Secretariat: MITA
1300 North 17th Street, Suite 900, Arlington, VA 22209, USA
http://www.dicomstandard.org/
dicom@dicomstandard.org
+1-703-841-3259

MINUTES

WORKING GROUP 14 Security

Date and Time	Tuesday 24 September 2019 11:30 AM - 12:30 PM EDT
Presiding Officers	Rob Horn, Producer Co-Chair Lawrence Tarbox, User Co-Chair
DICOM Secretariat	Lisa Spellman, General Secretary, DICOM

Voting Members Present	**Represented by**
Canon Medical Systems USA	Kevin O'Donnell (Alternate)
Fairhaven Technologies	Rob Horn (Co-chair)
GE	Matthew Hillyer
JIRA	Akihiro Yomoda
MISAT	Chung-Yueh Lien
Siemens	Hans-Martin Von Stockhausen
Siemens GmbH	Andreas Klingler
Univ. of Arkansas, Med. Sciences	Lawrence Tarbox (Co-chair)
Voting Members Not Present	**Represented by**
ACR	James Philbin
Agfa	Bill Jacqmein
Canon Medical Systems	Scott Nitsche
CFDA	Jia Zheng
Change Healthcare	Elliot Silver, Roger Trevisan
GE Healthcare	Matthew Hillyer
Hologic	Jeff Garrett
Konica Minolta Healthcare	Michael Laconti
Laitek	Douglas Sluis
OFFIS	Marco Eichelberg
PHC Co. LTD	Katsuya Watanabe
Philips	Jeroen Medema
Philips	Ben Kokx
PixelMed Publishing	David Clunie
Siemens Healthineers	Mohammed Aleem
Supersonic	Damien Lerat
Stryker	Corey Cochran
Alternate Voting Members, Observers, Guests Present	
Guest	Benedikt Kampgen (Guest)
MITA	Zack Hornberger (Observer)
Philips	Nikhilesh Sonar (Observer)
Philips	Wim Corbijn (Guest)

1. **Opening**
   1.1 Open the meeting and roll call.
   1.2 Review of antitrust and patent rule.
   1.3 Agenda review and approval.
   1.4 The minutes from 17 September 2019 were approved with no changes.

2. **Content development:** The focus of today's call was to create a plan to develop a small library of security-related content that can be easily accessed to reply to requests for information, particularly time-sensitive requests from media as we've received several in 2019 and we expect more to come.

- Media needs: The group discussed the typical needs of media which includes content that tells a clear story which includes character, problem, and movement. White papers can be helpful as background information, but these typically are not a story; journalists want stories.
- The group agreed to develop a communications matrix to identify target audiences and topics which includes the audiences listed below (though not limited to – the list below was just a first-cut discussion)
    - Journalists
    - End-user, vendors
    - Researchers
    - General public

<Action 1> Lisa will help WG to create the first draft to get things going.

3. **Existing white papers**: MITA and DICOM created a series of white papers years ago – it was thought that it could be as long as 2009 - and indicated the need to review and update.

   https://www.medicalimaging.org/policy-and-positions/joint-security-and-privacy-committee-2/)

- There are currently 12 white papers on the site (see list below). The WG did a brief cursory look at all 12 and decided is made sense to start with two papers for review and update. It was noted that we will need more WG-14 members to participate and help with the various writing and review tasks.
    1. Remote Services in Healthcare – Use Cases and Obligations for Customer and Service Organizations
    2. Information Security Risk Management for Healthcare Systems
    3. Management of Machine Authentication Certificates
    4. Break Glass-An approach for Granting for Emergency Access to Healthcare Systems
    5. Patching OTSS Used in Medical Information Systems
    6. Defending Medical Information Systems Against Malicious Software
    7. Introduction to the NEMA HIPPA Business Associate Contract Sample Language
    8. Identification and Allocation of Basic Security Rules in Healthcare Imaging Systems
    9. Remote Service Interface-Solution (A) – IPSec over the Internet Using Digital Certificate
    10. Security and Privacy Requirements for Remote Servicing
    11. Security and Privacy Auditing in Healthcare Information Technology
    12. An Introduction to HIPAA

