles exist to support masking of data for various purposes**
  - **Clinical trials**
  - **Teaching files**
  - **Risk Reduction**
- **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 does the same 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**
- ✓ **Consider government guidance, e.g. DISA STIGs, NIST 800 series.**

Useful Guidance Links

- **More and more general guidance is available**

- **Manageable Network Plan**
  - **https://www.nsa.gov/ia/mitigation_guidance/security_configuration_guides/networks.shtml**
- **NIST 800 family**
  - **http://csrc.nist.gov/publications/PubsSPs.html**
- **DISA**
  - **http://iase.disa.mil/stigs/Pages/index.aspx**

Questions? Thank you!