IDS Working Group

2010-06-11 Conference Call Minutes

1. Attendees

Nancy Chen	Oki Data
Ira McDonald *	High North/Samsung
Joe Murdock	Sharp
Glen Petrie *	Epson
Brian Smithson *	Ricoh
Michael Sweet	Apple
Jerry Thrasher	Lexmark
Ted Tronson	Novell
Randy Turner *	Amalfi
Bill Wagner	TIC
Rick Yardumian *	Canon
Pete Zehler	Xerox

* by phone

2. Agenda

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

09:00 –09:15 Administrative Tasks

09:15 –09:30 Review action items

09:30 –10:00 Document status and Review

10:00 –10:15 NEA and TCG Updates

10:15 –10:30 SCCM Binding Document

10:30 –10:45 Break

10:45 –11:00 MPSA Survey/Focus

11:00 –12:00 Standard Log File Discussion

12:00 –13:00 Lunch break

13:00 –14:45 Authorization Framework

14:45 –15:00 Wrap up and adjournment

Slides for this meeting: ftp://ftp.pwg.org/pub/pwg/ids/Presentation/2010-06-11a_IDS_F2F.pdf

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

ftp://ftp.pwg.org/pub/pwg/ids/minutes/IDS-call-minutes-20100603.pdf

There were no objections to the 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.

AI 033: Randy Turner will contact Symantec (when appropriate) to encourage discussion with the PWG about a SHV.

→ *No longer blocked, awaiting market rationale to send to Symantec (see AI #032).*
→ ***OPEN***

AI 034: Randy Turner will investigate Symantec's products and their method(s) to "remediate noncompliant endpoints."

→ ***OPEN***

AI 038: (For binding documents) Investigate localization issues.

→ *Cannot find any information about this in MS documents*
→ *Joe will add a localization attribute to the NAP binding spec*
→ ***Completed, CLOSED***

AI 041: (For Remediation) Look into providing a remediation URL.

→ *Joe has begun making an actual spec for remediation based on whitepaper*
→ ***Completed, CLOSED***

AI 044: (For NEA Binding) Recast the NEA Binding document as a TCG TNC Binding document.

→ ***OPEN, assigned to Randy Turner***
→

AI 045: Add HCD attributes to the system object in the MFD semantic model

→ ***Ira posted the XML Schema***
→ ***Completed, CLOSED***

AI 047: Take another look at SCAP and figure out what if anything to do in IDS

→ ***remaining OPEN, all IDS***

AI 048: Post a problem statement about authorization to the IDS list

→ ***Completed, CLOSED***

AI 049: Look at XACML

→ ***Completed, CLOSED***

AI 051: Compile wishlist for standard log content and format

→ ***Completed, CLOSED***

AI 052: Look at LogFS (http://www.logfs.org) and syslog (http://datatracker.ietf.org/wg/syslog/ and optionally http://www.syslog.org/)

→ ***remaining OPEN, all IDS***

AI 053: Do a brief overview and link to the market rationale for discussion/comment by MPSA (Jim Fitzpatrick)

→ ***OPEN, Joe Murdock and Bill Wagner***

7. Document Status

- HCD_ATR
  - ftp://ftp.pwg.org/pub/pwg/ids/wd/wd-idsattributes10-20100409.pdf
  - Stable (needs a binding prototype)
- HCD_NAP Binding
  - ftp://ftp.pwg.org/pub/pwg/ids/wd/wd-ids-napsoh10-20100608.pdf
  - 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
  - URL TBD
  - Initial Draft

8. Document Review

8.1 NAP Binding

ftp://ftp.pwg.org/pub/pwg/ids/wd/wd-ids-napsoh10-20100608.pdf

- Added section 5.1.3.3, HCD Natural Language attribute (page 22)
- Other changes were to fix up some incorrect numbers

Need to make the new attribute required in HCD_NAP and also add it to HCD_ATR.

