IDS Working Group

2011-02-24 Conference Call Minutes

1. Attendees

Carmen Aubry	Océ
Nancy Chen	Oki Data
Andrew Mitchell	HP
Joe Murdock	Sharp
Glen Petrie	Epson
Brian Smithson	Ricoh
Jerry Thrasher	Lexmark
Bill Wagner	TIC
Rick Yardumian	Canon
Pete Zehler	Xerox

2. Agenda

Joe Murdock opened the IDS meeting and provided the planned agenda topics:

- Review Action Item status
- Discuss remaining IAA slides not covered at Feb F2F

3. Minutes Taker

Brian Smithson

4. PWG Operational Policy

It was noted that all attendees should be aware that the meeting is conducted under the PWG Membership and Intellectual Property rules. There were no objections.

5. Approve Minutes from previous meeting

Minutes from the previous meeting are at ftp://ftp.pwg.org/pub/pwg/ids/minutes/IDS-f2f-minutes-20110203.pdf.

There were no objections to the previous meeting's minutes.

6. Review Action Items

NOTE: The most recent Action Item spreadsheet is available at: ftp://ftp.pwg.org/pub/pwg/ids/ActionItems/ . Changes made during this meeting are indicated by red text or red-highlighted white text.

33	12/10/2009	Randy Turner Ron Nevo	SHV	Randy Turner will contact Symantec (when appropriate) to encourage discussion with the PWG about a SHV.		No longer blocked waiting for AI #32 so we can send market rationale to Symantec. Need a volunteer to take over on this task. Ron Nevo will take this task.

34	12/10/2009	Randy Turner Ron Nevo	Remediation	Randy Turner will investigate Symantec's products and their method(s) to "remediate noncompliant endpoints." Ron Nevo will take over this activity. Randy will pass on his contacts to Ron.		Symantec wants an NDA, but PWG cannot do an NDA; will do a generic version; should we invite Symantec to a PWG IDS teleconference? Need a volunteer to take over on this task. Ron nevo will take over this task. Need to indicate to Symantec that we really wdon;t need too much proprietary information from them, but want to give them our information. Can we get Symantec to attend the April meeting in Cupertino?
44	3/11/2010	Jerry Thrasher Ira McDonald Brian Smithson	NEA Binding	TCG TNC Binding document		Make it a TCG document, not an IETF NEA document
58	6/11/2010	Joe Murdock and Ira McDonald	SCCM	Create a first draft SCCM binding spec based on the NAP binding specC	H	MS is releasing R3 of SCCM and also a beta of "R-next", while at the same time adding power management; WIMS group may also be interested. On hold due to priorities.
67	10/28/2010	Joe Murdock Ira McDonald	auth	Write IDS-Identification-Authentication-and-Authorization-Framework specification	P	direction is not "recommendations only", it is "requirements and recommendations" (pointing to existing standards) because there will be a conformance section
69	12/2/2010	Michael Sweet	log format	Write HCD Logging specification	C	New draft Feb 2011
70	12/9/2010	Brian Smithson	admin	Make arrangements for F2F meeting with NIAP/other schemes at Ricoh SF during RSA week	C	
73	12/9/2010	Joe Murdock Ira McDonald Ron Nevo	reqts spec	start an IDS common requirements spec to include out-of-scope and terminology sections		Base on new PWG template
76	2/3/2011	Bill Wagner, Brian Smithson	MPSA	Data security article: Bill to draft, Brian to finish		
77	2/3/2011	Joe Murdock	NAP Binding	Needs a prototype		
78	2/3/2011	Joe Murdock	Log spec	Change name from IDS-CLF to IDS-LOG		
79	2/3/2011	Joe Murdock	Common Reqts	Change name from IDS-CR to IDS-REQ		
80	2/3/2011	Joe Murdock, Brian Smithson	WG admin	Update the description of the IDS WG to include scope that is larger than just NAC/NAP/etc		do this after Mike makes the new PWG web site and wiki pages
81	2/3/2011	Joe Murdock	IDS-LOG	Find the user role definitions in the IA&A or schema documents and refer to them in the LOG document		
82	2/3/2011	Brian Smithson	2600.1 SD	Revise the charter draft as describe in the Feb F2F minutes	C	

7. 2600.1 SD project

Refer to documents:
Draft project charter: ftp://ftp.pwg.org/pub/pwg/ids/wd/wd-ids2600sd-charter-20110223.pdf
Whitepaper: ftp://ftp.pwg.org/pub/pwg/ids/white/2600sd-20110223.pdf

Brian reviewed the updated project charter draft and the whitepaper that contained background material taken from the previous draft of the charter. There were no further comments.

