IDS Working Group

2009-02-18 Face-to-Face Meeting Minutes

1. Attendees

Randy Turner	Amalfi Systems
Lee Farrell	Canon
Glen Petrie	Epson
Ira McDonald	High North
Harry Lewis	InfoPrint
Jerry Thrasher	Lexmark
Dave Whitehead	Lexmark
Ole Skov	MPI
Nancy Chen	Oki Data
Brian Smithson	Ricoh
Peter Cybuck	Sharp
Ron Nevo	Sharp
Bill Wagner	TIC

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

- Select Minute Taker
- Approve Minutes from February 5 Conference Call
- Review Action Items
- Review Secure time slides/proposal
- Ciphersuite
- Review Microsoft updates to their SOH document – how will it impact us?
- Review Attribute document – any comments?
- Review NAP Binding Document with Brian Smithson updates
- Decide how to present the bit-level contents of NAP packets?
- Do we need IDS mapping document? NAP, NEA, TNC?
- NEA Binding Document –start process- Who is the editor?
    - HCD-NEA spec plans and schedule
- 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 February 5 Conference Call

There were no objections to the previous Minutes.

5. Review Action Items

ACTION: 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"?

→ *Randy noted that Paul Sangster of Cisco has indicated interest to coordinate with the PWG for interoperability testing.*

→ ***ONGOING***

ACTION: Randy Turner will post the Microsoft name(s) for the PWG to make contact with regard to logo requirements.

→ ***CLOSED***

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

→ ***OPEN***

ACTION: Ron Nevo and Dave Whitehead will update the IDS Wiki pages to reflect current status.

→ ***CLOSED***

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

→ ***OPEN***

ACTION: 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.

→ *Randy said that Erhan Soyer-Osman has given him a name of someone (Chandra Nukala) that is willing to take architectural questions. However, it is important that we first do our homework on reading the available information on NAP and becoming familiar with it. We should avoid questions that have answers available in the current documentation. Randy will post links to relevant informative documents.*

→ ***OPEN***

ACTION: Everyone will review the latest Attributes document draft prior to the next teleconference, and prepare comments for discussion.

→ ***ONGOING***

ACTION: Ron Nevo will examine which time protocols could be used for providing authenticated time (with high integrity), and make appropriate recommendations.

→ ***CLOSED***

ACTION: Everyone will consider the Quarantine State attribute issue that Nancy Chen has raised and will provide recommendations for resolving.

→ ***OPEN***

ACTION: Brian will provide a proposed example illustrating the suggested format for review and acceptance.

→ ***CLOSED***

ISSUE: 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?

6. Review Secure time slides/proposal

Ron presented some information on time as an external or internal source:

- MFPs on a network will either be able to access an external network time source or not. In most cases they may not be able to directly access an external source
- Option 1 – MFP internal clock (on board clock) – no external synchronization
- Option 2 – External Network Source – such as NIST Time
- Option 3 – Internal Network Source
  - In this case the MFP must access a third party network appliance that provides the time for devices on the network and takes responsibility for Accessing the NIST time service or others

He provided some information on Network Time Protocol and NTP time servers, and reviewed the current definition in the IDS Attributes document.

- The Network Time Protocol (NTP) is the most commonly used Internet time protocol, and the one that provides the best performance. Large computers and workstations often include NTP software with their operating systems. The client software runs continuously as a background task that periodically gets updates from one or more servers. The client software ignores responses from servers that appear to be sending the wrong time, and averages the results from those that appear to be correct.
- Many of the available NTP software clients for personal computers don't do any averaging at all. Instead, they make a single timing request to a signal server (just like a Daytime or Time client) and then use this information to set their computer's clock. The proper name for this type of client is SNTP (Simple Network Time Protocol).
- NTP uses Marzullo's algorithm, and includes support for features such as leap seconds. NTPv4 can usually maintain time to within 10 milliseconds (1/100 s) over the public Internet,

and can achieve accuracies of 200 microseconds (1/5000 s) or better in local area networks under ideal conditions.

- In the Internet, NTP synchronizes computer system clocks to UTC; in isolated LANs, NTP is also commonly used to synchronize to UTC, but in principle it could be used to distribute a different time scale, for example local zone time.
- A less complex form of NTP that does not require storing information about previous communications is known as the **Simple Network Time Protocol** or **SNTP**. It is used in some embedded devices and in applications where high accuracy timing is not required. See RFC 1361, RFC 1769, RFC 2030, and RFC 4330.
- Note that NTP provides just the UTC time, and no information about time zones or daylight saving time. This information is outside its scope and must be obtained separately (most systems allow it to be set manually).

