DICOM
Digital Imaging and Communications in Medicine

DICOM Security Demonstration: Secure Transport Connections

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

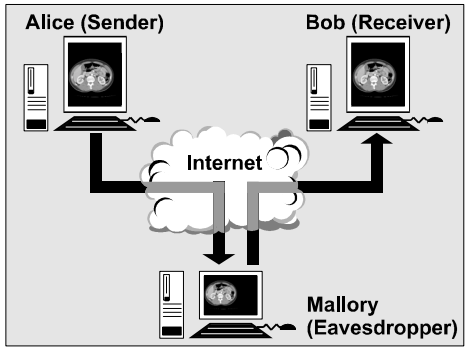
Introduction

Working Group 14 of the Digital Imaging and Communications in Medicine (DICOM) committee has developed an extension to the DICOM standard for implementing secure transport connections. This will allow applications to exchange DICOM data such as images or diagnostic reports in a secure fashion over the Internet. It also will allow authentication of the source of data and insure that data has not been changed during transport. This InfoRAD exhibit contains an implementation of the DICOM extension as specified in Supplement 31 as a technological proof of concept of this DICOM Supplement and for educational purposes

The Demonstration

The demonstration will show three networked workstations. Two of them, "Alice" and "Bob" (see figure), will 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 according to Supplement 31, 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.

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.

Covering other security aspects requires a more comprehensive security policy including site guidelines and policies that are beyond the scope of the DICOM Standard.

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 en-

cryption protocols used for network interchange might also include a message authentication code (MAC) or secure hash to further guard the integrity of the data.

Note that guarding the confidentiality of data stored within an entity (e.g. workstation), though needed for more complete security, is implementation dependent and outside the scope of DICOM Supplement 31.

The supplement adds information to several parts of the DICOM standard. It also creates a new part to the standard that holds Security Profiles that are used to specify mechanisms and algorithms for providing security. Implementations may claim conformance to one or more Security Profiles.

Use of DICOM Secure Transport Connections

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)

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 SOP Instances such as images or diagnostic reports.

Future Activities

This demonstration will be expanded at the European Congress of Radiology (ECR) 2001. The ECR demonstration will include DICOM Supplement 41 – Digital Signatures. Digital Signatures allow authentication, or verification, of the identity entity that created, authorized, or modified a DICOM Data Set. Their main intended use is in signing DICOM structured reports.

DICOM Working Group 14 is also 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 Radiological Society of North America (RSNA) has supplied the InfoRAD 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

Philips Medical Systems

Siemens Medical Systems

Monitors were supplied by Clinton.

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.

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/