IDS Working Group

2010-08-06 F2F Meeting Minutes

1. Attendees

Nancy Chen	Oki Data
Ira McDonald *	High North/Samsung
Joe Murdock	Sharp
Glen Petrie *	Epson
Ole Skov	MPI Tech
Brian Smithson *	Ricoh
Michael Sweet *	Apple
Jerry Thrasher	Lexmark
Bill Wagner	TIC
Rick Yardumian	Canon

* attended by teleconference

2. Agenda

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

1. Administrative Tasks
2. Review action items
3. Document status and Quick Review
4. NEA and TCG Updates
5. MPSA Liaison discussion
6. Remediation Specification
7. Standard Log File discussion
8. Authorization Framework discussion
9. 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

ftp://ftp.pwg.org/pub/pwg/ids/minutes/IDS-call-minutes-20100722.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.

→ ***OPEN***

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

→ ***OPEN***

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

→ ***CLOSED, first draft posted***

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

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

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***

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

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

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

→ ***CLOSED, first draft posted***

AI 060:	First draft of potential resource predicate values

→ ***OPEN, Joe Murdock***

7. Document status and Quick Review

7.1 Status

HCD-Assessment-Attributes

- ftp://ftp.pwg.org/pub/pwg/ids/wd/wd-idsattributes10-20100712.pdf
- Stable (needs a binding prototype)

HCD-NAP Binding

- ftp://ftp.pwg.org/pub/pwg/ids/wd/wd-ids-napsoh10-20100712.pdf
- Stable

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-NAP-SCCM Binding
- Mapping Spreadsheet: ftp://ftp.pwg.org/pub/pwg/ids/white/IDS-NAP-SCCM-Mapping_20090917.xls
- Specification under development

HCD-Remediation
- ftp://ftp.pwg.org/pub/pwg/ids/wd/wd-ids-standard-remediation10-20100730.pdf
- Initial Draft

HCD-Authorization
- White Papers:
  - ftp://ftp.pwg.org/pub/pwg/ids/white/ids-authorize.pdf
  - ftp://ftp.pwg.org/pub/pwg/ids/white/ids-authorization-predicates-20100805.xlsx
- Specification under development

HCD-Log
- White Papers:
  - ftp://ftp.pwg.org/pub/pwg/ids/white/ids-logging.pdf
  - ftp://ftp.pwg.org/pub/pwg/ids/white/IEEE2600.1_audit_events.pdf
- ftp://ftp.pwg.org/pub/pwg/ids/wd/wd-ids-log10-20100803.pdf
- Initial Draft

7.2 Quick document review

7.2.1 IDS Attributes

ftp://ftp.pwg.org/pub/pwg/ids/wd/wd-idsattributes10-20100712.pdf

Firmware patches are listed in reverse order (newest first)
Ira pointed out that there is a problem listing them in reverse order because one can't insert a new first member of the list. WG agreed to change it to normal order (oldest first)

→ ***Action Item:*** *Joe Murdock to change the firmware patches list order from reverse to normal in both HCD-ATR and HCD-NAP.*

Attribute Natural Language was added as a mandatory attribute
This was reviewed at a previous meeting. No issues.

7.2.2 NAP Binding

ftp://ftp.pwg.org/pub/pwg/ids/wd/wd-ids-napsoh10-20100712.pdf

Firmware patches are listed in reverse order (newest first)
(Same issue/action as in Attributes document)

Attribute Natural Language was changed from optional to mandatory attribute
This was reviewed at a previous meeting.

Ira pointed out that this should have also been added to section 6, Conformance.

→ ***Action Item:*** *Joe Murdock to add Natural Language to the conformance list in HCD-ATR section 6.*

8. NEA and TCG Updates

There has been nothing new in the NEA WG except for a lengthy discussion about the Ashokan attack.

TCG updates were presented during the PWG Plenary.

9. MPSA Liaison discussion

Bill Wagner has been working on a plan for how to introduce PWG activities to MPSA. With regard to IDS, section 3 of the plan covers security issues and section 4 covers access and logging.

