IDS Working Group

2008-06-25 and -26 Face-to-Face Meeting Minutes

1. Attendees

Lee Farrell	Canon
Glen Petrie	Epson
Ira McDonald*	High North
Harry Lewis	InfoPrint
Randy Turner	Konica Minolta
Jerry Thrasher	Lexmark
Dave Whitehead	Lexmark
Mike Fenelon	Microsoft
Ole Skov	MPI Tech
Nancy Chen	Oki Data
Ron Bergman	Ricoh
Brian Smithson	Ricoh
Shah Bhatti	Samsung
Peter Cybuck	Sharp
Joe Murdock	Sharp
Ron Nevo	Sharp
Craig Whittle	Sharp
Bill Wagner	TIC
Pete Zehler	Xerox

* via telephone

2. Minutes Taker

Lee Farrell

3. Day 1 Discussions

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

- Wednesday, June 25
  - 8:30 Introductions
  - 8:35 Agenda Bashing
  - 8:45 Review Status
  - 8:55 Report on difference between NEA and NAP
  - 10:00 Break
  - 10:15 Review Health Assessment Attributes Doc
  - 11:30 End
- Thursday, June 26
  - 9:00 Introductions
  - 9:05 NAP Binding & Proposed Extensions
  - 10:30 Break
  - 10:45 MS-NAP Protocol Stack Definition
  - 12:15 Wrap-up – Next steps
  - 12:30 End

3.1 Status

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

- Reviewed Network Assessment protocols
  - Cisco NAC (Network Access Control)
  - TCG TNC (Trusted Network Connect)
  - Microsoft NAP (Network Access Protection)
  - IETF NEA (Network Endpoint Assessment)
- NAP appears to be the most mature
  - Well documented (public documents)
  - Supported in MS O/S versions
- Defined an initial set of assessment attributes
- Current effort is to
  - Develop assessment attribute specification
  - Map assessment attributes into NAP
  - Determine the required NAP protocol stacks

Ron explained that the group has been unable to obtain reasonable documentation on the Cisco technology—even though they have a shipping implementation of their technology. The TNC material is evidently restricted to members of TCG. Because the Microsoft documentation is most accessible, the IDS group has started to focus on the NAP technology, and plans to define the first binding with that technology.

Pete Cybuck noted that Cisco currently owns 60% of the networking market—and should not be ignored.

3.2 NEA vs. NAP

Ron Nevo presented a few slides comparing the attributes of NEA vs. NAP. The following attributes are shared by both:

Attributes Type	Attributes name	NAP	NEA	NAP Comments
Product	Name	Vendor-specified SoH Attribute	Product Information	
	Version	Vendor-specified SoH Attribute	Numeric Version / String Version	
Vendor info	Name	--	Product Information	Vendor-specified SoH Attributes
	Id	part of MS System Generated IDs Sub Packet in MS System Generated IDs Packet which is one of SSoH attributes	Product Information	Optional -Vendor-specified SoH Attributes

Attributes Type	Attributes name	NAP	NEA	NAP Comments
OS	Name/type	-	Product Information	A mandatory SSoH attribute This value set is in MS-Machine-Inventory Packet (a SSoH attribute (TV pairs)) in SSoH. The packet also has 2-byte ProcArch at end.
	Ver.	OS Version Major , Version Minor, OS version Build	Numeric Version / String Version	
	Patches	SP ver. Major SP ver. Minor	Product Information	
	Install date and time	-	Product Information	
	Release date			

The NEA is currently examining the TNC-based attribute protocols. The NEA strategy has been to separate the attribute and transport protocols. It was suggested that this strategy should maximize the potential for compatibility with whatever technology emerges as the "winner".

3.3 Review Health Assessment Attributes Document

Jerry Thrasher provided a walk-through review of the document he has written on Health Assessment Attributes. [ftp://ftp.pwg.org/pub/pwg/ids/wd/wd-idsattributes10-20080618.pdf]

It was suggested that section 3.2 should include additional use cases:

- A specific configuration state that is not Common Criteria based
- Security-level checking

Jerry noted that he deliberately avoided some details (e.g., null-termination) in Section 4.1 General Attribute Definitions.

It was suggested that the attributes for Applications, Firmware, and Applets could be multi-valued.

For HCD Applet Name, Jerry raised the following issue about dynamic applications/applets:

> How will we describe multiple applets— in NAC for instance—if applets are downloaded and executed at run-time? They are not available for evaluation/measurement at power up.

Perhaps it would be appropriate to require a re-assessment after any download?

Would it be useful to include some kind of attribute for Application *Type*—to distinguish Firmware, Application, or Applet?

How about using a "structure" containing name, version, patches, and possibly type?

"NAC is all about network policy; NAP is all about assets."

Bill suggested that the group should make the effort to clearly define the differences between the different types. Shah said that we should be consistent with industry usage.

Why is it important to make a distinction between Applications and Applets? Is the only important characteristic whether it is "dynamically loadable" or not? Or is it also important to distinguish whether something is

The labels "Downloadable Application" and "Resident Application" were agreed. Additionally, a Boolean attribute for "Downloadable Applications Enabled" was also suggested.

The group agreed to use multivalued attributes (for Firmware and Applications)—and multiple instances of each.

