DICOM
Digital Imaging and Communications in Medicine

DICOM Security Demonstration:

Secure Transport Connections and Digital Signatures

Sponsored by the NEMA Committee for the Advancement of DICOM and DICOM Working Group 14

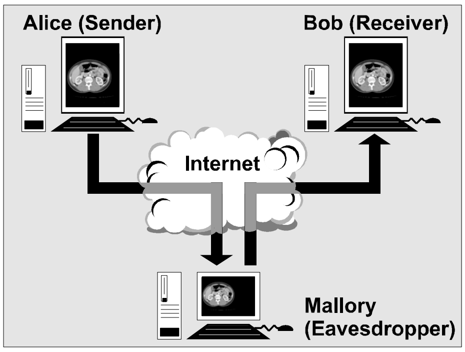
Introduction

Working Group 14 of the Digital Imaging and Communications in Medicine (DICOM) committee has developed two extensions to the DICOM standard for implementing secure transport connections and digital signatures. These extensions will allow applications to exchange and archive DICOM data such as images or diagnostic reports in a secure fashion. This ECR exhibit contains an implementation of the DICOM extensions as specified in Supplement 31 and 41 as a technological proof of concept and for educational purposes.

Secure Communication

The demonstration consists of two scenarios. The first one shows three networked workstations. Two of them, “Alice” and “Bob” (see figure), run software that allows them to load and display DICOM images and structured reports, to edit the reports and to exchange images and reports over the network using DICOM network transmission. The software allows the use of either a conventional DICOM communication or a secure DICOM communication, based on the Transport Layer Security (TLS) protocol standard.

The third workstation, “Mallory”, relays all transmissions between Alice and Bob as an Internet router would do. When Alice and Bob transmit reports with conventional DICOM communication, Mallory can eavesdrop and see confidential information from the reports or even modify data during transmission without Alice or Bob noticing the modification. Additionally, Mallory can claim to be Alice and send fake reports to Bob, who cannot tell the difference.



DICOM Security Demonstration Scenario

When Alice and Bob switch to secure DICOM communication *without* encryption, Mallory can still eavesdrop, but any attempt to modify data is immediately noticed by Alice and Bob. Mallory also cannot claim to be Alice, because this would require a copy of Alice’s secret key, which is never transmitted over the network.

Finally, when Alice and Bob switch to secure DICOM communication *with* encryption, Mallory is completely “locked out” – even eavesdropping does not work anymore because all data is transmitted in encrypted form, and the encryption keys are only known to Alice and Bob.

Digital Signatures

The second scenario demonstrates the usage of digital signatures. Alice creates a DICOM Structured Report, attaches a digital signature to it, and sends it to Bob using DICOM network transmission. Before displaying the received report, Bob verifies the validity of the digital signature in order to find out whether the document is really valid and authorized by Alice. If Mallory has intercepted and somehow modified the report, the digital signature is invalid and Bob’s workstation reports an error message.

Bob’s software is also able to detect if Mallory tries to sign a report and claim to be Alice. In this case the digital signature is valid but “untrustworthy” because the issuer of the keys that Mallory has used to create the forged signature, the so-called “Certification Authority”, is unknown to Bob. Again, Bob’s workstation reports an error message.

Technical Background

DICOM until recently has not defined any features to allow sites to exchange DICOM messages and objects in a secure fashion. DICOM Supplement 31 was developed to endow DICOM with a limited set of features that facilitate the secure exchange of data between sites. This supplement is a first step toward a more comprehensive secure environment within which DICOM could operate. This supplement addresses the following aspects of security:

- Authentication – verifying the identity of entities involved in a DICOM operation.
- Confidentiality – guarding the data from disclosure to an entity which is not a party to the transaction.
- Integrity – verifying that data within an object has not been altered or removed during transport.

The authentication is done by verification through a secure handshake protocol of the entities involved in the interchange of DICOM objects such as images or diagnostic reports. This secure handshake would be done during the establishment of a DICOM network association for exchanging messages. During the secure handshake protocol, the entities involved in a network association identify an encryption protocol and exchange session keys to be used during the association. Entities then use end to end encryption of the data with the session keys to guard the confidentiality of the data while it traverses the communications links. The encryption protocols used for network interchange might also include a message authentication code (MAC) or secure hash to further guard the integrity of the data.

Supplement 41, which is still a working draft, i. e. not yet part of the DICOM Standard, enhances the various DICOM information object definitions such as CT image, MR image or Structured Report, with a means of embedding digital signatures inside the DICOM "header". While Supplement 31 solely addresses issues of network communication security, digital signatures as defined in Supplement 41 are independent of the location or means of transmission of the signed objects.

A DICOM digital signature consists of a message digest ("digital fingerprint") of a DICOM object, encrypted with the private key of the signatory, and a certificate containing the signatory's identification and public key. Certificates must be issued by a trusted "Certification Authority" which guarantees the authenticity of the signatory's identification. Optionally, digital signatures may also contain an official "time stamp" guaranteeing that a signature has been created at or before a certain point in time.

Use of DICOM Security Extensions

There are several ways that secure transport connections may be utilized in a clinical environment:

- Exchanging of images and reports in a secure fashion between different institutions over the Internet.
- Reliable identification of communication partners within enterprise networks (e. g. for audit trail purposes)

Typical application scenarios for digital signatures are:

- Archival of legal documents such as diagnostic reports in purely digital form. For example, most European countries have legislation in place that allows the storage of legal documents in digital form if signed with digital signatures fulfilling certain quality criteria.
- Reliable identification of the author (signatory) of images and reports exchanged between different Institutions.

DICOM Security Working Group

DICOM Working Group 14 (Security) standardizes extensions to address security issues within DICOM. The working group's goals have been to utilize commonly available mechanisms to add security aspects to DICOM. The initial output of this work has been Supplement 31, Secure Transports dealing with secure transport connections and Supplement 41, Digital Signatures dealing with lifetime integrity checks of DICOM objects such as images or diagnostic reports.

Future Activities

DICOM Working Group 14 is currently working on several other DICOM supplements including DICOM Supplement 51, Media Security and DICOM Supplement 55, Attribute Level Confidentiality. There may be future demonstrations including these supplements. Copies of these supplements can be obtained at NEMA's web site: http://medical.nema.org/dicom.html.

Acknowledgements

The European Congress of Radiology (ECR) has supplied the exhibit space for this demonstration.

The National Electrical Manufacturers Association (NEMA) coordinated contracting for the demonstration, which was sponsored by the Committee for the Advancement of DICOM based on work done by DICOM Working Group 14.

Monetary support was supplied by the following companies:

Eastman Kodak

GE Medical Systems

Marconi Medical Systems

Merge Technologies Inc

Philips Medical Systems

Siemens Medical Systems

Monitors were supplied by BARCO.

This implementation was developed by OFFIS and the University of Witten/Herdecke, the Institute for Microtherapy with project management provided by OTech Inc.

Institute for Microtherapy

OFFIS

OTech, Inc.

For further information, contact Vicki Schofield at NEMA: vic_schofield@nema.org

NEMA
Setting Standards for Excellence

After the demonstration, the source code developed with the supplied funding will be made freely available on the Internet at the following URLs:

http://www.microtherapy.de/go/dicomscope/
http://www.offis.de/projekte/dicom/
ftp://dicom.offis.uni-oldenburg.de/pub/dicom/offis/software/