IDS Working Group

2011-08-04 Face to Face Minutes

1. Attendees

Danny Brennan *	
Nancy Chen	Oki Data
Ira McDonald *	High North / Samsung
Joe Murdock	Sharp
Ron Nevo *	Samsung
Glen Petrie *	Epson
Amir Shahindoust *	Toshiba
Brian Smithson *	Ricoh
Jerry Thrasher	Lexmark
Bill Wagner	TIC
Rick Yardumian	Canon

* by phone

2. Agenda

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

- 9:00 – 9:15 Administrative Tasks
- 9:15 – 9:30 NAC Attributes
- 9:30 – 10:00 NIAP
- 10:00 – 11:00 TNC Document review
- 11:00 – 11:15 Short Break
- 11:15 – 12:30 Black Hat Embedded Security session web cast
- 12:30 – 13:15 IAA and Security Model
- 13:15 – 13:30 Summary

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-call-minutes-20110721.pdf. There were no objections to the previous meeting's minutes.

6. Review Action Items

The most recent Action Item spreadsheet is available at: ftp://ftp.pwg.org/pub/pwg/ids/ActionItems/. Action item updates are reflected in the updated action items spreadsheet.

7. Documents

7.1 Stable documents

- HCD-Assessment-Attributes
  - ftp://ftp.pwg.org/pub/pwg/ids/wd/wd-idsattributes10-20110127.pdf
  - Stable (needs a binding prototype)
- HCD-NAP Binding
  - ftp://ftp.pwg.org/pub/pwg/ids/wd/wd-ids-napsoh10-20100930.pdf
  - Stable
- HCD-NAC Business Case White Paper
  - ftp://ftp.pwg.org/pub/pwg/ids/white/tb-ids-hcd-nac-business-case-20100422.pdf
  - Final
- IDS Charter
  - ftp://ftp.pwg.org/pub/pwg/ids/charter/ch-ids-charter-201100503.pdf
  - Updated charter approved by Steering Committee

7.2 Active documents

- HCD-TNC Binding
  - Initial Draft still under development
- HCD-Health Remediation
  - ftp://ftp.pwg.org/pub/pwg/ids/wd/wd-ids-remediation10-20100930.pdf
  - Initial Draft
- IDS-Log
  - ftp://ftp.pwg.org/pub/pwg/ids/wd/wd-ids-log10-20110326.pdf
  - Draft
- IDS-Identification-Authentication-Authorization
  - ftp://ftp.pwg.org/pub/pwg/ids/wd/wd-ids-iaa10-20110801.pdf
  - Draft
- IDS-Model
  - ftp://ftp.pwg.org/pub/pwg/ids/wd/wd-ids-model10-20110524.pdf
  - Draft

We will retire the Remediation document from “active” and resurrect it if/when needed.

102	Joe Murdock	Remediation	retire the remediation document from the active list

8. NAC Attributes Extensions

9. NIAP Update

There has been no communication from NIAP's assigned people about the Support Documents (SDs), and we have not communicated with them either, since the kick-off meeting. Since NIAP rejected the idea of creating SDs with the objective to reinstate 2600.1 (plus SDs) at EAL3 as the US Government PP for HCDs, there seems to have been little motivation from vendors to pursue the project unless it has some benefit from the vendors' perspectives.

NIAP appears to be fully dedicated to EAL2 for now, and ultimately to eliminating EAL packages in favor of fully tailoring SARs to each technology area (e.g., HCDs). There remains some disagreement among the CC schemes about this approach to PPs. The US, UK, and AU/NZ schemes seem to be on board. Other schemes are either quiet or actively disagree.

The CC Development Board, composed of representatives from CC authorizing schemes, issued a "draft vision statement" earlier this year (introduction and link are here: http://www.commoncriteriaportal.org/communities/).

However, in a recent teleconference with members of the CC Forum (not the CC Vendor Forum), NIAP indicated that while this vision is being realized, NIAP will take the approach of (1) developing requirements in NSA, (2) translating into CC language as a PP, (3) accepting vendor comments, and (4) publishing the PP. This would appear to be a large step backwards, but at least NIAP acknowledges that "this is slightly different from the collaborative development methodology that is being advocated by the new statement from the CCDB".

There is some indication that IPA may be considering SDs, but it is not clear what is the status of their consideration or what is their purpose for SDs. IPA has written a detailed security analysis of MFPs (in Japanese only – there is no plan to translate to English: http://www.ipa.go.jp/security/fy21/reports/mfp/documents/20100830report.pdf).