AI 054: In HCD_NAP, Make language attribute required

→ ***NEW, Joe Murdock***

AI 055: In HCD_ATR, Add language attribute

→ ***NEW, Joe Murdock***

8.2 XML Schema

ftp://ftp.pwg.org/pub/pwg/mfd/white/health-20100525.xsd

In the case of multiple patches, each may need to be identified. It may not be representable as a simple sequence where one patch supersedes the previous patch.

AI 056: In MFP schema, Make simple element xxxPatches as a complex type sequence 0~n xxxPatch

→ ***NEW, Pete Zehler***

AI 057: In HCD_ATR, Patch attributes should be array of patches in order they are applied

→ ***NEW, Joe Murdock***

9. NEA and TCG Updates

No NEA update

TCG Updates: see slides

10. SCCM Binding Document

It was suggested that we make a separate binding document for SCCM:

- Start with the existing SCCM mapping paper
- ftp://ftp.pwg.org/pub/pwg/ids/white/IDS-NAP-SCCM-Mapping_20090917.xls
- Produce a formal document to map IDS Attributes to existing SCCM attributes

AI 058: Create a first draft SCCM binding spec based on the NAP binding spec

→ ***NEW, Joe Murdock and Ira McDonald***

11. MPSA Survey/Focus

Need to write introduction, and submit with the Business Case document. Bill Wagner has done similar work in WIMS and can offer guidance to IDS. Action item 053 changed:

AI 053: Do a brief overview and link to the market rationale for discussion/comment by MPSA (Jim Fitzpatrick)

→ ***OPEN, Joe Murdock ~~or Brian Smithson~~ and Bill Wagner***

12. Standard Log File Discussion

12.1 Discuss Brian's Log Standards Summary

ftp://ftp.pwg.org/pub/pwg/ids/white/IEEE2600.1_audit_events.pdf

- IEEE 2600.1 audit log requirements are fairly minimal
- It was difficult to even give examples or recommendations in a CC doc without risking an interpretation that the examples or recommendations are required functionality.
- IEEE 2600.1 has the most stringent requirements of the series 2600.1~2600.4.

12.2 Discuss Randy’s Log document

ftp://ftp.pwg.org/pub/pwg/ids/white/ids-logging.pdf

Logging is a useful capability for people who need to aggregate or review logs, and for those who are managing regulatory compliance.

- Mike will create a first draft, initial focus on security
- IEEE 2600 Appendix A.8 has additional information about security-relevant logging (NB: IEEE 2600 is the general hardcopy device/system security standard; 2600.1~2600.4 are protection profiles)
- We should identify the purpose of audit events, e.g., security versus accounting
- We are the Imaging Device Security WG, accounting may be better addressed by WIMS

AI 059: Create a first draft of a common logging specification

→ ***NEW, Michael Sweet***

13. Authorization Framework

Randy’s authorization document: ftp://ftp.pwg.org/pub/pwg/ids/white/ids-authorize.pdf

See slides 16~19 for discussion topics: ftp://ftp.pwg.org/pub/pwg/ids/Presentation/2010-06-11a_IDS_F2F.pdf

AI 060: First draft of potential resource predicate values

→ ***NEW, Joe Murdock***

14. Summary of New Action Items and Open Issues

New action items:

AI 054: In HCD_NAP, Make language attribute required

→ ***NEW, Joe Murdock***

AI 055: In HCD_ATR, Add language attribute

→ ***NEW, Joe Murdock***

AI 056: In MFP schema, Make simple element xxxPatches as a complex type sequence 0~n xxxPatch

→ ***NEW, Pete Zehler***

AI 057: In HCD_ATR, Patch attributes should be array of patches in order they are applied

→ ***NEW, Joe Murdock***

AI 058: Create a first draft SCCM binding spec based on the NAP binding spec

→ ***NEW, Joe Murdock and Ira McDonald***

AI 059: Create a first draft of a common logging specification

→ ***NEW, Michael Sweet***

AI 060: First draft of potential resource predicate values

→ ***NEW, Joe Murdock***

No new issues

15. Next meeting

The next IDS meeting is a conference call on June 24th, 2010, starting at 1:00pm EDT.
IDS meeting adjourned.