However, Randy advised that the group should avoid creating methods for specifying attributes that other (larger) standards groups will be defining (e.g., version information, firewall settings.) He stressed that we do not want to conflict with their methods of specification. He suggests that identifying a "placeholder" definition could be the best step at this time, and wait to see how other groups are specifying them.

ACTION: Joe Murdock will write up some discussion points regarding build date and/or version date as they apply to Applications, Firmware, etc.

The HCD Firewall Setting attribute was discussed at some length. There was some concern about the volume of data in the attribute, given potential entries for all port numbers. It was suggested that a default posture (e.g., "off" for all entries) and an explicit set of exceptions could be used.

It was observed that "Configuration State" isn't necessarily relevant to assessing network health, but is more appropriate for use policies.

ACTION: Joe Murdock will write up an example of how Certification State (and/or Configuration State) could be generated and used.

A three-tier prioritization was suggested for the settings that make up the Configuration State attribute:

1. Network Security
2. Device Security
3. Use Policy (or "other interesting stuff")

4. Day 2 Discussions

On Thursday morning, the IDS group continued with the review of the IDS attributes document.

It was agreed that HCD_Bridging_Enabled should be renamed to HCD_ Forwarding_Enabled.

The definition of HCD_PSTN_Fax_Enabled was extended to: "The HCD_PSTN_Fax_Enable attribute is a single bit-field that indicates if the PSTN fax interface *or other modem interface* on the device is enabled. (1 = Fax enabled)"

HCD_AdminPW_Configured was redefined to mean *all* passwords and credentials have been changed from the out-of-box configuration.

There was some discussion about how—or if—a "secure" time source can be evaluated. The definition for HCD_Secure_Time_Enabled was augmented to include that acquiring the time is done *in a secure manner*.

There was much discussion about the HCD_Min_Encryption_Cipher_Suite attribute.

Nancy suggested that the attribute should eliminate the reference to encryption, and be renamed to HCD_Min_Cipher_Suite.

Brian suggested that the attribute should be eliminated altogether. He believes the HCD is unable to determine what the "minimum" acceptable cipher suite is. He also feels that it reflects more of a security policy, rather than a health assessment.

Bill noted that the attribute does not appear to be uniquely related to HCDs. Are similar attributes defined/used elsewhere? Is it really necessary or appropriate for this activity? He is concerned that we will spend much time on characteristics that are not unique to HCD devices—only to have it redefined later by other standards bodies. Further, he feels that if the "other standards bodies" don't believe it is important, then neither should the IDS WG.

It was suggested that the attributes regarding time source and bridging should also be reconsidered for the same reason.

Randy volunteered to raise these attributes to the NEA WG at the IETF. Perhaps they can offer an opinion on the applicability of these items for the industry in general.

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.

After some of deliberation, the group decided to move the following attributes into a "not HCD-specific" bucket—to be considered later as a more generic computing device item:

- HCD_Secure_Time_Enabled
- HCD_Time_Source
- HCD_Min_Cipher_Suite
- HCD_Min_Encryption_Key_Length

The group also agreed to eliminate the HCD_Min_Security_Level attribute altogether.

The group then revisited the HCD_Configuration_State attribute, and noted that there are probably multiple levels of information that could/should be reflected—including vendor and device/model extensions.

It was noted that the group needs to focus on identifying which specific items should be reflected in the HCD_Configuration_State and HCD_Certification_State attributes.

To help clarify—and attempt to unify—everyone's understanding of the different sets of attributes (i.e., "buckets"), the following lists and labels were generated…

Bucket #1

HCD_Configuration_State
= configuration
= individual attribute (device specific opaque block)
attributes that the administrator "cares about" for a multiplicity of reasons—not exclusively about "network health"
n-bit hash
site/vendor/model/device
no remediation

Bucket #2

HCD-specific attested values
Hard disk encrypt
Hard disk erase
Service enable/disable
Interface enable/disable

Bucket #3

= generic computing device attribute (e.g., port filtering, cryptography, etc.)
also a formal 3rd party certification
OS/application/firmware

Bucket #4

HCD_Certification_State (e.g. Common Criteria)
a formal 3rd party certification (i.e., not self-certified)
= certification/network attribute

NOTE: Bucket #4 was initially identified to reflect the original intent behind HCD_Certification_State—but was ultimately eliminated. It was felt that Bucket #2 could be used to achieve this goal.

While the items under "Bucket #2" were being listed, it was opined that the group is going beyond the scope of identifying items related to "Network Health". Jerry pointed out that the Charter includes the goal to determine "fitness to attach to a network"—and explained that these items are definitely within scope.

There was also some discussion about whether information should be included to allow *remediation* of "fitness"—and if so, to what level?

ISSUE: Should Bucket #2 be defined as a value that can be *interpreted*, or merely used to determine changes and/or differences?

One person suggested that any attribute that explicitly has to do with "Network Health" will reside in Bucket #3.

It was agreed that Phase 1 of the IDS activity should be to focus on attributes in Bucket #1 and Bucket #3.

4.1 NAP Binding & Proposed Extensions

Due to time constraints, this topic was not addressed.

4.2 MS-NAP Protocol Stack Definition

Due to time constraints, this topic was not addressed.

IDS Meeting adjourned.