- There are two levels, or tiers, of Network Time Protocol (NTP) time servers that are available on the Internet:
  - First-level time servers are primarily intended to act as source time servers for second-level time servers. The first-level time servers may also be capable of providing mission-critical time services. Some first-level time servers may have a restricted access policy.
  - Second-level time servers are intended for general SNTP time service needs. Second-level time servers usually enable public access. It is recommended that you use second-level time servers for normal SNTP time server configuration because they are usually located on a closer network that can produce faster updates.
    The NTP uses port 123 so this port must be opened on a firewall or router to ensure proper communication with the NTP server.

After reviewing some additional material, Ron presented his recommendations:

- The MFP sync does not require synchronization with high precision.
- Time accurate to the second rather than the millisecond or nanosecond is adequate and acceptable for accurate time stamped audit records.
- Synchronization at boot-up time and also at periodic intervals (e.g. daily) should be adequate to minimize drift of an internal clock.
- The IDS group should recommend to synchronize the MFP with internal source. The accuracy of the internal source is the responsibility of the IT manager.
- It does not make sense that MFP will have a better time accuracy than the local server time!!!!
- In the attribute document we should have 2 options for clock: On board clock (Internal clock) or External Clock synchronization
- It is considered secure if the MFP has a mechanism to protect the time settings

Jerry Thrasher said that rather than reporting what a device is *capable* of supporting, the attribute should indicate what time source the device is *actually* using.

Some people in the group have gone back to using the term “secure time” in addition to “authenticated time.” It was suggested that “secure time” could be used as a more generic, umbrella term.

Does a "trusted" time source qualify as a "secure time"? Probably not.

The group agreed that regardless of the source of the time, it should be protected from alteration.

The Boolean for HCD_Secure_Time_Enabled (or HCD_Authenticated_Time_Enabled) was determined to be unnecessary.

Randy suggested that either a Host Name *or* a URL for the network time source should be acceptable.

Is it possible to define a URL convention to indicate an onboard realtime clock? It was suggested that a filespec (i.e., file:xxx) could be used. Could LocalHost be used?

It was agreed that using the string "onboard" could be used to indicate an onboard realtime clock source.

7. Ciphersuite

The group is having a difficult time on deciding on what to do with regard to Cipher suite and key length. Dave suggests that we recognize it is important, but it is outside of our scope to define. Perhaps an opaque value would be sufficient?

The group agreed to the following proposal:

> Delete the two attributes HCD_Min_Cipher_Key_Length and HCD_Min_Cipher_Suite and include the information [somehow, opaquely] in HCD_Configuration_State—as additional [optional] parameters.

In consideration of the "big hashes" such as SHA-512, the group agreed to increase the length of HCD_Configuration_State and HCD_Certification_State.

Brian Smithson suggested that the attributes should be variable length—and this was agreed. It was noted that the Binding specification documents will determine max lengths.

8. Microsoft SOH

The following issue was noted:

> ISSUE: 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?

Dave indicated that it might be difficult to resolve the above issue without some support from Microsoft. To ensure that the item is maintained, Dave volunteered to take on this issue as an Action Item.

ACTION: Dave will attempt to resolve the following issue: 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?

→ *The group consensus is that it does not belong in the Attributes document, but should be addressed in the Binding document.*

→ ***NEW***

Dave mentioned that he has noticed an update to the "SOH document". January 14, 2009 seems to be the latest draft.

ACTION: Dave Whitehead and Brian Smithson will review the latest SOH document and determine if the updates have any impact on the IDS activity.

→ ***NEW***

9. Review Attribute document – any comments?

The group would like to advance the Attributes document from "INTERIM" as soon as possible so that it can be sent to the IETF NEA WG for their review and comment.

Jerry led a review of the latest modifications—including the changes agreed to at today's meeting.

All modifications were approved.

ACTION: Jerry Thrasher will post the updated document marked as "PROTOTYPE" that reflects all changes agreed to at the Feb 18 meeting.

→ ***NEW***

→ ***CLOSED*** *[during the meeting]*

ACTION: Randy will send a link to the updated Attributes document to the NEA WG, and solicit their comments.

→ ***NEW***

It was suggested that the NEA and the NAP Binding documents should be examined and exercised more thoroughly before the Attributes specification is progressed to "STABLE."

