IDS Working Group

2009-04-30 Face-to-face Meeting Minutes

1. Attendees

Lee Farrell	Canon
Glen Petrie*	Epson
Ira McDonald*	High North
Harry Lewis	InfoPrint
Steve Hanna*	Juniper Systems
Jerry Thrasher	Lexmark
Dave Whitehead	Lexmark
Mike Fenelon	Microsoft
Nancy Chen	Oki Data
Brian Smithson	Ricoh
Peter Cybuck	Sharp
Joe Murdock	Sharp
Ron Nevo	Sharp
Bill Wagner	TIC

* via telephone

Dave Whitehead opened the IDS session and provided the planned agenda topics:

- Approve Minutes from April 16 Conference Call
- Review Action Items from April 16 Conference call
- Review Attribute document – any comments?
- Review NAP Binding Document with Brian Smithson updates
- TCG and IDS groups-Overlap??
- How to proceed with Microsoft NAP group
- 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 April 16 Conference Call

There were no objections to the previous Minutes.

5. 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”?

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

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

→ *In progress.*
→ ***OPEN***

AI 003: Joe Murdock will include sequence diagrams as illustrative examples for the NAP binding document.

→ ***CLOSED***

AI 004: Dave Whitehead will coordinate with Randy Turner to generate a proposal to Microsoft on proceeding with obtaining NAP information on what they envision would be the content of a profile—including remediation. Need to identify the appropriate point of contact within Microsoft.

→ *Mike Fenelon is acting as the liaison between IDS and the MS NAP team.*
→ ***OPEN***

AI 007: Dave Whitehead and Randy Turner will compile a set of questions that are intended for Microsoft—and maintain the answers on an ongoing basis for future reference. This list should include the topic of the four SOH attributes:

- MS-Quarantine-State
- MS-Machine-Inventory
- MS-Packet-Info
- MS-CorrelationId

→ *The list of questions has been sent to Microsoft.*
→ ***ONGOING***

AI 008: Ron and Dave will maintain an Action Item spreadsheet that assigns unique IDs to each Action Item and retains the resolution history.

→ *Ron sent a spreadsheet to Dave and Lee*
→ ***ONGOING***

AI 009: Everyone will review Steve Hanna’s comments [http://www.pwg.org/hypermail/ids/0242.html] and be prepared for discussion at the next face-to-face meeting.

→ *Reviewed at this meeting.*
→ ***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 has started this effort.*

→ ***OPEN***

6. Review Attribute document – any comments?

Dave led a review of the comments supplied by Steve Hanna (Jupiter Systems, IETF NEA Chair).

Comment 1:

```
The descriptions of both HCD_Certification_State and HCD_Configuration_State
say that a change in the underlying value "MUST cause a change in the
attribute" (or "in the attributes value"). Because of information theory,
that's not possible unless the attribute value is at least as long as the
underlying value. Otherwise, there will always be multiple underlying values
that will map to the same attribute value. I suggest that you change the
words I just quoted to "MUST be highly likely to cause a change in the
attribute value". In fact, I'd suggest that you go further and require a
cryptographic hash to be used for this value. Otherwise, implementers may
choose a simpler algorithm like CRC32 or even XOR that doesn't provide
preimage resistance, which you need.
```

The group acknowledged that the comment is theoretically correct. It was agreed that Jerry will qualify the text with the phrase “within the limits of information theory” to “A change to any configuration setting that is required for the device to maintain its certification status MUST cause a change in the attribute within the limits of information theory.”

Comment 2:

```
For HCD_Configuration_State, you are trying to quickly detect any variance
from a standardized configuration. If it might be possible for an
administrator to change which configuration settings are used to calculate
this value, you should probably say "A change to any configuration setting
that is included in the creation of this attribute or change to the set of
configuration settings that are included MUST be highly likely to cause a
change in the attribute value". That should ensure that a malicious
administrator can't just remove a setting from the configuration and then
change that setting without detection.
```

The group agreed to change “must be highly likely” to “must (within the limits of information theory.)”

