IDS Working Group

2009-10-15 Face-to-face Meeting Minutes

1. Attendees

Randy Turner*	Amalfi Systems
Michael Sweet	Apple
Lee Farrell	Canon
Glen Petrie	Epson
Ira McDonald*	High North
Lida Wang	Kyocera
Jerry Thrasher	Lexmark
Ole Skov	MPI Tech
Nancy Chen	Oki Data
Brian Smithson	Ricoh
Joe Murdock	Sharp
Ron Nevo*	Sharp
Bill Wagner	TIC

* via telephone

2. Agenda

Brian Smithson opened the IDS session and provided the planned agenda topics:

- Administrivia
  - Select Minute-taker
  - IP Policy Statement
  - Introduction and roles of new co-chairs
  - Approve Minutes from October 1 Conference Call
  - Review Action Items from October 1 Conference call
- Review/discuss any revisions to ATR/NAP/NEA documents
- Discussion on SHV issues:
  - Review SCCM binding spreadsheet
  - SHV development alternatives (plug-ins, SHVs, who develops?, …)
  - Reach decision on approach for HCD NAP deployment
- Discuss Randy's issues with multiple NICs ?
  - Info from Jerry Thrasher http://www.ietf.org/mail-archive/web/nea/current/msg01041.html
- Discussion on remediation techniques
  - How does remediation work (in general)
  - Alternatives…
  - How?
  - What is our approach to reach a decision?
- More administrivia
  - IDS futures and “phase II” activity (?)
  - New action items and open issues
  - Conference call / F2F schedule
  - Adjournment

3. Minutes Taker

Lee Farrell

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. New Co-Chairs

Joe Murdock and Brian Smithson are the new co-Chairs. Joe will Chair teleconferences, Brian will Chair face-to-face meetings.

6. Approve Minutes from October 1 Conference Call

There were no objections to the previous Minutes.

7. Review Action Items

AI 001: Randy Turner will try to find other contacts that would be willing to work with the PWG to help deploy NEA health assessment. (Juniper, Symantec, Cisco are suggested candidates.) Is someone willing to sit down with the PWG and "have discussions"?

→ ***ONGOING***

AI 010: Brian Smithson will investigate whether a formal relationship document can be created between TCG and PWG. He will find out their position on liaison agreements.

→ *TCG Board of Directors will meet and discuss this at their next face-to-face meeting (Oct 27-29), and get back to us with a response.*

→ ***OPEN***

AI 022: Joe Murdock will examine the possible mapping of HCD attributes to SCCM and evaluate the resulting "HCD health assessment" benefit. [This should also result in a list of deficiencies and recommended extensions to be suggested to the MS NAP team.]

→ *Proposed mapping spreadsheet was distributed. Questions have been sent to Microsoft.*

→ ***CLOSED***

AI 023: Jane Maliouta will take on the responsibility for creating a "value proposition" document to help justify the reason behind HCD NAP development. Peter Cybuck and Ron Nevo will provide market information as possible.

→ *Ron reported that Jane Maliouta (Microsoft) has done some investigation regarding the business justification of HCD NAP development. She and/or Mike Fenelon will provide their findings in the next few weeks.*

→ ***OPEN***

AI 024: Randy Turner will ask the NEA e-mail list about their assumptions on modeling [sub-]components with regard to MFD subunits. (Why does NEA not address BIOS and/or NICs as components within a PC?)

→ *Randy has received two responses. Steve Hanna (NEA Chair) is working on a list of comments on the NEA binding document.*

→ ***CLOSED***

AI 025: Peter Cybuck will do some market research about whether customers will accept the proposed method of gaining network access via SCCM.

→ *Still working on this. No other status available.*

→ ***OPEN***

8. HCD Health Attributes Document

No update. No discussion

9. NAP Binding Document

No update. No discussion.

10. NEA Binding Document

No progress to report.

No update. No discussion.

11. Discussion on SHV issues

Joe Murdock reviewed the spreadsheet that he had published on IDS-NAP-SCCM attributes mapping. Joe explained that he recently sent a copy of the spreadsheet to the Microsoft NAP team, along with a few questions about the flexibility of network health acceptance by the SCCM system.

He says he will attempt some evaluation of the SCCM when/if he can set it up.

