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 Wednesday 16 June 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

Present	First Name	Last Name	Organization	Voting Status
	Jeff	Romatoski	Acuotech	Observer
	Jos	De Baerdemaeker	Agfa HealthCare	Observer
Present	Bill	Jacqmein	Agfa HealthCare	Voting
	Jos	Jennes	AGFA HealthCare	Observer
	James	Philbin	American College of Radiology 4	Observer
	Robert	Godward	Apteryx, Inc.	Observer
	Tyler	Sutton	Apteryx, Inc.	Observer
	Patrick	Williams	Apteryx, Inc.	Observer
	John	Moehrke	By Light Professional Services	Observer
	Kevin	O'Donnell	Canon Medical Research USA, Inc.	Observer
	Jia	Zheng	CFDA	Voting
	Barbara	Macharia	Change Healthcare	Observer
	Elliot	Silver	Change Healthcare	Alt. Voting
	Roger	Trevisan	Change Healthcare	Voting
	David	Liu	DICOMSOFT CONSULTING LTD.	Observer
	Michael	Henderson	Eastern Informatics, Inc.	Observer
	Abhinav	Singh	Emids Technologies	Observer
	Nico	Bruining	European Society of Cardiology	Observer
Present	Robert	Horn	Fairhaven Technologies	Observer
	Masao	Murata	FUJIFILM Corporation	Observer

	Jeff	Anders	GE Healthcare	Observer
	Karl-Heinz	Fleischer	GE Healthcare	Observer
	Matthew	Hillyer	GE Healthcare	Voting
	Hiroshi	Kanamori	GE Healthcare	Alt. Voting
	Steven	Nichols	GE Healthcare	Observer
	Jouke	Numan	GE Healthcare	Observer
	Kjetil	Pedersen	GE Healthcare	
	Francisco	Sureda	GE Healthcare	Observer
	Elliott	Lavy	Harris Computer Corporation	Observer
	Takuro	Ono	Hitachi Medical Corporation	Observer
	Arnaud	De Kelper	Hologic Inc.	Observer
	Jeff	Garrett	Hologic Inc.	Voting
	John	Giese	Innolitics, LLC	Observer
	Ravindran	Padmanabhan	Innowave Healthcare Pvt Ltd.	Observer
	Lutz	Vorwerk	Institut fur Telematik	Observer
	Charles	Parisot	InteropEhealth	Observer
	Jörg	Riesmeier	IT Consultant	Observer
	Gunter	Zeilinger	J4Care GmbH	Observer
	Akihiro	Yomoda	JIRA	Voting
	Thomas	Guiot	Jules Bordet Institute	Observer
	Tetsuya	Iwata	Konica Minolta Corporation	Alt. Voting
	Michael	Laconti	Konica Minolta Medical Imaging USA, Inc.	Voting
	Harry	Solomon	Laitek	Observer
	Douglas	Sluis	Laitek Inc.	Voting
	Bronson	Hokuf	Laurel Bridge Software, Inc.	Observer
	T. Roger	Keane	Laurel Bridge Software, Inc.	Observer
	Peyman	Najmabadi	Leica Biosystems Inc.	Observer
	Aaron	Stearrett	Leica Biosystems Inc.	Observer
Present	Chung-Yueh	Lien	Medical Image Stds Association of Taiwan	Voting
	Zsolt	Hegyi	Mediso Medical Imaging Systems	Observer
	Mark	Halliday	Medtronic, Inc.	Observer
	Guy	Hembroff	Michigan Technological University	Observer
Present	Zack	Hornberger	MITA	Observer
	Luiza	Kowalczyk	MITA	Observer

