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 17 December 2019 9:00 – 10:00am US ET
Presiding Officers	Rob Horn, Producer Co-Chair Lawrence Tarbox, User Co-Chair
DICOM Secretariat	Lisa Spellman, General Secretary, DICOM

Voting Members Present	**Represented by**
Fairhaven Technologies	Rob Horn (Co-chair)
PHC Co. LTD/JAHIS	Katsuya Watanabe (Voting
Siemens Healthcare GmbH	Hans-Martin Von Stockhausen (Voting)
Univ. of Arkansas, Med. Sciences	Lawrence Tarbox (Co-chair)

Voting Members Not Present	**Represented by**
ACR	James Philbin (Voting)
Agfa	Bill Jacqmein (Voting)
Canon Medical Systems USA	Kevin O'Donnell (Alternate)
Canon Medical Systems	Scott Nitsche (Voting)
CFDA	Jia Zheng (Voting)
Change Healthcare	Roger Trevisan (Voting)
GE Healthcare	Hiroshi Kanamori (Alt)
GE	Matthew Hillyer
Hologic	Jeff Garrett (Voting)
JIRA	Akihiro Yomoda (Voting)
Konica Minolta Healthcare	Michael Laconti (Voting), Tetsuya Iwata (alt)
Laitek	Douglas Sluis (Voting)
MISAT	Chung-Yueh Lien (Voting)
OFFIS	Marco Eichelberg (Voting)
Philips	Jeroen Medema (Alt Voting)
Philips	Ben Kokx (Voting), Elisabeth George (Alt)
PixelMed Publishing	David Clunie (Voting)
Siemens GmbH	Andreas Klingler (Alt Voting)
Siemens Healthineers	Mohammed Aleem (Alt voting)
Supersonic	Damien Lerat (Alt voting)
Stryker	Corey Cochran (Voting)
Alternate Voting Members, Observers, Guests Present	
MITA	Lisa Spellman (WG Secretary)
MITA	Zack Hornberger (Observer)
Philips	Nikhilesh Sonar (Observer)
Canon Medical Systems Europe BV	Keith Knight

1. **Opening**

1.1 Open the meeting and roll call.

1.3 Review of antitrust and patent rule.

1.3 Agenda review and approval.

1.4 We were unable to review minutes from 2019-10-15 and 2019-11-19 since we did not have quorum. The minutes have been posted for several weeks. If no requested edits or concerns are received by 2020-01-31, the minutes will be considered approved.

2. **Any other new "hot issues" that have come up since the last WG-14 tcon?**

- Rob noted that there continues to be a growing challenge of ransomware scooping up data before encrypted. Hospitals afraid of the bad publicity and of threat are failing to report these breaches.
- Ransomware has more levels of blackmail than people thought
- Hospitals need to report breaches. If they do not, it is a violation of HHS regulations. But hospitals are not always recognizing that a ransomware attack is also a breach that must be reported. The ransomware authors look for failure to report and make another request for money.

3. **DSC discussion of article "Your DICOM Images have been hacked, now what?**

- **The content below from minutes of DSC meeting held at RSNA19**
- **Article *"Your DICOM Images have been hacked, Now What?"***
- It was felt the article was a bit inflammatory, the more positive information came later in the article
- Moving forward: Should a letter to the AJR be written to clarify DICOM or Lawrence, Rob & Steve to clarify and damped the hype? It is believed AJR would be interested to publish.
- DICOM/MITA did submit a CV Report. Lawrence noted that the lead author was stating fact that two other reference papers claimed that DICOM had a vulnerability. It was noted that the issues are more often related to the deployment of DICOM and not DICOM itself

<Action 5 from DSC RSNA Meeting 2019-12-05>

- 5.1 Steve Hori indicated that he would discuss the matter with the lead author of the paper.
- 5.2 Ask WG-14 to consult with MITA Cyber to determine who best situated to address some of the negative outcomes regarding the article among some communities. Lisa will work with WG-14, Zack and ExComm on communication.
- https://www.dicomstandard.org/wgs/wg-14/

Discussion points from today's call

- The core of the DSC concern is that the article made it sound as if DICOM has serious security flaws and as already noted and as shared in writing to issues, the problem is typically not with DICOM, inappropriate use, such as unsecured ports, have been the source of problems.
- Per the DSC action item, Steve Horii plans to speak to the primary author to see if he would be willing to make a statement for clarification as the feeling is that a statement of "clarification" from the author will land better than something from DICOM which will make it sound defensive and we are not defensive, we simply want to be sure that end users understand and take steps to secure their systems
- Phrase as a "clarification" and add the qualifier – "improperly configured DICOM can have security holes"

<Action 1> Lawrence will check with Steve to see if the primary author agrees or not regarding the request to make a clarification statement.

