Secretariat: MITA
1300 North 17th Street, Suite 900, Arlington, VA 22209, USA
http://www.dicomstandard.org/
dicom@dicomstandard.org

Minutes- Tcon

WORKING GROUP 14 Security

Date and Time	Tuesday 24 March 2021 11:00am-12:00pm US ET US ET
Presiding Officers	Rob Horn, Producer Co-Chair Lawrence Tarbox, User Co-Chair
DICOM Secretariat	Carolyn Hull, DICOM

Voting Members Present

Fairhaven Technologies	Rob Horn
Agfa	Bill Jacqmein
Medical Image Standards Association of Taiwan	Chung-Yueh Lien
GE Healthcare	Steve Nichols
Laitek Inc.	Douglas Sluis
AAPM/Univ. of Ark. for Medical Sciences	Lawrence Tarbox
PHC co.,Ltd	Katsuya Watanabe
JIRA	Akihiro Yomoda

Voting Members Not Present

Canon Medical Systems USA, Inc.	Scott Nitsche
Canon Medical Systems USA, Inc.	Kevin O'Donnell
Center for Medical Device Standardization Admin.,CFDA	Jia Zheng
Change Healthcare	Roger Trevisan
GE Healthcare	Hiroshi Kanamori
GE Healthcare	Jeff Anders
Hologic Inc.	Jeff Garrett
Konica Minolta Corporation	Tetsuya Iwata
Konica Minolta Healthcare Americas, Inc.	Michael Laconti
OFFIS - Institute for Information Technology	Marco Eichelberg
Philips	Ben Kokx
Philips	Elisabeth George
Philips	Jeroen Medema
PixelMed Publishing	David Clunie
Siemens Healthcare GmbH	Andreas Klingler
Siemens Healthineers	Mohammed Aleem
Stryker Communications	Corey Cochran
SuperSonic Imagine	Damien Lerat

Alternate Voting, Observers, and Staff Present

MITA/DICOM Carolyn Hull

1. **Opening**
   1.1 The meeting was called to order and roll taken.
   1.3 Antitrust and patent rule were reviewed per NEMA guidelines
   1.3 The agenda was approved.
   1.4 Review of minutes. Minute were approved by a vote.

2. **Any other new "hot issues" that have come up since the last WG-14 tcon?** Questions: With medical sites being under intense attack, anything DICOM-related?

   Microsoft vulnerability announced related to open-type fonts that might affect DICOM:

   https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/ADV200006

   https://kb.cert.org/vuls/id/354840/

   DICOM prohibits embedded fonts in images, but many DICOM implementations will depend upon system provided fonting like the Microsoft system.

3. **DSC discussion of article "Your DICOM Images have been hacked, now what?"** -AJR article is printed. Cover article, printed. Benoit doing webinar mid-April. Will accept any changes. The WG-14 in reviewed slides. RSNA section was accepted. Presenters: Steve Horii, Lawrence, and Benoit.

   Note: Should send out to IronGeek, and AJR probably holds copyright. The webinar is targeted for physicians as part of CME credit. Could ask if when the seminar is over, they'd be willing to release on a delay. Benoit could ask.

   Edit: Implemented by **some** manufacturers on "Slide 26: Confidentiality feature in DICOM standard…" not implemented by most customers. Add in slides

   On encryption of DICOM files-key distribution is a problem. Suggest insert: Encryption "**at rest"** of DICOM files. Suggest a talking point that getting certificate used to be difficult but now is easy.

   Slide 39: devices and workstations –add in workstations on right side. Doctors might not recognize that "device" includes things like workstations and tablets.

   Protecting Availability slide: slide 42: Discuss also issues with backing up 1,000 terabytes of image archives. Most hospital archives are many terabytes of images.

   Other organizations have also dealt with archives that can be petabytes - (see CERN article and NOAA weather satellite ground system designs).

   Eg: http://highscalability.com/blog/2014/2/3/how-google-backs-up-the-internet-along-with-exabytes-of-othe.html

   A*Send two articles to Benoit on this.

47- MFA (user authentication) needs special attention in medical context. This is a discussion point rather than a slide change.

49- Conclusion slide: Customers should use, vendors should implement security.

When we have the RSNA educational session we should request RSNA to publish this openly after it has been given for CME credit.

4. **MITA Cybersecurity update –** Did not discuss March 24

Collaborative White Papers – MITA/DICOM/JIRA/COCIR: Feedback from MITA Section (s).

- See the update from Zack passed on from 3/24 (in meeting older) on which they recommend keeping and removing.
- Next step for upcoming call. After completed, DICOM or MITA should contact JIRA and COCIR to see if they wish to collaborate again on these documents

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

5. **Development of shelf-ready content-** Did not discuss March 24

- This project still holds a high priority as it's important for DICOM & MITA to have these resources.

Action: 2/18: Discussion of table. The group ID'ed the first four topics were high priority. Rob to take the lead on "Why doesn't DICOM…" Other updates below.

Concept description:

- Develop a series of short documents – stories – around 700 words that can be posted on DICOM website as FAQ-type info and able to send to have these short pieces at the immediate ready when some issue blows up and media and others request written feedback with an ASAP timeline.
- **Audience**: These are not meant to be technical engineering papers. These are something a product manager or a regulator would read. ~700 words is about the length of an opinion piece, be able to give to media and use in an FAQ.

Topic / Title	Content to be included	Lead
Why doesn't DICOM mandate security"	– *Possible content: DICOM is not a regulatory body* – *Not always the best fit solution for a particular organization*	Rob
"How can I tell if my system is exposed?"	We describe how to do it.	Hans v on tcon 2019-12-17
"*How to turn on encryption and why"*	Different for modalities and PACs	Hans v on tcon 2019-12-17
"How an administrator could use SHODAN to find leaks"	– "*You've heard about all of those exposed DICOM ports, you can find out if any of yours are exposed at your institution. Enter info into Shodan & it will tell you the open ports and IP addresses..."* – Can be tricky if have dynamic IPs and such, but at least give them guidance	Bill, Zack to assist 2020-02-18 tcon
" Hey administrator, have you looked at X / have you considered…?"	– DICOM is not responsible for the deployment. We don't want to come across as defensive, rather, explain what the reader can do	
"What to put in an RFP".	– Ensure content doesn't stray into anti-trust territory. We think we can include content that is general, but helpful.	

	– Maybe just include hyperlinks to sections? Call out the preamble, gives the mindset, intent – this could turn into a nice short piece	
One-Pager Checklist	– Audience: For administrators, including PACS and CISOs. – 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 are to aim end users at **NSA 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 – **Status**: The WG started a draft on the call today (2019-12-17). –	

- **3/24 call: Get update on Hans-Martin's new questions/answers with information from the group**

6. **2 Factor authentication-**

7. **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 **NSA 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
   - **Review during 3/24 call**

8. **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. 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
   - **Status update:** Review during 3/24 tcon.

9. **Messaging/education opportunity: Possible session at RSNA20 to address recent critical security topics**
   - This session has been submitted.

10. **Digital Signature issue**

11. **Expected Process activity, DICOM Section 8.4**

12. **Potential new work item re: Profile/standardizing a user authentication scheme**

13. New Business/Old Business 8. Next Meetings – tcons: (Usually the 3rd Tuesday, please note alternating times, 9-10am or 11am-12pm US ET)

Tuesday 14 April 2020: 9:00am-10:00am US ET

10. Next Meetings - F2F

- None scheduled at this time.

11. Adjournment

12:00PM

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.

Reviewed by Counsel 6/11/21