IDS Working Group

2008-08-13 Face-to-Face Meeting Minutes

1. Attendees

Randy Turner*	Amalfi Systems
Lee Farrell	Canon
Rick Landau	Dell
Tim Jenness	Delta
Jason Tsai	Delta
Glen Petrie	Epson
Harry Lewis	InfoPrint
Jerry Thrasher	Lexmark
Dave Whitehead	Lexmark
Nancy Chen	Oki Data
Ron Bergman	Ricoh
Brian Smithson	Ricoh
Shah Bhatti*	Samsung
Nam Heo	Samsung
Peter Cybuck	Sharp
Joe Murdock	Sharp
Ron Nevo	Sharp
Craig Whittle	Sharp
Bill Wagner	TIC
Sameer Yami	Toshiba
Pete Zehler	Xerox

* via telephone

2. Minutes Taker

Lee Farrell

3. IDS (Imaging Device Security) Introduction

On Wednesday morning, Ron Bergman opened the IDS session and provided the planned agenda:

- Review Health Assessment Attributes document
- Action Item: Submission to IETF NEA WG
- Review HCD NAP Binding Specification
- Discuss Microsoft NAP Protocols document

4. Status

Ron gave a brief overview of the group's goals and current status:

- Develop Assessment Attribute Specification
  - Second version of the spec to be reviewed
- Binding of Assessment Attributes into NAP
  - A proposal was reviewed in the 7/24 telecon
  - The proposal is now a formal specification

    - First review today
- Define the required NAP protocol stacks
    - Review "Microsoft NAP Protocols" document
    - How to include this into a specification

5. Review Health Assessment Attributes document

Ron led a review of the latest updates in the draft. Most of the modifications were accepted as written. During the review, the Editor noted various additional editorial changes to be made to the document. He will issue an update after the meeting.

During the review, HCD_Model_Number was changed to HCD_Model and HCD_Vendor_OID was changed to HCD_Vendor_SMI_Code. These changes were a result of previous teleconference discussions.

Q: When a Downloadable Application becomes downloaded and installed, does it become a Resident Application?

A: It was agreed that the distinction between these two types of applications needs to be clarified further.

ACTION: Jerry Thrasher will clarify the definitions of Downloadable Application and Resident Application.

ISSUE: It was noted that the expected NEA definition of "firmware" will likely be different than the PWG definition and usage of the term "firmware."

It was agreed that PSTN should be added to the acronym section (assuming one is created.)

Q: Is it possible that a Minimum Cipher Suite can be "none"?

A: Yes. A string value of "none" should be added.

ACTION: Jerry Thrasher will determine whether "none" or "NULL" (or something else) will be used to indicate no Minimum Cipher Suite.

Randy noted that the NEA is planning to create a hierarchical structure of attributes within "category". When the IDS group identifies its attributes, it will be useful to consider the categorization. Currently, the NEA does not have a "System" category—but it will probably be useful to define.

Jerry asked the group if anyone had any additional attributes to add to the current list—regardless of its category.

Nancy Chen suggested "Security Level"—but no one had a clear definition for the attribute. There was some dispute about whether this was a practical attribute for determining whether an Imaging Device should be allowed to connect to the network.

It was suggested that a survey could be made of existing tools that are used to determine whether devices can be attached to a network. It might provide some insight to possible attributes that should be included.

5.1 Mandatory Base and Extended Attributes

Ron led a discussion on identifying the categorization of attributes into Mandatory "Base" and "Extended" sets.

It was suggested that the distinction between the terms could be that the Base Set refers to Mandatory attributes, while the Extended Set refers to Conditionally Mandatory attributes.

It was then suggested that we should consider adding an Optional Set of attributes as well.

The following breakdown of attributes was proposed:

Base Set (Mandatory)	**Extended Set (Conditionally Mandatory)**
HCD_Name	HCD_Downloadable_Application_Name
HCD_Model	HCD_Downloadable_Application_Version
HCD_Vendor_Name	HCD_Downloadable_Application_Patches
HCD_Vendor_SMI_Code	HCD_Resident_Application_Name
HCD_Firmware_Name	HCD_Resident_Application_Version
HCD_Firmware_Version	HCD_Resident_Application_Patches
HCD_Firmware_Patches	HCD_Certification_State
HCD_Downloadable_Application_Enabled	HCD_PSTN_Fax_Enabled
HCD_Firewall_Setting	HCD_Secure_Time_Enabled
HCD_Forwarding_Enabled	HCD_Time_Source
HCD_AdminPW_Configured	HCD_Min_Cipher_Key_Length
HCD_Min_Cipher_Suite	

Optional Set

HCD_Configuration_State

It was noted that for each of the Extended Set attributes, the necessary condition should be clarified.

Q: What if a device has multiple interfaces?

A: Then each interface will be assessed/evaluated per interface.

ACTION:	[TBD] will figure out how and where the description of each attribute applies to each interface being assessed.

5.2 Security Considerations

Jerry asked for a volunteer to write the section on Security Considerations. No one volunteered.

Randy suggested that people could pick up a copy of the IETF Guide to Internet Drafts and review it for possible adaptation into our document.

5.3 IETF vs. PWG

The group needs to determine which part(s) of our efforts should be submitted to (and through) the IETF NEA effort—and which part(s) should remain as a PWG standards effort.

For example, Jerry mentioned that a Boolean datatype is not currently defined in the NEA protocol. Should we endeavor to get one defined within the NEA standard?

6. Review HCD NAP Binding Specification

It was noted that each protocol binding specification that the group creates will be a separate document.