Ira suggested that the definition of the HCD_Configuration_State attribute be changed to qualify it as something that the administrator modifies. The group agreed to modify the definition to say the “is an administratively configured vendor-specific field…”

Comment 3:

```
For HCD_Downloadable_Application_Enabled, I would expect that a value of 0
would not only disable the ability to download applications but also the
ability to run downloadable applications that have previously been downloaded.
Why? Because I think the goal is to lock down the HCD to only built-in
functions. Am I right? If so, this should be documented.
```

It was felt that Steve's comment was not based on a correct interpretation of the attribute. However, the group agreed that the name of the attribute is somewhat ambiguous. The name should be changed to Application Download Enabled. And a note should be added to clarify that it is not intended to disable previously downloaded or resident (persistent) applications.

A bit more discussion generated more confusion and disagreement, because of the current definitions of downloadable applications vs. resident application vs. persistent applications vs. user downloadable vs. administrator downloadable applications. There seems to be some overlap in the definitions—which creates difficulties in interpretation.

Ira volunteered to re-visit the term definitions to [hopefully] clarify the differences of downloadable applications.

To help the clarification difficulty, one person asked "What is a user-downloadable application?" PDL interpreters were given as examples.

Jerry and Joe suggested that from a health assessment standpoint, there is no practical difference between persistent and non-persistent downloadable applications. Ira disagreed.

The group agreed that "downloadable application" should be re-defined to "user application". Another attribute should be added to determine whether downloadable applications can be persistent (across jobs) vs. temporary.

It was later suggested that the document should identify some recommended default values for these attributes.

Comment 4:

```
I think that there might be several attributes of type
HCD_Downloadable_Application_Name in a single assessment. Each one of these
attributes might be followed by the Patches, String_Version, and/or Version
for that application. Right? If so, these attributes seem to be grouped
together by the fact that they come one after the other.

I'm not sure that all network health assessment protocols support having
multiple attributes with the same ID and that they preserve order. For the
NEA specs, you should be OK if you place the attributes as PA-TNC attributes
within a PA-TNC message. That PA-TNC message will be delivered to the Posture
Validator, which will have its own code to parse the message. That code can
accommodate multiple attributes with the same ID and ensure that the order of
the attributes within the PA-TNC message is properly interpreted.
```

> Similarly, you should be fine for the TNC specs as long as you place all the attributes that pertain to one downloadable application within one IF-M message. You can even place all of the HCD-related attributes within one IF-M message.
>
> With Microsoft NAP, I think you're going to run into message size limitations very quickly. There is a 4KB maximum message size for NAP. All of the attributes that the NAP agent sends to the NAP server must fit within 4KB! So I don't think that you'll want to send over a long list of application names and patches.
>
> I don't know much about Cisco NAC's message format. You should ask someone who's more familiar with that whether there are limitations that might affect you.

The group agreed that when the Binding documents to NEA, NAP and NAC are addressed, it will be necessary to include some type of correlation ID—or equivalent capability.

Comment 5:

> How will the HCD_Forwarding_Enabled attribute be handled in a NEA or TNC environment since PA-TNC now includes a Forwarding Enabled attribute that has a similar definition to HCD_Forwarding_Enabled but not quite the same. HCD_Forwarding_Enabled is only non-zero if the network interface that's requesting access is forwarding. PA-TNC's Forwarding Enabled attribute is on any time that forwarding is happening on any interface.

Yes, they are similar—but not identical.

Later, Steve explained his concern: If you have two interfaces, and one is being health checked while another has forwarding enabled, what does this really mean in terms of [potential] data leakage?

The group agreed that the IDS document will be modified to handle this attribute in the same way as the NEA method. However, Dave said that he would like to limit this topic to *external facing* (i.e., outside of the device) network interfaces. Steve agreed. Bluetooth, WiFi, and “nets and rings” should all be included in the definition of external facing network interfaces.

