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 17 April 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
	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
Present	John	Moehrke	By Light Professional Services	Observer
	Kevin	O'Donnell	Canon Medical Research USA, Inc.	Observer
	Jia	Zheng	Center for Medical Device Standardization Administration,CFDA	Voting
	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
	Sergio	Santoro	Eurisko	Observer
Present	Robert	Horn	Fairhaven Technologies	Observer
Present	Masao	Murata	FUJIFILM Corporation	Observer
	Jeff	Anders	GE Healthcare	Observer
	Karl-Heinz	Fleischer	GE Healthcare	Observer
	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
Present	Akihiro	Yomoda	JIRA	Voting
	Thomas	Guiot	Jules Bordet Institute	Observer
	Tetsuya	Iwata	Konica Minolta Corporation	Alt. Voting
	Hitoshi	Yoshimura	Konica Minolta Medical & Graphic, Inc.	Alt. Voting
	Michael	Laconti	Konica Minolta Medical Imaging USA,	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
	Chung-Yueh	Lien	Medical Image Standards Association of Taiwan	Voting
	Zsolt	Hegyi	Mediso Medical Imaging Systems	Observer
	Mark	Halliday	Medtronic, Inc.	Observer
Present	Zack	Hornberger	MITA	Observer
Present	Luiza	Kowalczyk	MITA	Observer
Present	Lisa	Spellman	MITA	Observer
	Peter	Weems	MITA	Observer
	Yueh-Hsun	Shih	National Yang Ming University	Observer
	Marco	Eichelberg	OFFIS - Institute for InfoTechnology	Voting
	Michael	Onken	Open Connections GmbH	Observer
	Katsuya	Watanabe	PHC co.,Ltd	Voting
	Elisabeth	George	Philips	Alt. Voting
	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
Present	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
Present	Lawrence	Tarbox	University of AK for Medical Sciences	Voting
	Nathan	Cross	University of WaA 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 Minutes from 20 March 2019 were reviewed and approved with no changes.

2. **Announcements**
   - Members are welcome to share news of interest to the WG or questions.
     John Moehrke has a question – see new item 5 below

3. **Member survey reminder** (Lisa)
   - Lisa showed a member survey for WG-14. We ask members to please complete the survey – we need your feedback to help identify topics and activities of interest to WG-14 members. It is quick – just three questions with plenty of space for comments.

     Link to survey: https://www.surveymonkey.com/r/9DF2Q8K

4. **Japan Report, DICOM Book 2 (Akihiro Yomoda)**
   - Showed document and reviewed major sections. The document is in today's meeting folder.

5. **IHE question (John Moehrke)**
   - John had a question about Audit Message schema doing some FHIR-based changes. There was a brief discussion. It was determined that the valueless groupers should be removed.

6. DICOM security issue (Lawrence)

- An issue has come up. A security researcher has indicated and published on github that they have found a DICOM has a security flaw regarding the 128-byte preamble. Email copied below.
- This matter was picked-up by the media who gave us three hours for a reply which was published
- Lawrence and Rob explained the history of the matter.
- The question was asked: How big of a risk is this that someone would embed an executable? Brief discussion:
- It is worth it to warn people that do DICOM importers to check for malicious preambles

<Action 1>

a. Lawrence and Rob to create a response to send for the media request, share with the WG and then will reply to authors.

b. Lisa will also speak with Pat Hope, MITA Executive Director and see if we can loop in MITA's PR firm, Schmidt Communications and will also alert NEMA/MITA legal counsel.