→ ***Action Item:*** *Bill Wagner to add the plan to a new section of the PWG wiki.*

10. Remediation Specification

ftp://ftp.pwg.org/pub/pwg/ids/wd/wd-ids-standard-remediation10-20100730.pdf

This is the first review of this document (i.e., there are no change marks because it is all new). Changes to the document were made during the meeting to create a new version. Significant changes or discussions are summarized below:

1. Ira suggested that the terminology section should refer to the HCD-ATR document instead of cutting and pasting, because the definitions may diverge. The terminology section would list only new terms that are used in this specification.
2. The WG discussed and decided that password remediation is not practical, so it was changed to simply inform the administrator.
3. What issues might occur if there are two NAP-enabled networks that had policy settings which conflicted with each other? Would the remediation servers fight it out? This might occur if the HCD shared firewall settings for all interfaces. Generally, however, the HCD would end up with the most restrictive settings for shared attributes and that would satisfy policies for both networks.
4. What happens if the trusted time source is changed, and the time value is significantly different? What should happen to secure connections or other processes that depend on time? What

happens to log entries that are time-stamped? It seems that the HCD should save jobs and do a soft reboot.

5. In cases where applications should no longer be enabled, there was a question about terminating applications that may leave something in an unstable or undefined state. The WG decided that "orderly termination" was a better requirement, and that some implementations may need to do a reboot to accomplish that termination.
6. When a device cannot be automatically remediated, how is the administrator notified? The WG decided that the device itself could not be expected to notify the administrator, and it would be the responsibility of the remediation server to do so. This is also true for cases where the device does not fulfill the policy requirements but that policy allows the device to join the network anyway.
7. For some attributes like vendor name or machine type model, what should happen if the HCD reports a different value? Is it a "fatal" error? Should the machine shut down? The WG decided to work on this off line.

→ ***Issue:*** *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?*

→ ***Issue:*** *What is a "fatal" error? Under what circumstances (if any) do we require the HCD to be shut down?*

11. Standard Log File discussion

ftp://ftp.pwg.org/pub/pwg/ids/wd/wd-ids-log10-20100803.pdf

This is the first review of this document (i.e., there are no change marks because it is all new). Changes to the document were made during the meeting to create a new version. Significant changes or discussions are summarized below:

1. The first discussion was about scope of effort for the IDS group. Common log format could encompass security audit, accounting, and maintenance logs. IDS is primarily concerned with security; WIMS would be concerned with the others. We could have a single specification to which both groups contribute or a specification that specifies format and protocol but not content and then the two groups do their own content specifications.
2. Rationale section will have general statements about why we want a common log format, then Use Cases would describe typical use cases (such as for security audit, accounting, and maintenance).

12. Authorization Framework

ftp://ftp.pwg.org/pub/pwg/ids/white/ids-authorization-predicates-20100805.xlsx

This is the first review of this document. It was an introduction with limited discussion. It defines three kinds of users (individual, group, and device), and provides a framework for defining how users are permitted to use resources associated with services or operations based on policies.

Discussion:

1. Ira suggested that other policy languages do not permit user privileges to be elevated above those of their group. More often, the privileges can be made more restrictive than those of their group.

2. Can a user can be member of more than one group? Answer: yes.
3. Is group was the same as role? The initial answer was yes, but then it was pointed out that role may imply permissions that are defined by a user's function within an organization, but group can also be used to delineate permissions that are defined by organizational boundaries. Both Role and Group would be useful; e.g., an administrator role in the Engineering group who does not have permission to administer the Manufacturing group.

13. Summary of New Action Items and Open Issues

13.1 New action items

AI 061:	Change the firmware patches list order from reverse to normal in both HCD-ATR and HCD-NAP

→ ***OPEN, Joe Murdock***

AI 062:	Add Natural Language to the conformance list in HCD-ATR section 6

→ ***OPEN, Joe Murdock***

AI 063:	Add the plan to a new section of the PWG wiki

→ ***OPEN, Bill Wagner***

13.2 New 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 meeting is a conference call on Thursday, August 19, 2010, starting at 1PM EDT.

IDS meeting adjourned.