AI 026: Joe Murdock will follow up with Eran Dvir (Microsoft) about the SCCM issues, questions, and capabilities.

→ ***NEW***

AI 027: Joe Murdock will add NAP System Health ID to NAP Binding document and determine how to register a PWG system health ID value.

→ ***NEW***

Under HCD_Firewall_Setting, it was noted that there is no version number.

Joe indicated that Printers will need to "lie" about some of the values to be allowed access to the network by the NAP Server. The group agreed that using the phrase "administratively configurable" is preferable to the word "lie."

Joe recommends that we respond with "Antivirus software not installed." He thinks we can get away with not needing it. However, until we receive a response from Microsoft or test the actual interaction, this might not be acceptable for gaining access to the network.

It was noted that printers *could* respond by saying they have Antivirus software installed. Although this might be technically incorrect, it could be "administratively configured" for the sake of gaining network access.

Joe explained that Security_Updates_WSUSServerName is required by SCCM, but the IDS attributes do not have a good mapping for this entry. Something will need to be substituted or invented.

In summary, the IDS attributes only seem to include the following items that are used by SCCM:

- Firmware version
- Configuration state
- Firewall – yes or no

The relevant question before the group is whether or not these attributes are sufficient to justify continued effort? To date, no consensus within the group has been reached. The critical answer to this is whether customers will find this information adequate for their purposes. Feedback from the marketplace is necessary. [This is what AI #25 is intended to address.]

Ira McDonald suggested that regardless of the findings from the marketplace feedback, the IDS group should at least produce an informational document that gives "best effort" recommendations on how to deal with [today's] SCCM NAP environment. Even if Microsoft is anxious to develop something for HCD support in the future, it is expected that any solution will not be available within the next year—or more.

Jerry Thrasher suggested that perhaps the IDS group could identify a set of "SCCM attributes" as part of a recommended SCCM binding specification.

It was generally agreed that *some* level of document for SCCM should be created. Whether or not it is labeled a "standard" or just an "informational" document might be impacted by feedback from Microsoft.

Randy Turner expressed interest in understanding the benefit of having a SCCM-based solution for HCDs. What is the perceived value for the market—and is it worth the additional overhead and/or the burden on the administrator?

Randy said that Symantec is developing a product for Windows-based network health assessment. It was suggested that if the IDS group could complete the NEA binding for the HCD attributes, it might be possible to get them to include support for HCD devices.

12. Multiple Processes on One NIC

Jerry suggested that the issues relating to a structured device should be deferred to a "Phase II" topic of IDS. He noted that the current NEA specifications do not address virtual machines. Although this might be addressed in the future, he thinks it would be premature for the IDS group to take on this topic for HCDs.

Randy said that the NEA specification does handle PA-subtypes, which could [possibly] be used to address this topic. However, he said it is fine with him to defer until a later time—especially if the deferral is motivated by a schedule desire to achieve something useful in the near-term.

Randy has not yet received any response on his "request for guidance" note that he sent to the NEA group.

The group agreed that for "Phase I activity", the focus will be limited to only the main controller board. It was also agreed to defer the PA-subtype definitions. "We use 0 where we can use the standard attributes, otherwise we use our SMI for PWG-only attributes."

13. Remediation Techniques

The group has agreed to accept the use of a manual remediation technique for the near-term. This will be re-visited in the future as appropriate.

14. IEEE P2600 and "Tailored Assurance Requirements"

A while ago, the question was raised about whether the PWG should consider taking on the task of updating the P2600 Protection Profile specifications. However, after additional consideration of the issues related to IEEE copyrights, this does not seem to be a practical activity for the IDS group at this time.

15. New Action Items and Open Issues

ISSUE: How does an administrator plug in "good values" for health assessment into a SHV? What would that data interface be? [This is not a unique problem for HCDs.]

AI 026: Joe Murdock will follow up with Eran Dvir (Microsoft) about the SCCM issues, questions, and capabilities.

AI 027: Joe Murdock will add NAP System Health ID to NAP Binding document and determine how to register a PWG system health ID value.

16. Next Teleconference

The next IDS teleconference will be held on October 29, 1pm Eastern time. [Refer to PWG Google Calendar: http://www.google.com/calendar/embed?src=istopwg%40gmail.com]

The subsequent teleconference is currently planned for Nov 12.

IDS meeting adjourned.