Initial email:

From: Apostolos Bakoyiannis [mailto:paul.bakoyiannis@cylera.com] **Sent:** Monday, April 15, 2019 8:19 PM
To: General
Subject: DICOM File Format Flaw

Hello,
I'm Paul, part of a medical device cybersecurity startup named Cylera. One of our engineers recently uncovered an issue in the DICOM file format which allows the embedding of executable code due to the large 128-byte Preamble at the start of each file, which is large enough to fit a PE header.
We've reached out to NEMA and were also pointed to this address to contact as well. An initial draft of a technical paper discussing the issue can be found on the researcher's Github and we've posted a draft of our follow-up analysis and general discussion on our soon-to-be blog.
The issue is simple from a technical perspective, but if there are any questions we'd be more than happy to try to answer them. Since this is not something a software patch or document revision can resolve, we are releasing a set of detection signatures and cleanup tools so healthcare organizations can properly detect and remediate any existing malicious use of the issue in the wild. We would be happy to send your way first if you would like to distribute them as well.
Let me know if you have any questions. Best, Paul

Article published as a result of feedback from Rob and Lawrence (Thank you for the quick response)
https://www.healthcareinfosecurity.com/researchers-malware-be-hidden-in-medical-images-a-12388

7. Issue: Hackers simulate cancer in images

- This issue was big news. This is not DICOM specific, but of course is relevant and has appears in many posts and re-postings. The issue was first reported in the Washington Post.

https://www.theweek.in/news/health/2019/04/04/Researchers-hack-CT-scans-to-create-fake-cancers-in-imaging.html

Discussion

- There are steps end users can take to protect such as to use DICOM TLS
- It was agreed that a Task Group (TG) needs to be formed to address these and other issues as they arise.
  - TG members: Lawrence Tarbox, Rob Horn, Bill Jacqmein, Pim Philipse, Zack Hornberger, Lisa and Luiza. Will also Cc: Kevin O'Donnell and Ken Persons from WG-10.

- Take on task of identifying where WG-14 should reply
- Publish a letter to the editor or comment to the journal article (most permit this)
- Since this issue has appeared in the national press, we can send a reply to the editors and make that written info posted on DICOM website
- Other possible media outlets:
  - Aunt Minnie
  - If get lucky, may be able to publish as an editorial comment
  - GitHub
- April 30th at 9-10 am specific to work on responses to these two articles and try to have draft responses

<Action 2>

a. Task Group to Create a reply; find the right vehicle to point out features already have
b. Share with WG14 for feedback
c. Will also loop in MITA and PR firm, MITA/NEMA legal counsel

8. **MDS2 re-ballot**: A question was asked if WG-14 members had any comments about the new ballot - RFC 8520 MUD -- looks similar to MDS2 https://www.ietf.org/blog/mud/. There were no comments, but was put on today's agenda for discussion.

9. **Sup/209, Updating DICOM Conformance Template**:
   - Review draft updates
     - **CP on section F.1** Basic Network Address Management Profile, specifically to clean section F.1.8 Conformance and maybe section F.1.5
       - ***Zack Hornberger (MITA)***
     - **CP on section H.2** DNS Service Discovery to finish the section
       - ***Bill Jacqmein (Agfa)***
     - **Finally, on 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.
       - ***Rob and Lawrence will work on section 8.6***
       - Update from 1 April meeting with Sup/209 during WG-31 tcon: Rob meet with the Sup/209 Task Group on Mon 1 April to discuss printing and security.

10. **White paper based on NSA Manageable Network Plan as a joint project with MITA**
    - Review drafts for discussion
    - 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/Next Steps>

- Zack will take to MITA MII and Cyber committee to seek volunteers from a PACs perspective
- Bill Jacqmein will start a reply based on today's discussion for review on the next tcon

11. **Agenda planning discussion**: What would members like to cover the on the coming calls?
    - Ran out of time to discuss on today's call. No new topics were presented since it was agreed the security responses have to be dealt with first.

12. New Business

- No new business was presented.

13. Old Business

9.1 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.

Action/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.

9.2 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:

- Did not have time to address today. Discuss in April or May.

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

Wed 15 May 2019
https://global.gotomeeting.com/join/118956565

Wed 19 June 2019
https://global.gotomeeting.com/join/895299237

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

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

15. Next Meetings - F2F

- None scheduled at this time.

16. Adjournment

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

Reviewed by counsel: CRS, May 2, 2019.