ACTION: Ron Nevo or Dave Whitehead will initiate a WG Last Call on the Attributes specification whenever it is appropriate.

→ ***NEW***

10. IETF NEA Working Group Meeting

It was announced that the IETF NEA Working Group is planning to have a face-to-face session during the week of March 23. Neither Dave Whitehead nor Jerry Thrasher will be able to attend the meeting to represent the IDS group or the PWG organization.

Because the PWG has a strong interest in the progress of the NEA activity, it was noted that someone from the IDS group should attend if at all possible.

11. Review NAP Binding Document with Brian Smithson updates

Brian Smithson led a review of the significant update to the NAP Binding specification.

In addition to the new content, he noted the formatting used for defining the bit-level contents of fields, and the overall document organization.

During the review, it was suggested that a few "noteworthy rules" that are embedded in individual field descriptions should somehow be highlighted and tagged as noteworthy. If there are enough of these, it might be appropriate to collect these items and include them in a higher-level section.

It was agreed that the Product Name TLV will be eliminated, but the Machine Type Model Number will be used instead.

While discussing Section 4.3.2.1 HCD Downloadable AP Name, it was noted that Microsoft has a different use for the term "Correlation ID." It was suggested that the name be changed.

Brian said that he will need to update the Binding document to be consistent with today's changes to the Attributes document.

12. Do we need IDS mapping document? NAP, NEA, TNC?

NAP: yes
NEA: yes
TNC: because NEA is really based on the TNC work, a separate document is probably not necessary.

13. NEA Binding Document

To date, no one has explicitly volunteered to be the Editor for the NEA Binding document.

At a previous IDS session:

- Jerry said he is willing to help with the editorial tasks (e.g., formatting and document creation), but he indicated a lack of familiarity with the protocol detail.
- Randy said he would consider his availability to work on content creation.
- Dave said he will "help a bit."

Randy said he will take a "first cut" at content and coordinate with Jerry and Dave.

ACTION:	Randy Turner will make a "first cut" attempt at providing content for the NEA Binding specification. He will coordinate with Jerry and Dave to get it into a properly formatted document.

→ ***NEW***

14. Quarantine State

The group agreed that the four attributes that Nancy has identified should be added to the specification:

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

It was noted that not all devices will be running Windows—and the MS-Machine-Inventory is a bit presumptuous. Perhaps an "Other" characteristic would be appropriate? It is assumed that somewhere there will be a means to indicate whether the device in question is actually running Windows or not. It was pointed out that Microsoft's desire to support TNC would suggest that they plan to support non-Windows devices.

Apparently, mapping into MS-Machine-Inventory for a non-Windows system is not specified in the latest TNC SOH mapping document.

AS before, the group concluded that we need to ask for help from Microsoft on this issue. The group also decided that a set of questions intended for Microsoft should be collected into a single document, and referred to on an ongoing basis. It should be updated to record the most current answer(s) determined at any given point in time.

ACTION: Someone (Dave? Brian?) will compile a set of questions that are intended for Microsoft—and maintain the answers on an ongoing basis for future reference.

→ ***NEW***

15. New Action Items and Open Issues

ACTION: Dave will attempt to resolve the following issue: 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?

→ *The group consensus is that it does not belong in the Attributes document, but should be addressed in the Binding document.*

→ ***NEW***

ACTION: Dave Whitehead and Brian Smithson will review the latest SOH document and determine if the updates have any impact on the IDS activity.

→ ***NEW***

ACTION: Jerry Thrasher will post the updated document marked as "PROTOTYPE" that reflects all changes agreed to at the Feb 18 meeting.

→ ***NEW***

→ ***CLOSED*** *[during the meeting]*

ACTION: Randy will send a link to the updated Attributes document to the NEA WG, and solicit their comments.

→ ***NEW***

ACTION: Ron Nevo or Dave Whitehead will initiate a WG Last Call on the Attributes specification whenever it is appropriate.

→ ***NEW***

ACTION: Randy Turner will make a "first cut" attempt at providing content for the NEA Binding specification. He will coordinate with Jerry and Dave to get it into a properly formatted document.

→ ***NEW***

ACTION: Someone (Dave? Brian?) will compile a set of questions that are intended for Microsoft—and maintain the answers on an ongoing basis for future reference.

→ ***NEW***

16. Next Teleconference

To be announced.

IDS meeting adjourned.