Ron led a page-by-page review of the document, highlighting the organization and content of the draft.

He noted several editorial changes to be made to the document, and noted the required changes resulting from answers to the ISSUES that were in the document.

A few attributes were noted to be moved into the Optional Attributes section.

It was agreed that three octets will be used for HCD VENDOR OID SUB-TLV.

ACTION: Ron Bergman will add string representation of versions for firmware application, resident application and downloadable application in the optional table.

It was agreed that we need to include a correlation value to group the associated Name, Version, and Patches attributes. (This also applies to the Resident Applications.)

ACTION: Ron Bergman will update the Firewall Setting to be consistent with the new NEA format.

It was agreed to define a bit map for identifying whether several of the attributes are supported and/or enabled or not—where each attribute is represented by two bits (supported/not, enabled/not).

ISSUE: Should the Conformance section include a discussion of the NAP protocols required or add a new section?
→ Deferred until Joe Murdock presents his material on NAP protocols.

Everyone was encouraged to submit additional document references if they know of any.

It was suggested that a section regarding the observation of Microsoft patents should be included.

7. Security Content Automation Program

Peter Cybuck gave a very quick high-level presentation on the topic of the S-CAP program that is being considered within the US Government for security compliance on government networks. They believe that it will expand into acceptance and deployment into the private commercial sector as well.

He referenced the national Vulnerability Database (nvd.nist.gov) as a database that contains references on product vulnerabilities.

It was suggested that the IDS group might benefit by monitoring this program to see if/how it might relate to IDS activity.

8. Microsoft NAP Protocols Document

Joe Murdock presented his slides on Microsoft NAP protocols, noting that the IDS activity is relevant to the NAP client.

He noted that Microsoft NAP supports multiple access control methods:

- DHCP (RADIUS)
- 802.1x (PEAP - Protected Extensible Enrollment Protocol)
- VPN (PEAP)
- IPSec (HCEP – Health Certificate Enrollment Protocol)

ACTION:	Joe Murdock will investigate whether a PEAP request is made to a switch, and then the switch makes the request to RADIUS.

He showed a few sequence diagrams showing some detail on the flow of multiple protocols involved with the network assessment process:

Bill Wagner said he was surprised that there seemed to be no reference to DNS. Joe indicated that he could not find anything about NEA relevant to DNS.

It was noted that the list of protocols that an MFD is required to support is smaller than originally expected.

9. Action Item: Submission to IETF NEA WG

Jerry noted the following Action Item that was established at the previous face-to-face meeting:

ACTION:	Randy will ask the IETF NEA WG (and other groups?) for their thoughts on [general] attributes such as Time Source, Minimum Cipher Suite, Bridging, Minimum Encryption Key Length, etc. Perhaps they can offer an opinion on the applicability of these items for the industry in general.

He noted that the NEA WG appears very willing to consider any submitted proposal regarding any enhancement to the NEA protocol attributes or packages – or the PWG interests.

Randy said that the NEA group has recently issued a request for submissions on categories and/or attributes that could be added to the current specifications:

> **From:** nea-bounces@ietf.org [mailto:nea-bounces@ietf.org] **On Behalf Of** Paul Sangster
> **Sent:** Friday, August 08, 2008 3:27 PM
> **To:** nea@ietf.org
> **Subject:** [Nea] Request for new Attributes and Component Types (subtypes) for PA
>
> As discussed in Dublin, we have a tight schedule for the PA and PB specs prior to WGLC, so need to make major progress right away on all major open topics for the specifications. The primary open question for PA is to complete the standard attribute name space and list of component types (subtypes) for the 1.0 spec. The editors are currently working on additional attribute proposals, but we would like to hear from the WG.
>
> At the start of open mic in Dublin, we presented 2 slides (32 and 33) listing the currently defined attributes and components and requested feedback from the WG (see slides at www3.ietf.org/proceedings/08jul/slides/nea-0.ppt). The editors would like to request a final call for new attributes and components types for PA by 5PM PDT on Aug 22nd. Proposals should describe the need and use of the new attribute (or component type) and any associated information required. This will enable us to get another revision out by the end of August and stay on schedule.
>
> Thanks,
>
> Paul and Kaushik
> PA Editors

Jerry again commented on his concern that the NEA defines firmware as *separate* from the OS. Within the PWG (and embedded systems products), it is more typical to include the OS as part of the firmware.

From a health assessment standpoint, does this distinction make a difference?

Randy suggested that it might be possible to define an abstract “module” model to allow the coexistence of both approaches. He believes that previous efforts in the IETF have stumbled over attempts to model things based on architectural implementations—and could be the basis for convincing the NEA group to reconsider their current model. Based on the categories currently defined in the NEA protocols, it appears that the NEA WG perspective seems to be very PC-oriented.

Is there any evidence—especially of shipping products—that could help Randy in his argument with the NEA WG? If so, please pass it along.

ISSUE: Should we propose a “Hardcopy Device” category for the base standard of NEA—or should we just plan to use the PWG SMI code to define a vendor-specific extension?

Ron noted that PSTN_FAX seems to be the only HCD-specific attribute currently identified.

Three items that should be raised in the proposal to the IETF NEA WG include:

- Categories
- Attributes
- The concept of a modular architectural model

Jerry also suggested that the “opaque value” concept should also be included in the proposal to the NEA.

Randy said that he will make an attempt at producing a draft proposal—and send it to the IDS e-mail list on the night of August 14.

IDS meeting adjourned.