	Lisa	Spellman	MITA	Observer
	Peter	Weems	MITA	Observer
	Mariza	Foster	MRI + Radiology Centre	Observer
	Yueh-Hsun	Shih	National Yang Ming University	Observer
	Marco	Eichelberg	OFFIS - Institute for Information Tech	Voting
	Michael	Onken	Open Connections GmbH	Observer
	Katsuya	Watanabe	PHC co.,Ltd	Voting
	Elisabeth	George	Philips	Alt. Voting
	Glen	Hodges	Philips	Observer
	Ben	Kokx	Philips	Voting
	Joe	Luszcz	Philips	Observer
	Jeroen	Medema	Philips	Alt. Voting
	Nikhilesh	Sonar	Philips	Observer
	Vinayachandra	Aithala	Philips India	Observer
	David	Clunie	PixelMed Publishing	Voting
	Michael	Owens	RefleXion Medical	Observer
	Masuyoshi	Yachida	Ricoh Corporation	Observer
	Rex	Kerr	rk-logix, inc	Observer
	Pim	Philipse	Rogan-Delft BV	Observer
	Angeline	Cosca	Sdmi	Observer
	Dezheng (Bruce)	Li (Lee)	Shanghai United Imaging Healthcare	Observer
	Andreas	Klingler	Siemens Healthcare GmbH	Alt. Voting
	Hans-Martin	von Stockhausen	Siemens Healthcare GmbH	Voting
	Nikolaus	Wirsz	Siemens Healthcare GmbH	Observer
	Mohammed	Aleem	Siemens Healthineers	Alt. Voting
	Stephen	Vastagh	Standards Management Company	Observer
	Corey	Cochran	Stryker Communications	Voting
	Damien	Lerat	SuperSonic Imagine	Alt. Voting
	Keith	Knight	Toshiba Medical Visualisation Systems	Observer
	Lawrence	Tarbox	University of Arkansas for Medical Sciences	Voting
	Nathan	Cross	University of Washington Medical Center	Observer
	Sebastian	Korber	VISUS Technology Transfer GmbH	Observer
	Jonathan	Whitby	Vital Images, Inc.	Observer
	Nicholas	Pons	VITEC Multimedia	Observer

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 mminutes from 29 May 2019 were approved with no changes.

2. **Status update and discussion on current security issues**

2.1 Discussion: CVE write-up

- The vulnerability of the DICOM file format was reviewed by MITRE and now has a Common Vulnerabilities and Exposures (CVE) number: CVE 2019-11687. It is felt that the majority of the write-up is acceptable, but there is concern over the last two lines. Rob reviewed a draft of the CVE summary description with a security firm; they honed-in on 1.8 exploitability score and Rob thought this was acceptably low.
- Rob showed a draft of an updated response and will post for people to review and make suggested edits.
- It was noted that the way it's written makes sound like a big deal, if people would configure their software properly, then would be much safer but how to say this nicely?
- Rob reminded that the WG agreed that it would be a good idea to identify a list of topics and create up to 700-word response that would be ready to post as needed or to preemptively post on DICOM website.
- Possible topics:
    - Here is a medical device, key issues/approaches you should be considering.
    - We need to have more education or awareness for security people, unless you've worked in a hospital, many of the issues are not as obvious
    - Where is the patient safety message? Patient safety is not a topic that vendors encounter unless they've spent time in healthcare setting. It would also be useful to add MITA/NEMA voice to this as well. Something like "Patient safety introduction for cyber-security experts"
    - Bill mentioned that he remembered a good presentation at RSNA 3-4 years ago, a medical doctor presenting on cybersecurity based around patient safety, this could be a good primer

<Action 1>

- Bill Jacqmein (Agfa) offered to draft a response focused on patient safety
- Timeline: Have a draft for review at July tcon

Next Steps

- **Review and comment**: ***Members, please review and comment on Rob's draft in today's meeting folder. Please focus on***
    - The first two sentences are in the write up and it sends people down the wrong path.
    - Make text persuasive to a MITA security person for why they should remove those two out of the CVE description

2.2 **Hackers simulate cancer in images**

- First reported in the Washington Post. There are steps end users can take to protect such as to use DICOM TLS or digital signatures or other data integrity checks www.theweek.in/news/health/2019/04/04/Researchers-hack-CT-scans-to-create-fake-cancers-in-imaging.html
- WG14 should draft a response to "Hackers simulate cancer in images" and collaborate with MITA, MITA PR and legal on response. MITA PR firm suggests that we write a response and/or another FAQ and publish on DICOM website. Stay under 700 words and target skill level of the reader

- As noted with the CVE discussion, we need to draft a series of short topics up to 700 words and good keyword tagging, people would start to find them and then if something more comes up, direct people
- This one would be more radiologist, and image quality focused, which gets to one of the real headaches with digital signatures. These have been part of DICOM and potentially are part of medical record for decades but are not used. Even if we get them widely used the old signatures subject is still a problem area. Medical records can last 30-50 years. No digital signature standard has lasted that long.

<Action 2>

- Lawrence Tarbox will draft a response.
- Timeline: To share at July tcon

3 Digital Signature issue (Lawrence, Rob)

- We are not going to update the security template at this moment; we are going to revamp the profiles. Someone needs to review the profile.