Comment 6:

> I assume that HCD_Default_Password_Enabled will be handled in a NEA or TNC environment by using the Default Password Enabled attribute defined in PA-TNC. Right? There's no need to have an HCD-specific version of this attribute in that environment since there's already a standard PA-TNC attribute defined for this purpose.

It was determined that the description of the HCD_Default_Password_Enabled attribute should be changed to:

> “The HCD_Default_Password_Enabled attribute is a single bit-field that indicates **that one or more** of the devices’ administrator passwords or other credentials **are set to** the factory defaults. (0 = no default passwords)”

Comment 7:

```
In section 5.2.1, the second sentence should have these additional words at
the end: "if this feature is enabled". If an HCD supports dynamically
downloadable applications but this feature has been disabled through
administrative interfaces, the HCD_Downloadable_Application_Enabled attribute
should not be set!
```

Agreed. The Note in Section 5.2.1 will be removed.

The remaining Comments provided by Steve were all editorial—and were accepted as suggested.

Given the changes identified for the document, the group agreed that the PWG Last Call on this specification will be extended through to the next face-to-face meeting.

AI 011:	Dave Whitehead will send a note to Steve Hanna providing the details of the group's resolutions to his comments.

→ ***NEW***

7. Review NAP Binding Document with Brian Smithson updates

Brian explained that the significant modifications were contributed by Joe Murdock. Joe led a review of the latest updates.

He explained the various modifications to Sections 5 and 6.

Jerry raised a question about the text in Section 5.2: "The conforming HCP NAP client MUST generate an updated Statement of Health and repeat the validation process." He noted that it might be impractical to "re-evaluate" (and disconnect from the network?) when encountering an in-line "user application" in the middle of a job.

It was suggested that a re-evaluation should be done immediately after the job was processed. It does not seem practical to interrupt a job to do the re-assessment. If the user application is persistent, then the re-assessment should be done at the earliest opportunity.

Changes in the other critical attributes identified as triggers for "immediate" re-assessment were accepted as proposed.

It was noted that one of the sequence diagrams in Section 12.4 might need to be corrected.

There were several "open issues" identified at the end of the document that the group addressed:

- BS1: What do we do to define HRESULT values? It is a Microsoft term.
  ➔ It is just an [opaque] integer return value. It is possible to define specific PWG-defined values.

- BS2: What is the subtype code for the Firmware Name TLV?
  ➔ General suggestion is that the value is 2—but this should be verified.
- BS3: Need a good definition of under what conditions conditionally mandatory attributes are required.
  ➔ Refer to the definition in the Attributes specification and adapt as appropriate.
- BS4: What is this (Product Name TLV) attribute, and how is it different from machine_type_model? The description is wrong, and there is no HCD_Product_Name in HCD-ATR.
  ➔ The group agreed to remove the Product Name attribute.

8. TCG and IDS groups – overlap??

The IDS group is interested in making sure that the TCG Hardcopy Working Group activity does not overlap with the IDS activity. Another teleconference with the TCG HCWG is planned for this evening to discuss a proposed update to their Charter. IDS members are welcome to participate and express their thoughts.

9. How to proceed with Microsoft NAP group

Mike Fenelon reviewed the questions that had been sent to the NAP group—and the initial responses received to date.

Mike suggested that it might be possible for someone from the NAP group to participate at a future meeting/teleconference. He also indicated that he plans to have a follow-up discussion with the NAP group to obtain further elaboration on some of the responses. It was noted that a few of the questions require further investigation by the NAP team before they can answer adequately.

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

→ ***NEW***

10. Review discussion on NEA Binding document

There was nothing to review other than table templates – which the group felt was not very productive.

11. Closing Summary

AI 013:	Dave will announce the next teleconference details.

→ ***NEW***

12. New Action Items and Open Issues

AI 011:	Dave Whitehead will send a note to Steve Hanna providing the details of the group's resolutions to his comments.

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

AI 013: Dave Whitehead will announce the next teleconference.

13. Next Teleconference

To be announced.

IDS meeting adjourned.