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 September 2019
11am – 12pm 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**
Agfa	Bill Jacqmein
Canon Medical Systems USA	Kevin O'Donnell (Alternate)
Fairhaven Technologies	Rob Horn (Co-chair)
GE	Matthew Hillyer
JIRA	Akihiro Yomoda
MISAT	Chung-Yueh Lien
Philips	Ben Kokx
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
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	Elizabeth George (Alt voting), Jeroen Medema
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 21 August 2019 were approved with no changes.

2. **Status update on MDS2** (Rob)
   - Publication expected the week of 30 September 2019.

3. **Review of WG-14 Change Proposals (CPs) in process**

CP1965, NTP Security considerations ***(recently assigned #1965)***
- Note: This is one of the items needed by the Sup/209 DICOM Conformance Template Task Group
- Status: Reviewed at recent WG-06 meeting. Not yet added to a voting pack. Remains assigned to Rob.

CP1947, Add security considerations for encapsulated formats (working title for now from Rob)
- Note: This is one of the items needed by the Sup/209 DICOM Conformance Template Task Group
- No technical changes, mostly editorial fixes.
- Status: It's a candidate for CPack-104 in November 2019 Voting Package.

CP1948, Part 10-format-security-considerations
- This CP deals with the malicious file format header issue that was addressed a few months ago.
- No technical changes, mostly editorial fixes.
- Note: This is one of the items needed by the Sup/209 DICOM Conformance Template Task Group.
- Status: It's a candidate for CPack-104 in November 2019 Voting Package.

New CP, number not yet assigned. Working title
Lead: Wim and Rob
- Was discussed at September WG-06 meeting.
- Overview: DICOMweb related. From a security perspective, this could potentially increase risk of exposing patient data, either exposing all if using TLS or info is inside a TLS wrapper. Not so much patient data are exposed, rather, URL and body can be exposed if TLS wrapper not used. Attack surface is important.
- There was a brief discussion about move-forward approach. Treat the log files as PHI.
- Agreement that it is important to provide clarity.

Action 1:

1a. Start a CP to update the security section in part 18 to describe these issues.
- The current TLS support protects the URL equally with the body.
- But, many Internet appliances such as proxies, caches, and load balancers, process the URL and log their activities. The administrators might be unaware of the PHI issues or improperly configure their appliances for PHI. Using the URL for queries usually includes PHI into the URL. Changing the query encoding to use a POST with the query as part of the body reduces the associated risk. The Internet appliances and administrators usually treat the POST body and reply as private information.
- The issue is whether we should revise the query approach to reduce this attack surface.

1b. Alert WG-27 to review. Issue: query in the URL versus query in the body for protecting PHI. Consider whether the protocol should change to reduce the attack surface.

4. **NIST**

Issued draft available and open for comment. WG-14 members to review and share feedback
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

Action 2:

- Lisa to circulate the document and request feedback. Then discuss at the 19 Oct WG-14 tcon
- Security deadline to reply: **17 NOV 2019**

5. **Update on letter from German Broadcasting / ProPublica**
   - DICOM Secretariat received inquiry. We quickly assembled a response task group and met the requested deadline. The final letter was sent to entire DICOM Community ~ 2,100+ in mailing list.
   - We think they now understand that the responsibility lies with the end user to implement the available security protocols.

   Next steps:
   - Since some groups may hear only fragments of this discussion, WG-14 will work with WG-29 to help ensure breadth of communication. For technical aspects, we can work with SIIM, RSNA and others to help communicate.
   - See if we can do a session at RSNA19: This information is important to the typical RSNA attendee including radiologists and other end users. We believe this topic will continue to have media pick-up. Lawrence will ask Chris Carr if we could provide a brief update to discuss the importance of end users securing their systems.
   - Article: Lawrence and Rob are secondary co-authors on an article that was accepted by American Journal of Roentgenology (https://www.ajronline.org/). This information can be shared once published.

   Action 3:

   3.1 RSNA19: Lawrence will contact Chris Carr about having a special session at RSNA.

   3.2 Greenbone article: Members are asked to please review Greenbone article. Share with WG-14 and will be discussed on October tcon.

   http://www.greenbone.net/wp-content/uploads/CyberResilienceReport_DE.pdf

   3.3 Ongoing communication: Since these topics are will continue to circulate, work with WG-29 to communicate security update topics.

6. **Communicating security issues**
   - It was suggested that WG-14 create a DICOM security best practices document.
   - It was noted that we should evaluate need to update DICOM white papers and other 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.
   - Peter Mildenberger sent an article which is blaming DICOM for the issue

7. **White paper review:** Bill Jacqmein reviewed a draft paper he wrote for consideration, working title *"Medical Device Safety and Cybersecurity"* to review some of the differences between cybersecurity IT versus medical devices. Review updated draft that was circulated.
   - Q: Intended audience for this document? A: Cybersecurity person reviewing a medical device that is looking for vulnerabilities. The intent is to focus this paper at organizational security people, how should I structure/frame my analysis. "Here are the broad categories of risk to understand…"
   - It was noted that we need to develop some small "chunks" of content to allow for quick response. Identify: Intended audience, desired action, question from a reporter: here is an answer – content easy

to adapt if needed, have like a set of FAQs for easy access; "why is cybersecurity for healthcare different? Why is this not the same as what a developer might have done for a bank, for example.

- We have already had three major media issues in the past six months that are not DICOM issues, but media usually goes there first.
  - Cancer injector, 128-Byte, ProPublica/German
  - End-users have the responsibility even if you have outsourced,
  - Need: "Here is our fact sheet, do with MITA Cyber so manufacturers can use. Here are questions we are seeing and so on…"
- List resources

8. Digital Signature issue

- On hold into October tcons, after Bangkok meetings.

9. Expected Process activity, DICOM Section 8.4

- On hold into October tcons, after Bangkok meetings.

7. New Business/Old business

- No new or old business was presented.

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

10. Next Meetings - F2F

- None scheduled at this time.

11. Adjournment

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

Report reviewed by MITA/NEMA legal counsel. CRS, September 18, 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.