IDS Working Group

2009-02-05 Conference Call Minutes

1. **Attendees**

Randy Turner	Amalfi Systems
Lee Farrell	Canon
Glen Petrie	Epson
Ira McDonald	High North
Dave Whitehead	Lexmark
Nancy Chen	Oki Data
Lida Wong	Kyocera Mita
Brian Smithson	Ricoh
Bill Wagner	TIC
Peter Cybuck	Sharp
Ron Nevo	Sharp

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

- Identify minute taker
- Meeting conducted under rules of PWG IP Policy
- Review/approve minutes from PWG Jan. 22 teleconference
- Review Action Items
- Document Review
  - Attributes
  - Binding
- Review Issues
  - Nancy's questions on 4 SOH attributes
    - MS-Quarantine-State
    - MS-Machine-Inventory
    - MS-Packet-Info
    - MS-CorrelationId
  - Class plug-in for assessment without remediation is not as useful. Are there any common remediation steps the PWG could define?
- F2F Meeting Topics/Agenda
- Next Steps / Next Meetings

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 January 22 Conference Call

There were no other 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"?

→ *Still needs to pursue this further. No new information to report.*
→ ***ONGOING***

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

→ *Randy has requested a contact name, but no response yet.*
→ ***OPEN***

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

→ ***OPEN***

ACTION: Brian Smithson will update and re-write the Network Access Protection Protocol Binding document, taking into account the comments from the October meeting and the comments that Dave Whitehead has posted.

→ ***CLOSED***

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

→ *Some updates have been done, but not yet complete.*
→ ***OPEN***

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: Jerry Thrasher will change the term "secure time" to "authenticated time" throughout the Attributes document.

→ ***CLOSED***

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

→ *Ron will make this material available for the face-to-face meeting.*
→ ***OPEN***

ACTION: Nancy Chen will identify a specific issue that she has found with regard to the Quarantine State attribute in the TNC SOH document, and will post it (and any recommendations) to the e-mail list.

→ ***CLOSED***

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

→ ***OPEN***

6. Attributes Document

Jerry has indicated that he would very much like to accept the latest modifications and issue a new revision. There were no objections.

It was noted that any additions of the Quarantine State attribute(s) will occur after Jerry's update.

7. Binding Document

Brian raised a concern about the abundance of linkages and references to information outside the Binding document. He agreed that the binding document(s) should point elsewhere for attribute descriptions, but maintain a detailed description of "which bits go where" in the individual Binding documents. Because the Binding documents are closer to an implementers guide, it was generally agreed that these details should be included. However, it was also agreed that the document should include references to which specific documents (and dates) the details are drawn from.

Suggested items to include:

- Name of the attribute
- A reference to the full attribute description (document and section number)
- A condensed description of "which bits go where".

Randy suggested that the Table of Contents from all Binding documents should be [essentially] identical. The specific text contents of each section will be different, but the document structure and the section subjects should be very similar.

Randy will send Brian a suggested/sample TOC structure.

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

→ ***NEW***

It was noted that a conformance section should be included in the document.

Randy mentioned that the way Microsoft handles non-compliant devices for network acceptance is not very friendly. He warned that "… the DHCP stuff is not really optional on a Microsoft network." He cautioned that we need to be more careful in our claims of what is required and optional. For those items we describe as optional, we should be clear as to what the impact is if the item is not implemented.

Dave [later] summarized the issue for the group to consider:

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?

It might be worthwhile to add some warning that Microsoft extensions to DHCP are necessary. Perhaps this should not be in the Conformance section—but possibly a section on "Other Considerations."

8. Nancy's Questions on Four SOH Attributes

It seems 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? Randy says he assumes that somewhere there will be a switch to indicate whether the device in question is actually running Windows or not. He thinks that Microsoft's desire to support TNC would suggest that they plan to support non-Windows devices.

Ira pointed out that the latest TNC SOH mapping document is worth examining. Apparently, mapping into MS-Machine-Inventory for a non-Windows system is not specified.

9. Class plug-in

It has been noted that a class plug-in for assessment without remediation is not as useful. Are there any common remediation steps the PWG could define?

There were no suggestions.

10. Cipher Suite and Key Length Attributes

There is a question about whether these attributes are actually useful. [Refer to e-mail discussions for details.] Brian asked if HCDs are the only devices doing this, is it really appropriate for us to support at all? He proposes that we should eliminate them altogether. If an individual vendor wants to support it, they can simply roll it up into the configuration state attribute.

How do other companies specify this information? Would our approach create a mapping problem for other implementation methods?

Because we seem to be the only ones considering this, do we run the risk of having the industry create some kind of solution that will be incompatible with our [proposed] approach?

Randy suggested that a survey should be done to identify how others determine minimum security policy descriptions and evaluation.

Ira said that HIPAA requires 128-bit AES as a minimum. AES 256 is being used by the DoD, although they are currently accepting 128.

11. Face-to-face Meeting Topics/Agenda

Other than Ron's topic on time protocols, there were no new agenda items suggested.

12. Next Teleconference

March 5, 1:00pm EST.

13. Summary of New Action Items and Issues

In addition to the existing OPEN Actions Items, the following new item was generated:

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

And the following Issue was raised:

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?

IDS meeting adjourned.