- It is felt that these look dated and can cause the reader to wonder if DICOM is outdated, so even if the content is still correct, the white papers cause doubt.
- It was noted that development and distribution of white papers may be a DICOM-specific activity or one that should be done jointly with MITA and even other partners such as SIIM – need to decide for each paper updated as we want to get end-user community input into white papers and other outreach, noting that the white papers are often targeted to hospital and end users.
- The group decided that the following two or three documents (from the list of 12) should be updated first.

Management of Machine Authentication Certificates

This paper helps healthcare providers and medical device engineering organizations decide how to use digital certificates to secure machine to machine communications.

- Perhaps we do this for DICOM. Do we note that people are not deploying TLS? Are they finding it too hard? And there could be other reasons as well.
- How many modalities have actually implemented TLS? It's on the laptop of the development engineers

Decision:

- **Content:** The group thinks the content for this document is mostly ok, but some updates are needed.
- **Look:** The look must be updated across all documents.
- DICOM only or joint with MITA?

Defending Medical Information Systems Against Malicious Software

This white paper informs both vendors (manufacturers and integrators of MedIS) and users (for example, hospitals and medical practices) about possible malware attacks and suggests ways to protect against them.

Decision:

- **Content:** The group thinks the content for this document is mostly ok, but some updates are needed.
- **Look:** The look must be updated across all documents.
- DICOM only or joint with MITA?

Identification and Allocation of Basic Security Rules In Healthcare Imaging Systems

This paper identifies a set of security and privacy rules that, if properly enforced by healthcare providers or their medical imaging Information Technology (IT), can help them meet their legal obligations.

- The group also discussed this paper as a possible next update as well. Discuss on the 15 Oct call.
- MITRE has its "Att&ck Matrix. How about developing an "Att&ck Matrix" for DICOM?

Decision:

- **Content:** The group thinks the content for this document is mostly ok, but some updates are needed.
- **Look:** The look must be updated across all documents.
- DICOM only or joint with MITA?

4. NSA Manageable Network paper

- This has been discussed on several past calls. The proposal is for WG-14, jointly with MITA, to create a white paper based on NSA Manageable Network Plan
- NSA created a high-level project plan. We propose to add details about how to use DICOM and MDS2 to help fill in the gaps. MITA will help to produce and promote.
- Target audience: Hospital CISOs
- Link to draft: Rob Horn started a rough draft, is in Meeting Folder for 15 May 2019 (Note: DICOM does not list link to meeting folders in the Minutes).
- Link to NSA site: https://apps.nsa.gov/iaarchive/search.cfm?criteria=manageable+network+plan
- Updates: Bill Jacqmein started a draft which was reviewed on the 17 Sept tcon. He is going to update based on the discussion.

5. Other general discussion notes for the development of shelf-ready content

- Possible top questions/topics of no more than 700 words:
- *"Why doesn't DICOM include security?"*
    - Tell a story about how it does through a story. The media wants the story to be 700 words or less
- "*What do I do when someone says "I've configured incorrectly?"*
- *" Hey administrator, have you looked at this…have you considered…?"*

- **One pager checklist paper**: For administrators, including PACS and CISOs to include a short, focused list, a one pager/check-list for PACS Admins and only coming from the DICOM side (noting which may be DICOM-only and which may need to be DICOM-MITA jointly developed.
  - The content and goal is to aim end users at the "**Manageable Network**" paper
  - Example: The real basics, Step 1: the real danger is connected to your network, many do not realize that they have holes, know your use case

6. NCCoE- NIST Cybersecurity Practice Guide SP 1800-24, Securing Picture Archiving and Communication System for public comment.