At the RSA Conference, Brian met with Carol Houck and Shaun Gilmore of NIAP. NIAP has authorized a resource to work with us on the SDs, although that resource was not identified. Carol said that ours is an example of a technical community that wrote a PP which got international acceptance, so it's sort of a success story for their concept of technical communities. This may encourage NIAP to be receptive to the idea of making it work with the SDs as a way to promote their concept of tailored assurance.

Our next step is to propose dates/times for conference calls with NIAP. We discussed possible times for such conference calls, and it looked like we could schedule 2pm-3pm EST on Thursdays on alternate weeks from the IDS meeting. (Scheduling 1pm-2pm on those days would conflict with the WIMS meeting). Brian will propose this to NIAP.

New action item:

83	2/24/2011	Brian Smithson	2600.1 sd	Propose a schedule for teleconferences with NIAP		Alternate with SC meeting, Thursdays at 2pm-3pm EST

8. Document Status

- HCD-Assessment-Attributes
  - ftp://ftp.pwg.org/pub/pwg/ids/wd/wd-idsattributes10-20110127.pdf
  - Stable (needs a binding prototype)
  - Latest version fixed a simple typo
- HCD-NAP Binding
  - ftp://ftp.pwg.org/pub/pwg/ids/wd/wd-ids-napsoh10-20100930.pdf
  - Stable
  - Needs a prototype
- HCD-TNC Binding
  - Initial Draft still under development
- HCD-NAC Business Case White Paper
  - ftp://ftp.pwg.org/pub/pwg/ids/white/tb-ids-hcd-nac-business-case-20100422.pdf
  - Final
- HCD-Remediation
  - ftp://ftp.pwg.org/pub/pwg/ids/wd/wd-ids-remediation10-20100930.pdf
  - Initial Draft
- HCD-NAP-SCCM Binding
  - Specification on hold
- HCD-CLF
  - ftp://ftp.pwg.org/pub/pwg/ids/wd/wd-ids-log10-20110126.pdf

  - Draft
  - Recommended to change name to IDS-CLF
- IDS-Identification-Authentication-Authorization
  - Mind Map: ftp://ftp.pwg.org/pub/pwg/ids/white/ids-iaa-framework-20110202.xmind
  - Specification: ftp://ftp.pwg.org/pub/pwg/ids/wd/wd-ids-iaa10-20101202.pdf
- IDS-CR
  - Recommended to change name to IDS-REQ

9. Notes from RSA

Joe gave some informal observations from this year's RSA conference:

- There is a Gartner analyst for NAC, and he wasn't aware of anything that the PWG was doing. Now he is.
- Some people are using NAC to remove devices from the network instead of for admitting devices to the network.
- Along with the usual "something you have, something you know, and something you are" authentication factors, some systems are now also using "something you do". These systems look for behavioral anomalies.

10. Remaining slides from the F2F

Refer to ftp://ftp.pwg.org/pub/pwg/ids/Presentation/2011-02-03_IDS_F2F.pdf

There were some topics from the F2F that we didn't have time to cover:

- IAA: added claims-based authentication.
- Security ticket: added "organizational security", "physical security", and "cloud considerations".

These items should be reviewed by IDS members for discussion.

11. Summary of New Action Items and Open Issues

11.1 New action items

83	2/24/2011	Brian Smithson	2600.1 sd	Propose a schedule for teleconferences with NIAP		Alternate with SC meeting, Thursdays at 2pm-3pm EST

11.2 New issues

No new issues.

11.3 Old issues

1. How are administrators notified of remediation issues? Does the HCD ever initiate a notification, or is it always the remediation server that initiates notification? Does this same issue apply to policy servers?

2. What is a “fatal” error? Under what circumstances (if any) do we require the HCD to be shut down?

12. Wrap up and adjournment

The next IDS conference call is on Thursday, March 10, 2011, starting at 1PM EDT. After that we will have another call on Thursday, March 24, 2011, in preparation for April’s F2F meeting in Cupertino (at Apple).

IDS meeting adjourned.