4. **MITA Cybersecurity update (Zack)**

Yarra Rules: Feedback from MITA Section (s)

- Zack reported that the MITA Section passed on the idea of posting Yara Rules on the MITA website feeling that doing so would be a liability and a challenge.

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

- Zack reported that the MITA Section didn't know that these papers were on the NEMA website and we agreed the most WG-14 members didn't know either.
- They agree that these are dated, and they plan to review all of the documents and then let DICOM know which documents, if any, they would volunteer to help update.
- **Timeline:** MITA Section will review in January/February 2020

<Action 2>

2a. Zack will let WG-14 know around mid-February of the outcome of their review

2b. Then 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/)

- **WG-14 has identified the three white papers below as the candidates to 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.

- Do we note that people are not deploying TLS? Are they finding it too hard?
- How many modalities have implemented TLS? It's on the laptop of the development engineers
- **Content:** The group thinks the content for this document is mostly ok, but some updates are needed.
- **Look:** To be updated across all documents. Rob found the original WORD of the published PDFs

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.

- **Content:** The group thinks the content for this document is mostly ok, but some updates are needed.
- **Look:** To be updated across all documents. Rob found the original WORD of the published PDFs
- Anyone know where this WORD document is? July 8, 2003

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.

- MITRE has its "Att&ck Matrix. How about developing an "Att&ck Matrix" for DICOM?
- **Content:** The group thinks the content for this document is mostly ok, but some updates are needed.
- **Look:** To be updated across all documents. Rob found the original WORD of the published PDFs
- Rob found the draft for approval but change between the draft and editorial. Things like footnotes and such. It would be nice to have.

5. Development of shelf-ready content

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

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*	
"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	
" 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).	

<Action 3>

- Hans-Martin Von Stockhausen: Hans von volunteered to write rough drafts for the following and present for the January or February tcon. ***Thank you, Hans!***
- *"How can I tell if my system is exposed?"*
- *"How to turn on encryption and why"*

6. **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
   - **Status**: The WG started a draft on the call today

7. **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:** Reviewed on the call today and used part of this for the checklist and might also use for the RSNA Course Refresher proposal

8. **Messaging/education opportunity: Possible session at RSNA20 to address recent critical security topics**
   - Idea: Submit a Course Refresher request, carry over to next agenda, maybe invite someone from NCCOE to co-present for RSNA 2020.

Process to submit for consideration as an RSNA Refresher Course

- Review: Review the past courses to see what has not been offered in some time. The model is to usually place it later in the week and if catches on, it will often get moved to a better slot and run a few years.
- **Process:**
  - Send a brief abstract to the RSNA Refresher Committee with a proposal. It need not be a full-blown abstract but needs to be enough for them to stimulate some interest.
  - Send the abstract to programs@rsna.org
  - **Deadline:** There is not a set deadline for refresher courses, but they recommended that the concept/abstract be sent be end **of January/early February**. If the Curriculum Committee is interested, they will let submitter know and ask for more information and so on.
  - https://www.rsna.org/en/annual-meeting/abstract-submission
  - Phone number for questions: For US: 1-877-776-2227. Outside of US: 1-630-590-7774

To submit abstracts for RSNA20

- Call for Abstracts opens end of January 2020
- https://www.rsna.org/en/annual-meeting/abstract-submission

9. **Digital Signature issue**
   - On hold for future tcons.

10. **Expected Process activity, DICOM Section 8.4**
    - On hold for future tcons.

11. **New Business/Old Business**
    - No old or new business was presented.

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

Tuesday 21 January 2020: 11am – 12pm US ET: https://global.gotomeeting.com/join/435759061

Tuesday 18 February 2020: 9:00 – 10am US ET: https://global.gotomeeting.com/join/533760429

Tuesday 17 March 2020: 11am – 12pm US ET: https://global.gotomeeting.com/join/791748869

10. Next Meetings - F2F

- None scheduled at this time.

11. Adjournment

The call adjourned at 12:10pm US ET. Minutes prepared by Lisa Spellman, DICOM General Secretary.

Report reviewed by MITA/NEMA legal counsel: CRS, December 19, 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.