IDS Working Group

2009-06-23 Face-to-face Meeting Minutes

1. Attendees

Randy Turner*	Amalfi Systems
Lee Farrell	Canon
Ira McDonald*	High North
Jerry Thrasher	Lexmark
Dave Whitehead*	Lexmark
Ole Skov	MPI Tech
Nancy Chen	Oki Data
Brian Smithson*	Ricoh
Joe Murdock	Sharp
Ron Nevo	Sharp
Peter Cybuck*	Sharp
Bill Wagner	TIC
Pete Zehler	Xerox

* via telephone

Ron Nevo opened the IDS session and provided the planned agenda topics:

- Approve Minutes from June 4 & 18 Conference Calls
- Review Action Items from June 4 & 18 Conference calls
- Review Attribute document – any comments?
- Final review of Attribute specification before moving to Last Call
- How to proceed with Microsoft NAP group – Discuss meeting agenda with Microsoft in Redmond
- Discussion on remediation techniques – need an authorized method for remediation
- Review discussion on NEA Binding document
- New Action Items and Open Issues
- Closing Summary

2. Minutes Taker

Lee Farrell

3. 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.

4. Approve Minutes from June 4 & 18 Conference Calls

There were no objections to the previous Minutes.

5. Review Action Items

NOTE: The latest Action Item spreadsheet is available at: ftp://ftp.pwg.org/pub/pwg/ids/ActionItems/

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"?

→ *No new info to report.*
→ ***ONGOING***

AI 002:	Joe Murdock will add NAP protocol information to document and update the conformance section.

→ ***CLOSED***

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.

→ *Brian will talk to Seigo Kotani this week.*
→ ***OPEN***

AI 012:	Mike Fenelon will coordinate the next opportunity for a discussion with the Microsoft NAP team.

→ ***ONGOING***

AI 015:	Jerry Thrasher will create yet another LCRC draft of the Attribute document to include corrections identified at the June 4 teleconference.

→ ***CLOSED***

6. TCG HCWG

During the Action Item review, the question was raised about whether the IDS group should make any positive action regarding the TCG HCWG activity. Bill pointed out that if the IDS group does *not* do anything, they will have no room for complaining when another organization attempts to "fill in the void."

7. HCD Certification State

It was noted that Randy Turner had sent the following e-mail regarding the HCD_Certification_State attribute:

```
Hi All,

I noticed in the meeting minutes from the 6/18 teleconference that there was
a discussion on vendor-specific attributes - these are definitely handled by
a vendor-specific plug-in, however, in the case of the attribute
HCD_Certification_State, we may can draw on how the OpenSSL project handles a
similar value.
```

```
For FIPS 140-2 certification, a specific version of source code was
submitted, including instructions for how to build a "FIPS" version of the
codebase.

In addition, a SHA-1 fingerprint for this specific set of source code is
generated - source code fingerprints are fairly common for security- related
open source projects.

In addition, during the build process, the individual object files are
fingerprinted as well.

There is an additional integrity check performed at runtime.

So there is a source-level, link-time, and runtime verification performed to
make sure that the code that is compiled, built, and run, is the exact same
code that was certified by the FIPS laboratory.

The runtime check is made by the code calling fips_mode_set(), and the
compiler/build-system must be able to order the OpenSSL FIPS code always in
the same order (with respect to relocatable addresses), so that the runtime
fingerprint generated by the FIPS Lab is the same as is generated each time
the code runs.

The value of the FIPS fingerprint could be an example of the
HCD_Certification_State value.

This is a concrete example of how we might think of the
HCD_Certification_State attribute.

Comments?

Randy
```

Although it was agreed that this is a fine example, there is some concern that may not address the issue raised by Mike Fenelon regarding the difficulties of a Validator having to deal with a vendor-specific value. [Unfortunately, Mike was not present to contribute to the discussion.]

Ira McDonald suggested that it would be possible to include a text attribute that describes the particular certification methodology used. Or it would be possible to use a URI that points to a description of how the Certification State value is used. This could lead to an enumeration of the different techniques employed.

Jerry Thrasher noted that the “correct value” of the URI would need to be verifiable for security purposes.

Should this task be added to the IDS list of things to do? It was generally felt that this would be a good idea—and was actually discussed in the past as a “phase II” activity.

Until this [optional] attribute is more clearly defined in terms of its content, should it remain in the Attribute document—or should the attribute be removed until “phase II”?

Ira suggested that even though the attribute is optional, it is not a good idea to include an optional attribute that has undefined semantics.

The previous assumption for the use of this attribute was that a vendor-specific plug-in would be necessary. Mike Fenelon's comments at the June 18 teleconference have led the group to question whether this is a viable approach.

AI 017:	Joe Murdock will send an e-mail to one of the Microsoft NAP team members asking his opinion on the use of an opaque value for HCD Certification State—and specifically the topic of using vendor-specific plug-ins.

→ ***NEW***

In conclusion, the group decided to defer the decision on the HCD Certification State attribute (and whether to keep it in the Health Assessment Attribute specification) until Joe gets a reaction back from the Microsoft NAP team member.