Brian and Carmen are planning to attend the upcoming International Common Criteria Conference (September 27-29, near Kuala Lumpur, MY, see http://12iccc.cybersecurity.my/). Brian is presenting a status report on behalf of the "Hardcopy Devices Technical Community". Meeting with NIAP, IPA, and others, at the conference may help clarify the whole situation.

Brian will provide an update at the next face-to-face meeting, in October. In the meantime, this topic will be tabled.

Action items from this topic:

103	Brian Smithson	2600 SD	post URL for IPA research report on MFP security
104	Brian Smithson	2600 SD	post links to join CCVF and CCF
105	Brian Smithson	2600 SD	report on ICCC at October F2F

10. TNC Document review

Refer to:
ftp://ftp.pwg.org/pub/pwg/ids/wd/wd-ids-tnc10-20110804.pdf

Document review notes were captured by the author. A few issues that needed further consideration were added as action items:

106	Joe Murdock / Ira McDonald	TNC Binding	consider IANA registration procedure for PWG health attribute types and how to reference them in PWG specs, and registering new ones for binding-specific ones
107	Ira McDonald	TNC Binding	look at NEA common values wrt PWG defined attributes in NAP
108	Ira McDonald	TNC Binding	consider normalizing abstract attribute names so they conform with the semantic model

11. Black Hat Embedded Security session web cast

We took a break to watch a live webcast from BlackHat USA 2011, “Corporate Espionage for Dummies – The Hidden Threat of Embedded Web Servers”. It *may* be possible to watch this presentation on demand for the next 60 days by registering here: https://www.blackhat.com/html/bh-us-11/bh-us-11-uplink.html.

12. IAA and Security Model

Refer to:
ftp://pwg@ftp.pwg.org/pub/pwg/ids/wd/wd-ids-iaa10-20110801.pdf
ftp://pwg@ftp.pwg.org/pub/pwg/ids/wd/wd-ids-iaa10-20110801_rev.pdf
Schema and WSDL
ftp://ftp.pwg.org/pub/pwg/ids/wd/schema/PwgSecurity.wsdl
ftp://ftp.pwg.org/pub/pwg/ids/wd/schema/PwgSecurityOpMsg.xsd
ftp://ftp.pwg.org/pub/pwg/ids/wd/schema/Security.xsd
ftp://ftp.pwg.org/pub/pwg/ids/wd/schema/SecurityOperations.xsd

The XML schemas were reviewed and some edits were captured by the author. A few general action items were added:

110	Joe Murdock / Ira McDonald	IAA	change "attributes" to "elements"
111	Joe Murdock	IAA	change "request elements" to "negotiate elements"
112	Joe Murdock	IAA	add some verbiage to the Security Considerations section about how to handle multiple negotiate security element requests; add security elements to system elements, and security ID to XSSL elements
113	Joe Murdock	IAA	add a fifth choice "document security" to request security attributes
114	Joe Murdock	IAA	Add Dublin Core to document security ticket

13. Summary of New Action Items and Open Issues

13.1 New action items

102	Joe Murdock	Remediation	retire the remediation document from the active list
103	Brian Smithson	2600 SD	post URL for IPA research report on MFP security
104	Brian Smithson	2600 SD	post links to join CCVF and CCF
105	Brian Smithson	2600 SD	report on ICCC at October F2F
106	Joe Murdock / Ira McDonald	TNC Binding	consider IANA registration procedure for PWG health attribute types and how to reference them in PWG specs, and registering new ones for binding-specific ones
107	Ira McDonald	TNC Binding	look at NEA common values wrt PWG defined attributes in NAP
108	Ira McDonald	TNC Binding	consider normalizing abstract attribute names so they conform with the semantic model
110	Joe Murdock / Ira McDonald	IAA	change "attributes" to "elements"
111	Joe Murdock	IAA	change "request elements" to "negotiate elements"
112	Joe Murdock	IAA	add some verbiage to the Security Considerations section about how to handle multiple negotiate security element requests; add security elements to system elements, and security ID to XSSL elements
113	Joe Murdock	IAA	add a fifth choice "document security" to request security attributes
114	Joe Murdock	IAA	Add Dublin Core to document security ticket
115	Joe Murdock	IAA	Add document element branch to security ticket

13.2 New issues

None

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?
3. Increase interaction and work tracking with other working groups (IPP-Everywhere)

14. Wrap up and adjournment

The next IDS meeting is a teleconference, on Thursday, August 25, 2011, starting at 1:00PM EDT / 10:00AM PDT.

IDS meeting adjourned.