- The NCCoE has released the draft version of ***NIST Cybersecurity Practice Guide SP 1800-24, Securing Picture Archiving and Communication System*** for public comment.
- WG-14 members encouraged to review and share feedback
- Deadline: Public comments on the draft will close on **November 18, 2019.**
- https://www.nccoe.nist.gov/projects/use-cases/health-it/pacs
- https://www.nccoe.nist.gov/sites/default/files/library/sp1800/hit-pacs-nist-sp1800-24-draft.pdf
- Review comments received thus far
- WebEx tomorrow (25 Sept)

<Action 2>

2a. Lisa to send a notice to WG-14 members inviting them to make comment.

2b. Rob & Lawrence will also put together some comments– have ready by the 15 October tcon. It was noted that we know some companies will do formal for aspects that matter for them.

7. There was a discussion about HIP

- The discussion about NCCoE migrated into a discussion about HIP, some of these comments might be used in the DICOM response to NCCoE
- HIP to cloudy containerized deployments makes sense. Seeing a highly cloudy containerized work and maintaining IP addresses is difficult… is HIP a relevant technology for DICOM-based solutions?
- As DICOM moves into the cloud, what do we do about HIP?
- What do about IT management when have thousands of virtual machines being spun up & down?
- Noted is will require someone getting into deep details.
- Open a shared document for pointers to background materials and NCCOE might provide some more information on this. TLS seems to be missing.
- Comments on router-based implementation, VLAN,
- How do we describe where DICOM stops talking and beyond that, determine where we want to draw our boundary, there was discussion about how far into the ISO stack does DICOM go?
- It would stop at level 4, as we go through our current discussion, whether its level 4, 5, whatever, be able to describe the dotted line, explain switch-over/hand-off, it's the level 4 protocol which is TCP
- Can you describe which side of the line is HIP? The layering has gotten more complex.
- If look at a protocol like HIP, it adds another addressing layer, the host level rather than MAC level,
- We can write this as a story, which gets more attention as a dry layering, also need normative & policy
- Cannot get security from the network, that didn't happen,
- **Maybe WG-23 should address HIP**: Send a note to WG-10 to start a general discussion and get their feedback and then send to WG-23 if WG-10 agrees.

<Action 4> Lisa to work with Rob to draft request to WG-10 for discussion

8. **Messaging/education opportunity: Possible session at RSNA19 to address recent critical security topics**
   - Lawrence to provide feedback from Chris Carr.

9. **Ramping up WG-14 communication on "hot" security issues**
   - It was suggested that WG-14 create a DICOM security best practices document and update DICOM white papers and other relevant informational documents. It was noted that ProPublica is making cyber and health a regular beat and have reporters looking for issue, so we need to have these kinds of documents available quickly.

10. **White paper review:** Working title *"Medical Device Safety and Cybersecurity"*
    - Bill Jacqmein drafted and was reviewed on 17 September WG-14 tcon
    - Status update: To be reviewed again on the 15 October tcon.

11. **Update on letter from German Broadcasting / ProPublica**
    - No comments have been received from WG-10 members about the Greenbone article. Our intent is to communicate that that everything needed is already in the DICOM standard.
    - https://www.greenbone.net/en/unprotected-patient-data-on-the-internet-a-massive-global-data-leak/
    - http://www.greenbone.net/wp-content/uploads/CyberResilienceReport_DE.pdf

12. **DICOM Secretariat response to German magazine publisher Heise**
    - Peter Mildenberger and Andreas Klinger sent info about magazine press blaming DICOM for the issue - notes from Andreas below

      "Additionally, the renowned German computer magazine publisher Heise has a news on it which unfortunately makes DICOM responsible for this: https://www.heise.de/newsticker/meldung/Unsicher-konfigurierte-Server-leaken-Daten-von-Millionen-Patienten-4531255.html
      "Schuld daran ist konkret der aus den 80er Jahre stammende Kommunikationsstandard DICOM (Digital Imaging and Communications in Medicine)" (Which translates to: Concretely the communication standard DICOM, which dates from the 1980-ies, is to blame for this.) @Lisa Spellman: I recommend to send a note from the secretariat to the authordes@heise.de that this is not due to a fault of the standard but due to a misconfiguration, which by the way is also stated by the security researchers. (Or some excerpts of our answer to the BR/Propublica)…"
      Update: The letter below was sent to the author on 19 September from the Lisa Spellman as Secretariat. No response as of 20 September when this agenda was posted.