8. Health Assessment Attribute Specification

Jerry led a review of all the modifications contained in the June 18 draft. It addresses all of the Last Call comments that have been received.

All of the changes were approved—with only a few minor exceptions. Jerry will publish another update to show the remaining changes as well as a clean version with all updates. It was agreed that the Formal Vote will be deferred until the determination of the HCD Certification State attribute is resolved.

9. Review NAP Binding Document

Joe Murdock led a review of the June 19 draft update of the NAP Binding document, highlighting the latest modifications. During the review, he also addressed the comments that were submitted by Dave Whitehead in his June 22 e-mail: http://www.pwg.org/archives/ids/2009/000281.html

Several additional changes were noted during the review, and will be included in the next draft.

It was pointed out that the new attributes included in the Attribute specification also need to be included in the NAP Binding update.

AI 018:	Brian Smithson and/or Joe Murdock will include the attributes that were added to the latest Attribute specification in the next version of the NAP Binding document.

→ ***NEW***

10. How to proceed with Microsoft NAP group

Mike Fenelon had previously proposed that the IDS group try to set up a face-to-face meeting with the Microsoft NAP team on the Monday before the August face-to-face meeting (Aug 17.)

As preparation, the group attempted to identify several agenda topics for that meeting:

- The questions that were originally sent to the NAP team, and any follow-up questions to their responses (e.g., What is meant by "deferred enforcement"?)
- Any new questions generated
- Confirm that the Microsoft Print Team is doing an HCD Validator
  - How are vendor-unique attribute values (e.g., firmware version) entered into the system?
  - How are administratively defined values entered into the system?
- Microsoft's thoughts about HCD remediation – standardized or not?
  - What will be the specifics regarding the situation: "your current configuration is not acceptable – fix it"
  - Other non-Microsoft computing platforms (e.g., configuration updates)
  - Auto vs. Manual update: Manual for Phase I, Automatic for Phase II

Bill Wagner noted that for some of the responses we received on the original set of questions, we might have some follow-on questions to their responses.

It was suggested that a deadline for additional questions to Microsoft should be set. New questions should be submitted to the IDS e-mail list.

AI 019:	Dave Whitehead will collect all questions for the Microsoft NAP team that are submitted to the IDS reflector and will pass them along to Microsoft.

→ ***NEW***

The question was raised about whether all the Printer vendor companies are willing to define a standardized [automated] remediation method? And if so, are they willing to commit the effort and necessary resources to implement it? Would it be an acceptable compromise to standardize on returning a URI value that points to a location containing the necessary remediation information?

Jerry suggested that it would probably take a [very] long time to come to agreement on a standardized method of automated remediation. Perhaps a simpler manual method would be satisfactory?

It was pointed out that *any* method of standardized remediation would need support from Microsoft. If they are not willing to implement it, then it will not be very useful.

Dave noted that the response to question #5 from the list of original questions to the NAP team included the term "deferred enforcement." What is exactly meant by this?

```
Q5:
Which of the defined transport(s) are required to be supported in order to
guarantee a device can attach to the network?  MS defines DHCP, 802.1x,
IPSec, and VPN and has extended each to add SOH information.  So, in an
environment where we are attaching wirelessly via 802.1x and receive our IP
address from DHCP, what happens if we only support SOH over DHCP (or 802.1x)?
Will we attach or fail?
```

```
I think the answer is that unless we are enrolled in their health certificate
solution (MS-HCEP), we'll need to re-assess.  However, this is something we
need to clarify with MS.

[MS-NAP] The answer to this question _entirely_ depends on the needs of the
customer and the deployment they choose.
Note that customers can choose to deploy one, a subset or all of the
different transport mechanisms (we call the "enforcement clients", though
enforcement may not be required or desired by the customer).
For example: a customer could choose to do the following:
Deploy
802.1x NAP (L2 access control)
+
DHCP NAP (upper L2/lower L3 access control)
+
IPSec NAP (L3 access control)
+
VPN and TSG NAP (remote access control)
etc. etc

The different layers can do enforcement, deferred enforcement or simply
reporting, they can do auto-remediation (or no remediation), etc, etc.
```

11. NEA Binding document

It was reported that Randy, Dave, and Jerry have collaborated to produce some material on the NEA Binding document, but it is not yet ready for draft publication. Randy will attempt to provide more content and send it to Jerry for formatting.

12. New Action Items and Open Issues

AI 017:	Joe Murdock will send an e-mail to one of the Microsoft NAP team members asking his opinion on the use of an opaque value for HCD Certification State—and specifically the topic of using vendor-specific plug-ins.

AI 018:	Brian Smithson and/or Joe Murdock will include the attributes that were added to the latest Attribute specification in the next version of the NAP Binding document.

AI 019:	Dave Whitehead will collect all questions for the Microsoft NAP team that are submitted to the IDS reflector and will pass them along to Microsoft.

13. Next Teleconference

There will be three teleconferences planned for July: July 9, 23, and 30.

July 9 is the deadline for agenda updates for Microsoft meeting.
July 30 is the deadline for any additional questions for Microsoft to be sent to the IDS reflector.

IDS meeting adjourned.