Discussion points

- Do a CP to update RFCs to tweak algorithm list, expand list of those not recommended
- If we want to deprecate, a note is not sufficient because a note is not normative. A note can add a section to outline recommended action and point to NIST and others for background
- Perhaps add additional notes as to why people are deprecating some signature methods and write a new section to explain how DICOM users can respond.
- Can we make a change like that without creating a new profile? If an entity were compliant last year, DICOM can't do something throw out of compliance next year. (This is why profiles are retired and new profiles created.)
- DS Profiles: Creator, Reader, Validator, Authorization.
  - Review attribute list to ensure is still appropriate
  - Should new profiles include the specific purpose of Signature?
- CID 7007 track reference for ETSI or ASTM, we need a CP. Wecan add codes & coding systems in CPs
- Do we need a new supplement, or do we need a CP to deprecate algorithms?
- Need a CP to add new purpose code
- Review the attribute list to ensure nothing has fallen through the cracks over the years. Probably retire and do a new, increases visibility if say retired old and here is a new
- If we think signatures are important, we need to give greater visibility
- We have a vote about what going to do is revamp DS but not necessarily require in Conformance Statement, so probably a supplement to retire and replace
- Add to TID 7007 to add to the Supplement. If the CP arrives before the Supplement, can cause confusion, if arrive together makes more sense. Rob has a copy of ASTM E2084 that he will review.
- Next month this falls in middle of AAPM, so Rob need to chair

<Next Steps> Continue discussion in July and August

4. Sup/209, Updating DICOM Conformance Template Security topics

4.1 CP on Section F.1 Basic Network Address Management Profile, specifically to clean section F.1.8 Conformance and maybe section F.1.5. **Lead**: Zack Hornberger (MITA)

Status: Zack submitted a draft (thank you, Zack). Rob reviewed and discussion for edits.

- Rob drafted a CP for WG-06 review, it will receive a CP number
- Document is in today's meeting folder should any members wish to review
- Rob will report with feedback from WG-06 at the June tcon
- This was not addressed on today's tcon. Rob will address in July.

4.2 CP on Section H.2 DNS Service Discovery to finish the section. **Lead :** Bill Jacqmein (Agfa)
Status: Bill sent a draft via email on 15 May (Thank you, Bill).

- Rob drafted a CP for WG-06 review, it will receive a CP number
- Document is in today's meeting folder should any members wish to review
- Rob will report with feedback from WG-06 at the June tcon
- This was not addressed on today's tcon. Rob will address in July.

4.3 Sup/209, Section 8.6 Expected Process activity, we decided that WG 14 should provide a paragraph about what should be seen in the document.
Leads: Rob and Lawrence will work on section 8.6

- Rob drafted a CP for WG-06 review; it will receive a CP number. Document is in today's meeting folder should any members wish to review. Rob will report with feedback from WG-06.
- This was not addressed on today's tcon. Rob will address in July.

5. White paper based on NSA Manageable Network Plan as a joint project with MITA

- 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: See Rob Horn draft in today's meeting folder.
- Link to NSA site: https://apps.nsa.gov/iaarchive/search.cfm?criteria=manageable+network+plan

<Action 4 >

a. Zack indicated that the MITA MII and Cyber committees are interested to from a PACs perspective
b. Bill Jacqmein is working on a draft reply.
c. Move to the July agenda as we ran out of time to discuss this today

7. New Business

- No new business was discussed.

8. Old Business

8.1 Use of ACME certificates at Connectathons, IHE ITI profile proposal

- A proposal was sent to Eric Poiseau, Technical Manager, European Connectathon and Steve Moore, Technical manager, 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
- There was a discussion on January's call regarding ACME Certificates and other methods.

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.

8.2 Possible response to Rik Primo article *"Cybersecurity in Medical Imaging-NovDec-2018.p29-32"*

- Security is a site problem that involves policies and procedures and discussed MDS2, it didn't mention DICOM or HL7 FHIR or IEEE11073 or TLS or TCP.
- It was suggested that DICOM WG14 could submit a response or article with the focus: For some of the issues, DICOM solves these 1, 2, 3…

Action/Next steps:

- Tabled to a future meeting

8. Next Meetings – tcons (3rd Wed each month, 9-10amUS_ET)

- There was a discussion to possibly move this can hour or two later to help west coast people attend – please discuss and determine if want to move the time to a bit later.

Wed 17 July 2019, 9-10am US ET
https://global.gotomeeting.com/join/278981725

Wed 21 August 2019, 9-10am ET
https://global.gotomeeting.com/join/490836789

9. Next Meetings - F2F

- None scheduled at this time.

10. Adjournment

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

Reviewed by MITA/NEMA legal counsel: CRS, June 27, 2019.