2021-03-18 Minutes

Attendees:

Voting Participants: Mark King, Mark Hapner, Richard Wilsher, Ken Dagg, Martin Smith

Non-voting participants: Tim Reiniger, James Jung, Pete Palmer

Guests: Rene McIver (SecureKey)

Staff: Colin Wallis, Ruth Puente

Quorum: 3 out of 5. There was quorum.

Agenda

Administration:
Roll Call
Agenda Confirmation
Minutes Approval 2021-03-11 DRAFT+Minutes

2. Discussion

a. Review NISTIR 8344 (Ontology for Authentication) available at https://nvlpubs.nist.gov/nistpubs/ir/2021/NIST.IR.8344-draft.pdf (Deadline to comment: April 9, 2021)
b. NIST open discussion issues in light of SP 800-63 rev.4: https://github.com/usnistgov/800-63-4/issues (Deadline to comment: May 15, 2021)
c. Kantara 63B_SAC subset vs NIST source text (clarification request).

3. Any Other Business

Minutes Approval

2021-03-11 Minutes were approved by motion. Moved: Mark King Seconded: Mark Hapner. Unanimous approval.

Review NISTIR 8344 (Ontology for Authentication)

- Doc: https://nvlpubs.nist.gov/nistpubs/ir/2021/NIST.IR.8344-draft.pdf
- Deadline to comment: April 9, 2021

- Martin found the breakdown confusing. He added that the words "entity" and "object" are not clearly defined and they're not in a glossary. He said he was hoping to see a more fundamental discussion of what are we trying to accomplish with authentication because is often overestimated. He thinks it would be useful to drill down into that.
- Mark King: It's useful to have a coherent position because the definition of authentication varies from person to person and country to country.
- Mark K: Line 1157 "However, there appear to be two solutions: anything or “two-factor” authentication". What "anything" means?, he believes a word is missing.
- Mark K: Lines 624-626 "Two major forms of digital signatures are DSA and PKI. However, Merkle signatures schemes are often used for blockchain protection against change". This is confusing.
- IAWG agreed that it seems like a lot of theory that hasn't been thought through and in a coherent matter.
- Richard pointed out that the practices have not been adopted by service providers, it seems impractical to meet a pseudo normative standard based on a theoretical paper.
- Several participants have issues with the authorization part.
- Ken pointed out that some things could not be feasible at present but are there, similar to 800-63 rev3.
- Mark H. commented that there is an explosion of authentication mechanisms with personal devices and other services on the web that work.
- Mark K. added that in terms of definitions.ISO SC27 has collated those and made those public admittedly technically in the security area, they should state how this document is different to that or not.
- Some participants think that this document is not an ontology.
- It is not clear what's the purpose of this document.

63B_SAC issues

ARB questions on two 63B_SAC criteria, 63B#0030 and 63B#0150.

1.Re 63B#0030 – The KI criterion and NIST source text says this criterion is limited to Agencies. ARB wonders if this could be considered for any CSP.

- Richard explained that originally, when they did 63B_SAC, they didn't have the choice of roles. They only had the assumption that it was a CSP. They introduced this new criterion with the last revision, stimulated by the creation of the 63C criteria, which assigns criteria to various roles within the Federation. So, the four roles are derived directly from the roles identified in 63C. For consistency reasons, they chose to replicate those four roles in 63A and 63B SACs.

- IAWG does not want to change this because they don't have any grounds for making it applicable to CSP or maybe RPs as well, because the NIST requirement clearly says “Agencies”.

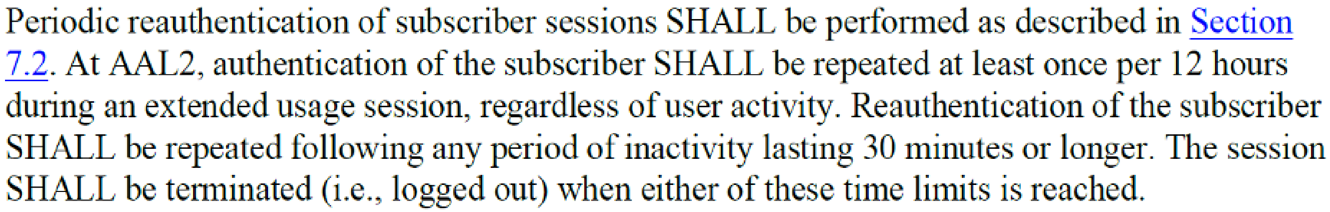
2. Re 63B#0150 - ARB pointed out that they are separate re-authentication requirements, not optional.

Kantara criteria:

“The RP SHALL terminate a session and the life of the current session secret whenever they are unable to receive affirmative re-authentication of the Subject, either:

1. a) prior to a period of session inactivity reaching 30 minutes; OR
2. b) prior to an extended usage session reaching 12 hours since the last successful re-authentication, regardless of user activity”.

NIST text:



Periodic reauthentication of subscriber sessions SHALL be performed as described in Section 7.2. At AAL2, authentication of the subscriber SHALL be repeated at least once per 12 hours during an extended usage session, regardless of user activity. Reauthentication of the subscriber SHALL be repeated following any period of inactivity lasting 30 minutes or longer. The session SHALL be terminated (i.e., logged out) when either of these time limits is reached.

- *Response from IAWG and Note added to the 63B#0150 criteria:*

[Note that EITHER of the conditions in a) or b) is grounds for the termination of the session and therefore the CSP must continue to check BOTH conditions in order to determine whether either has been breached.
The NIST text makes three separate statements but the third is conditional upon EITHER of the two preceding requirements being unsuccessful, but in fact is poorly expressed since termination is implicitly conditional on it not being possible to reauthenticate the user but this qualification is not stated - s written it could be found that termination SHALL occur after either 30 mins or 12 hrs (and the second case would never be true). This third 'SHALL' expression needs to be qualified by stating "if reauthentication fails", hence the Kantara clause is constructed as is and needs no change].

- It was clarified that the 63B#0150 only apply for RPs and not CSPs.
- Richard explained how they made that determination when developing the criteria: They have turned the NIST text around a little bit and had to invert the sentence structure of NIST text to better understand the requirement. IAWG analyzed the requirements and came up with a workable solution, because the goal is to have a reason to terminate. The RP shall terminate the session, whenever it is unable to receive affirmative re-authentication. So, if they don't get positive re-authentication either by not allowing a session to go beyond 30 minutes, or not allowing an extended section to go beyond 12 hours, then you terminate it. So although it says “either”, in order to accomplish the termination if either of these is achieved, or it becomes true, you actually have to test for each of them all the time. It was sustained that in this case, KI criteria are consistent and more accurate than the NIST requirement. Once authentication has been provided by the CSP, the RP has no participation in what that session is about. So it has to be the RP that stimulates the re-authentication and then terminates according to whether it does or does not get a successful response to that authentication.