IDS Working Group

2008-12-15 Conference Call Minutes

1. Attendees

Randy Turner	Amalfi Systems
Lee Farrell	Canon
Dave Whitehead	Lexmark
Ira McDonald	High North
Glen Petrie	Epson
Nancy Chen	Oki Data
Peter Cybuck	Sharp
Joe Murdock	Sharp
Ron Nevo	Sharp
Shah Bhatti	Samsung
Bill Wagner	TIC

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

- Meeting conducted under rules of PWG IP Policy
- Identify minute taker
- Review/approve minutes from PWG Face-to-Face
  ftp://ftp.pwg.org/pub/pwg/ids/minutes/IDS-ftf-minutes-20081203.pdf
- Review Microsoft responses to 7 questions
  [see email forwarded by Dave Whitehead on Friday 5 December on IDS list]
- Review Secure Time definition
- 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 December 3 FACE-TO-FACE and 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"?

→ ***ONGOING***

→ *No new information.*

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

→ ***OPEN***

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

→ ***OPEN***

ACTION: Dave will pursue answers on the 7 questions to Mike Fenelon and Erhan Soyer-Osman of Microsoft.

→ *Dave said that Microsoft has provided a reply.* ***CLOSED***

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.

→ ***OPEN***

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

→ ***OPEN***

ACTION: Jerry Thrasher will attempt to re-write the definitions of “resident” and “downloadable”.

→ ***OPEN***

ACTION: Dave Whitehead will write up a definition of “secure time” for inclusion in the Attributes document.

→ ***CLOSED***

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

→ ***OPEN***

6. Review Secure Time definition

The group reviewed Dave’s submission:

> Secure Time: This attribute signifies that the time source used to set the device's clock(s) is considered a trusted source. Many security mechanisms rely on accurate time to enforce security. Examples include validity periods on X.509 certificates and Kerberos Tickets. As such, it is important to know that the device's internal clock(s) acquire time in a secure manner. If the time source is not secure, it could lead to denial of service (set time outside the validity period) and/or allow unauthorized access (set time to within validity period.) There are several ways to acquire the time including Network Time Protocol (NTP) and explicitly set by the user via some user interface. NTP has the ability to utilize encryption and integrity checks using pre-shared keys.

> The user interface to the clock can be protected using passwords. It is important to note that RTCs are often used in devices and may utilize a bus structure, such as I2C. In such cases, the bus used MUST NOT be accessible externally from the device.

A few modifications were suggested and Dave will include them in the document update. It was noted that some of the "definition" was really elaboration or rationale that could be separated as "usage considerations".

Randy mentioned that he raised the topic of secure time with the NEA WG. He was encouraged to see the TICTOC(?) WG for requirements. Evidently, they are addressing reliability of time, and how it can be maintained and synchronized.

Bill expressed some surprise that "secure" time was not accepted as a core part of the NEA protocol. Randy suggested that it did not qualify as "low hanging fruit"—and would [probably] be difficult to address remediation. Bill suggested that the IDS group should avoid spending too much effort on the attribute—because he believes that eventually it will/should become something that another IETF working group defines.

Is there a NIST standard that could be leveraged? Ira believes that SP800-series standards should be relevant.

> ACTION: Peter Cybuck will examine the NIST standards for insight or material on secure time.

Dave said that he thinks the NTP standard contains some information on time synchronization mechanisms.

> ACTION: Dave Whitehead will examine the NTP standard (RFC 4330) for insight or material on secure time. (There is a reference to MIL-03 which should be followed.)

7. Review Microsoft responses to 7 questions

Dave reviewed the responses to the questions:

1. The NAP spec states UTF-8 string encoding and TLV elements. There is also a statement about strings being NULL terminated. We believe the NULL terminator was inadvertently added since it is not required for TLV elements. That is, do we really need NULL termination?

> [NAP Team] Yes. The current implementation requires "Null termination"

2. Is it Microsoft's current and future desire/intent/direction for strings to be UTF-8 encoded?

> [NAP Team] Currently we use UTF-8 and as of now plan to use UTF-8 in the future releases (To the best of our knowledge) but we will notify/update the necessary document when this changes along with backward compatibility directions if this changes.

3. Is Microsoft planning any type of interoperability between NAP and Network Endpoint Assessment (NEA) from the TNC? Maybe a gateway?

> [NAP Team] Microsoft has donated NAP's Statement of Health specification to the TCG's TNC group, companies wishing to support NAP in their products can download and use the specification free of charge. This SOH has also been made a standard by the TNC (IF-TNCCS-SOH). See the white paper at http://download.microsoft.com/download/c/1/2/c12b5d9b-b5c5-4ead-a335-d9a13692abbb/TNC_NAP_white_paper.pdf.
>
> We will be working with TNC/NEA in future releases as well.

It was noted that this response seemed to avoid the heart of the question, but the short answer *seems* to be "No."

4. What happens when a device passes assessment under one mechanism but then is challenged again? For example, first over 802.1x to attach and then DHCP to receive an address. Do we need to start the assessment again from scratch or is there a shortcut?

> [NAP Team] There is no shortcut. However customers will usually choose one enforcement. Multiple enforcement is supported but there are no smarts targeted at multiple enforcement. You need to resend the SoH to the enforcement mechanism but you can use the cached SoH intelligently.

5. It looks like most, if not all, of the evaluation attributes will be extensions to NAP. The only NAP attribute that may be applicable is the Product Name. Is it appropriate for the PWG to use Product Name or should we define all our attributes as extensions?

> [NAP Team] Product Name is an "optional" TLV. It is defined to be used, but on the other hand they could define their own schema in the vendor specific TLV.

6. How can we get the extended PWG attributes to be recognized by the Microsoft validator/assessor? Is this a plug-in supplied by a third party? If this is an industry supported solution, would Microsoft be willing to supply any required plug-in?

> [NAP Team] The Microsoft WSHA/V currently does not support this. The third party can develop their own SHA/V and plug into the NAP infrastructure. Please refer to the samples provided in the NAP SDK.

Randy wondered if Microsoft recognizes a class plug-in for NAP. If not, then all vendor implementations will need to write much of the same code for collecting attributes.

ACTION: Randy Turner will follow up with Microsoft to ask if they will recognize a class plug-in for NAP.

7. Just to make sure we understand it, the PWG members would really like someone familiar with NAP to profile how it would operate with print devices. Would this be possible?

> [NAP Team] Yes. The NAP team would like to profile how NAP will operate with Print devices. Please let us know how we can proceed.

We would like an example. Block diagrams would be useful. Randy noted that he is mostly concerned with what happens when assessment fails. How is remediation handled? A detailed example would be very useful.

A detailed specification write-up would be appreciated for review. A follow-up question and answer cycle should be planned as well.

8. Summary of New Action Items and Open Issues

In addition to the existing OPEN Actions Items, the following new items were generated:

ACTION: Peter Cybuck will examine the NIST standards for insight or material on secure time.

ACTION: Dave Whitehead will examine the NTP standard (RFC 4330) for insight or material on secure time. (There is a reference to MIL-03 which should be followed.)

ACTION: Randy Turner will follow up with Microsoft to ask if they will recognize a class plug-in for NAP.

9. Next Teleconference

Subsequent teleconferences are scheduled for January 8, 22, and February 5.

IDS meeting adjourned.