# IDS Working Group

2011-04-06 Face-to-face Meeting Minutes

## 1. Attendees

| | |
|---|---|
| Nancy Chen | Oki Data |
| Ira McDonald | Samsung/High North |
| Till Kamppeter | Linux Foundation |
| Andrew Mitchell | HP |
| Joe Murdock | Sharp |
| Ron Nevo | Samsung |
| Glen Petrie | Epson |
| Brian Smithson | Ricoh |
| Michael Sweet | Apple |
| Jerry Thrasher | Lexmark |
| Randy Turner | Amalfi |
| Henning Volkmer | ThinPrint/Cortado |
| Bill Wagner | TIC |
| Lida Wang | Kyocera |
| Rick Yardumian | Canon |

## 2. Agenda

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

9:00 – 9:15 Administrative Tasks
9:15 – 9:45 Discussion on NAC (Direction and Attributes)
9:45 – 10:15 TNC Binding Discussion
10:15 – 10:45 Common Criteria
10:45 – 11:00 Break
11:45 – 11:30 Common Log
11:30 – 12:00 IDS Charter Review
12:00 – 13:00 Lunch
13:00 – 13:45 IAA and Security Ticket
13:45 – 14:00 Wrap up and adjournment
14:00 – 15:30 Open Printing

## 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-20110324.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 and comments:

- AI #73 was updated to indicate that the document is renamed "IDS Model"
- AI #83 was updated to indicate that a tentative kick-off teleconference with NIAP will be held on May 5, 2011
- AI #84 was completed

## 7. Document status

Refer to document status on slides #6 and #7 of ftp://ftp.pwg.org/pub/pwg/ids/Presentation/2011-04-06_IDS_F2F.pdf.

## 8. Discussion on NAC (Direction and Attributes)

At RSA 2011, there was some discussion of NAC being used to monitor devices and remove them from the network if they are out of some sort of policy. The question for IDS is whether we should limit the scope of HCD-ATR and related protocol bindings to its original purpose or expand it to include broader use.

It did not seem that this was being used for FISMA's new direction of continuous monitoring. Instead, it is being used by additional monitoring systems that check for behaviors that are considered out of policy and then NAC is used to revoke the device's acceptance on the network.

It was decided to just leave it alone but make sure that devices must respond to revalidation requests.

New NAC attributes under consideration:

- HCD_Syslog_URI (string)
- HCD_Syslog_Enabled (boolean)
- NAC IDS authentication service attribute
- Additional IDS security attributes?

Since it may or may not actually be the syslog protocol, it would be better to call it Security Log.

It isn't within scope for IDS to define what should or must be in the log, but it is within scope to define how to store a log event if such an event is to be logged. Definition of what should or must be logged is determined by certification or compliance requirements like Common Criteria or HIPAA.

Regarding the authentication or other proposed attributes, it was decided to consult with TCG, resulting in a new action item:

| | | | | |
|---|---|---|---|---|
| 86 | 4/6/2011 | Ira McDonald | HCD-ATR | Inquire with S. Hanna about the importance (or lack) of having attributes for authentication service, log URI, and log enabled |

## 9. TNC Binding Discussion

There was some discussion about this resulting in a new action item:

| | | | | |
|---|---|---|---|---|
| 87 | 4/6/2011 | Ira McDonald | TNC Binding | Inquire with S. Hanna about whether flat binding is appropriate for embedded systems like MFPs, referring to IF-TLV document |

## 10. Common Criteria

We decided to hold off on submitting the charter to the SC until we've had at least one conversation with NIAP about the purpose and direction of the project.

The target for a kick-off teleconference with NIAP is May 5, 2011, during the regular PWG-IDS time slot.