      Dear DES@heise.de, article author:

      I have just read your story, *Uncertainly configured servers leak data from millions of patients*, in which you state: "The culprit is the communication standard DICOM (Digital Imaging and Communications in Medicine), which dates back to the 1980s. This is inaccurate. Simply put, the DICOM Standard does not inherently pose a security risk. The Secure Connection capability (specified in DICOM for almost two decades) is very secure. Proper security, however, requires more than just technical measures. It requires the implementation of institutional plans and policies to address various aspects of security (for example: infrastructure, device configuration, procedures, policies, training, auditing and oversight). The actual implementation, deployment, purchase, maintenance and configuration of systems that implement the DICOM Standard are the responsibility of the product vendors and their customers. Further, it is the responsibility of the vendors to provide and maintain software implementations. In short, proper security is a shared responsibility between device manufacturers and health delivery organizations. To claim it's the sole responsibility of a standard is false. As such, we suggest you review the report from Greenbone.net which also confirmed that the sites did not use the DICOM Secure transport protocol.
      Importantly, properly securing an institution that might use the DICOM Standard goes well beyond the charter of DICOM and by extension, the responsibilities of its committee members. National Institute of Standards and

Technology (NIST) and National Security Agency (NSA) documents make clear that a technical interchange standard by itself cannot assure security. It can provide the means to facilitate the secure exchange of information, but ultimately security is dependent on the environment in which the standard is used. If users do not deploy, activate and maintain secure communications protocols, or do not protect keys on which those protocols are based, there can be no guarantee of security.

I urge you to correct your story or at the very least update it to reflect our comments.

Sincerely, Lisa Spellman

13. Digital Signature issue

- On hold for October tcons, after Bangkok meetings.

14. Expected Process activity, DICOM Section 8.4

- On hold for October tcons, after Bangkok meetings.

7. New Business/Old business

- No old or new business was presented, other than the NCCoE as earlier noted.

8. Next Meetings – tcons: (Usually the 3rd Tuesday, alternating times, 9-10am, 11am-12pm US ET)

TUE 15 October 2019, 9-10am US ET: https://global.gotomeeting.com/join/647966269

TUE 19 November 2019, 11am-12pm US ET: https://global.gotomeeting.com/join/734478813

TUE 17 December 2019: 3rd Tuesday is Tuesday 17 December 2019: **Do 9-10 or 11-12pm?**

10. Next Meetings - F2F

- None scheduled at this time.

11. Adjournment

- The call adjourned at 12:39pm US ET. Report prepared by Lisa Spellman, DICOM General Secretary. Report reviewed by MITA/NEMA general counsel: CRS, October 15, 2019.

Appendix: Carry over information that we don't want to lose

Use of ACME certificates at Connectathons, IHE ITI profile proposal

- There was a discussion on January's call regarding ACME Certificates and other methods.
- A proposal was sent to Eric Poiseau, TM, European Connectathon and Steve Moore, TM, NA Connectathon. Steve and John Moehrke requested more info and pushed back a bit. They would like to better understand the need and value. Secure communications have not taken off (1) users don't know to ask for it (2) Vendors not pushing it

Next steps:

- Rob and Lawrence will do a bit more thinking and put together additional documentation.
- They might also draft a white paper. Continue discussion later in 2019.
- Lawrence has a presentation at SIIM2019 that will also cover some of this.
- Rob suggested that a good next step may be to draft a threat model to explain when and where it makes sense to use ACME. Perhaps also tie this to the MITRE ATT & CK model as well.