IDS Working Group

2011-02-03 Face to Face Meeting Minutes

1. Attendees

Ron Bergman	emeritus
Nancy Chen	Oki Data
Peter Cybuck	Kyocera
Constantinos Kardamilas	Samsung
Ira McDonald *	High North / Samsung
Andrew Mitchell	HP
Joe Murdock	Sharp
Tyler Odean	Google
Shin Ohtake	Fuji Xerox
Glen Petrie *	Epson
Sanjeev Radhakrishman	Google
Brian Smithson *	Ricoh
Michale Sweet	Apple
Jerry Thrasher	Lexmark
Randy Turner	Amalfi
Bill Wagner	TIC
Rick Yardumian	Canon

* by telephone/LiveMeeting

2. Agenda

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

- 11:15 – 11:20 Administrative Tasks
- 11:20 – 11:30 Review action items
- 11:30 – 12:00 MPSA Survey and Article
- 12:00 – 13:00 Lunch
- 13:00 – 13:15 Document Status
- 13:15 – 13:45 System Logging
- 13:45 – 14:30 Common Criteria Evaluation
- 14:30 – 15:00 Identification, Authentication and Authorization
- 15:00 – 15:15 Break
- 15:15 – 15:45 IDS Security Ticket
- 15:45 – 16:00 Wrap up and adjournment

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

No minutes were produced from previous meeting.

There were no objections.

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.

34	12/10/2009	Randy Turner Ron Nevo	Remediation	Ron will take over, Randy will provide contacts.		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.
66	10/20/2010	Brian Smithson Joe Murdock Ira McDonald	admin	Create a project charter for creating IEEE 2600.1 Supporting Documents	C	Posted for discussion at Feb F2F
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	P	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		
71	12/9/2010	Joe Murdock	ATR	propose by email a multivalued attribute for log location (a URI) to be added to HCD-ATR	C	Posted for discussion at Feb F2F
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
75	1/13/2011	Joe Murdock Ira McDonald Bill Wagner	MPSA	MPSA Security article	C	Also a WIMS action item

7. MPSA Survey and Article

Most of this was handled during the previous session. We're now talking about a follow-up series of articles. The first of which will be data security. Later, others like cloud printing and green printing.

New action item:

76	2/3/2011	Bill Wagner, Brian Smithson	MPSA	Bill provides a draft of data security article, Brian finishes it		Also a WIMS action item

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

New action items:

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 Requirements	Change name from IDS-CR to IDS-REQ		

9. System Logging

Refer to ftp://ftp.pwg.org/pub/pwg/ids/wd/wd-ids-log10-20110126-rev.pdf

Miscellaneous changes were made – refer to the updated document.

Brian noticed that the description if the IDS WG, taken from the web site, is out of date and needs to have an appropriately expanded scope.

Randy pointed out that the definition of user roles more properly belongs in the IA&A document. Ira thinks that roles are defined somewhere in the MFD schema.

New action items:

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		
81	2/3	Joe Murdock	IDS-LOG	Find the user role definitions in the IA&A or schema documents and refer to them in the LOG document		

The System Log IDS health assessment attribute was also discussed (see slides). Among the questions:

- How is logging relevant to system health? The idea is that if a system isn't logging activities to a log server, then it is not fit to join the network. But it is proposed as an optional attribute.
- The URI can refer to a local resource? Yes, it could be file://.
- Does the presence of a log URI imply that logging is enabled? Or does it just mean that there is a place to put logs if logging was enabled? Another boolean would be required to indicate that logging is enabled.

Some edits were made to the description of the proposed attribute, including changing its name to "HCD_Security_Log_URI" (to distinguish security logs from other kinds of logs). Further discussion will take place on the IDS mailing list.

10. Common Criteria Evaluation

Refer to ftp://ftp.pwg.org/pub/pwg/ids/wd/wd-ids2600sd-charter-20110202.pdf

Comments:

- It was suggested that the problem statement is too long, but its content could be put into a white paper and be referred to by a shorter problem statement in this project charter.
- The last part of OOS-1 and OOS-2 were considered to be in conflict with OOS-3 (new SFRs or SARs would be difficult to accept internationally), and should be removed.
- OOS-3 is of primary importance and should be listed first in the list of OOS items.
- The last part of OOS-3 was questioned, but not resolved. Although it may be useful to present US-specific references such as to FIPS or NIST as guidance for addressing the US market, other international standards and specifications make reference to FIPS and NIST. This issue will need to be given further consideration.

- OBJ-2 and OBJ-3 need some work, because they state objectives that depend on the actions of people outside of the PWG. It would be better to state OBJ-2 as an objective to submit the SDs to NIAP for consideration (etc.), and OBJ-3 as an objective (contingent on OBJ-2) to seek a policy change from NIAP.

New action item:

82	2/3/2011	Brian Smithson	2600.1 SD	Revise the charter draft as describe in the Feb F2F minutes		

11. Identification, Authentication, and Authorization

Refer to ftp://ftp.pwg.org/pub/pwg/ids/white/ids-iaa-framework-20110202.xmind
and ftp://ftp.pwg.org/pub/pwg/ids/wd/wd-ids-iaa10-20110202.pdf

We ran out of time to cover this item.

12. IDS Security Ticket

Refer to ftp://ftp.pwg.org/pub/pwg/ids/white/ids-security-20110202.xsd

We ran out of time to cover this item.

13. Summary of New Action Items and Open Issues

13.1 New action items

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		
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		

13.2 New issues

No new issues.

13.3 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?

14. Wrap up and adjournment

The next IDS conference call is on Thursday, February 24, 2011, starting at 1PM EDT.

IDS meeting adjourned.