

IDS Working Group

2008-05-08 Conference Call Minutes

1. Attendees

Attendees: Lee Farrell (Canon), Kevin Sigl (Hewlett Packard), Ira McDonald (High North), Jerry Thrasher (Lexmark), Dave Whitehead (Lexmark), Nancy Chen (Okidata), Ron Bergman (Ricoh), Peter Cybuck (Sharp), Joe Murdock (Sharp), Pete Zehler (Xerox)

2. Agenda

1. Identify minutes taker.
2. Approve minutes from April 24 meeting.
3. Microsoft NAP team discussion (until 1:30)
4. NEA team discussion
5. Next teleconference

3. Identify Minutes Taker

Lee Farrell

4. Accept Previous Minutes

There were no objections to the previous teleconference Minutes.

5. Review Action Items

ACTION: Jerry Thrasher will send a note to Cisco to find out if there is an information path we can develop to learn about attributes (e.g., if there is a better source of information.)

→ *A note has been sent, but no reply received yet.* **OPEN**

ACTION: Ron Nevo will contact the TNC Chair to try to get the TNC attributes information.

→ *A note has been sent, but no reply received yet.* **OPEN**

ACTION: Everyone will review the [recently identified] Microsoft and NEA documentation and determine the IDS attribute mappings to each.

→ **CLOSED**

ACTION: Jerry Thrasher will start a Definition of Terms list (i.e., some documentation)

→ *Started a list of terms, but definitions not yet complete.* **OPEN**

ACTION: Joe Murdock will distribute an attribute list spreadsheet to be used as a template for future mapping efforts.

→ **CLOSED**

IDS Working Group

2008-05-08 Conference Call Minutes

6. The Teams

Microsoft NAP Team

Joe Murdock
Peter Cybuck
Nancy Chen

NEA Team

Shah Batti
Brian Smithson
Ron Bergman

7. Microsoft NAP Team Discussion

The Microsoft team has developed a spreadsheet of the NAP attributes and distributed it for review to the group members. [[ftp://ftp.pwg.org/pub/pwg/ids/white/IDS-NAP-Attribute Mapping-05082008 NC.xls](ftp://ftp.pwg.org/pub/pwg/ids/white/IDS-NAP-Attribute%20Mapping-05082008%20NC.xls)] Joe led the group in a review of the spreadsheet content.

There was some discussion regarding whether Quarantine State Packet is applicable to the Hardcopy Devices, given that it is unlikely that the HCDs will be supporting Antivirus software. However, Nancy noted that it is a mandatory attribute that is used to reflect the assessment state. The issue of determining what should be done when the value is “restricted” was deferred.

It appears that NAP does not have a port filter attribute. However, it was suggested that a hash value “token” could be used as part of the “Configuration Token” attributes. It was noted that hash values are susceptible to value conflicts.

8. NEA Team Discussion

Ron led a brief review of the spreadsheet that he developed for NEA attributes. [<ftp://ftp.pwg.org/pub/pwg/ids/white/IDS-NEA-Attribute-Mapping-05062008.xls>]

He mentioned that sub-types are used in the NEA protocol.

9. Questions on Attributes

Jerry asked: What do we mean by “minimal security level”? Joe believes that it refers to the minimum security level that is accepted for incoming communications. Jerry wanted to know how to data type this information (a bit field?), but there was no consensus reached. It probably requires an ordered/prioritized list of alternatives.

Jerry also noted that we need to clarify the term “Application” – and how we plan to use it. Are they (generally) dynamically downloadable? How is this distinguished from upgrades to the OS? It was suggested that the terms “firmware” and “applets” should be used, as they seem more appropriate to the HCD environment.

10. Next Teleconference

May 29, 1:00pm EDT.