In preparation, IDS members should become familiar with the background by reading the whitepaper ftp://ftp.pwg.org/pub/pwg/ids/white/2600sd-20110223.pdf and be ready to discuss at the April 28 teleconference. New action item:

| | | | | |
|---|---|---|---|---|
| 88 | 4/6/2011 | Brian Smithson | 2600.1 SD | Post a reminder to the list to read the whitepaper ftp://ftp.pwg.org/pub/pwg/ids/white/2600sd-20110223.pdf |

Some changes were suggested for the charter:

- Insert a new OBJ-1 to find out from NIAP what we should do
- Change OBJ-3 to say "reinstate 2600.1 when augmented by…"
- Change milestone date to reflect new target for NIAP meeting

To help accelerate the discussion with NIAP, some ideas or proposals should be outlined for what should or could be included in a supporting document. New action item:

| | | | | |
|---|---|---|---|---|
| 89 | 4/6/2011 | Brian Smithson | 2600.1 SD | Outline ideas/proposals for SD |

## 11. Common Log

See document: ftp://ftp.pwg.org/pub/pwg/ids/wd/wd-ids-log10-20110326.pdf

Most of the changes to this document resulted from discussions at the previous face-to-face meeting. Below are some new discussions:

Title is a bit ambiguous (PWG Imaging Device Security Log Format) and could be misinterpreted to mean that it is a "security log" format. Returning to "common log" would be better. Also, is it for imaging devices, or hardcopy devices? Imaging devices (to the PWG) can include projectors. It was decided to call it PWG Common Log Format. Some new action items:

| | | | | |
|---|---|---|---|---|
| 90 | 4/6/2011 | Michael Sweet | IDS-LOG | Change the title so as to PWG Common Log Format |

| | | | | |
|---|---|---|---|---|
| 91 | 4/6/2011 | Joe Murdock | WG admin | Update the definition of "imaging device" to include projectors and such, not just HCDs |

There was some discussion about the Rationale section. There was agreement to update the rationale section to a higher level purpose (standard presentation/protocols to support existing analysis tools and techniques, syslog, ESM, SIEM, etc.), and also the need for new categories of use cases such as audits (like for SOX or HIPAA), security event identification, accounting, and maybe maintenance. New action items:

| | | | | |
|---|---|---|---|---|
| 92 | 4/6/2011 | Michael Sweet | IDS-LOG | Update the rational section to higher-level statements (see 4/6/2011 minutes) |
| 93 | 4/6/2011 | Brian Smithson | IDS-LOG | Send a message to the list to solicit use cases for the log spec |

Also out of scope is protection and retention of the logs.

Messsage level (e.g., error, warning, informational) is a more complex subject and will be addressed in a separate section.

Should there be a unique ID for log messages? Standard UUID (128 bit) would be too long, given the message length limitations. A local ID, such as a wrapping 32-bit number might suffice. It is a subject for additional discussion.

## 12. IDS Charter Review

See document: ftp://ftp.pwg.org/pub/pwg/ids/wd/wd-ids-charter-20110331.pdf

Comments were taken and edited in place.

## 13. IAA and Security Ticket

See document: ftp://ftp.pwg.org/pub/pwg/ids/wd/wd-ids-iaa10-20110402.pdf
(out of time for detailed discussion)

## 14. Summary of New Action Items and Open Issues

### 14.1 New action items

| | | | | |
|---|---|---|---|---|
| 86 | 4/6/2011 | Ira McDonald | HCD-ATR | Inquire with S. Hanna about the importance (or lack) of having attributes for authentication service, log URI, and log enabled |
| 87 | 4/6/2011 | Ira McDonald | TNC Binding | Inquire with S. Hanna about whether flat binding is appropriate for embedded systems like MFPs, referring to IF-TLV document |
| 88 | 4/6/2011 | Brian Smithson | 2600.1 SD | Post a reminder to the list to read the whitepaper ftp://ftp.pwg.org/pub/pwg/ids/white/2600sd-20110223.pdf |
| 89 | 4/6/2011 | Brian Smithson | 2600.1 SD | Outline ideas/proposals for SD |
| 90 | 4/6/2011 | Michael Sweet | IDS-LOG | Change the title so as to PWG Common Log Format |
| 91 | 4/6/2011 | Joe Murdock | WG admin | Update the definition of "imaging device" to include projectors and such, not just HCDs |
| 92 | 4/6/2011 | Michael Sweet | IDS-LOG | Update the rational section to higher-level statements (see 4/6/2011 minutes) |
| 93 | 4/6/2011 | Brian Smithson | IDS-LOG | Send a message to the list to solicit use cases for the log spec |

### 14.2 New issues

None

### 14.3 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)

## 15. Wrap up and adjournment

The next IDS conference call is on Thursday, April 14, 2011, starting at 1PM EDT.

IDS meeting adjourned.