IDS Working Group

2008-04-16 and -17 Face-to-face Meeting Minutes

1. Attendees

Lee Farrell	Canon
Rick Landau	Dell
Glen Petrie	Epson
Ira McDonald*	High North
Harry Lewis	InfoPrint
Randy Turner	Konica Minolta
Jerry Thrasher	Lexmark
Dave Whitehead	Lexmark
Erhan Soyer-Osman	Microsoft
Nancy Chen	Oki Data
Ron Bergman	Ricoh
Brian Smithson	Ricoh
Shah Batti	Samsung
Peter Cybuck	Sharp
Craig Whittle	Sharp
Joe Murdock	Sharp
Bill Wagner*	TIC
Dennis DeYoung	Xerox

2. Minutes Taker

Lee Farrell

3. Imaging Device Security (IDS) Status

On Wednesday morning, Ron Bergman opened the IDS meeting and provided the current status:

- Review of Network Assessment Protocols
  - Cisco NAC
  - TCG TNC
  - Microsoft NAP
  - IETF NEA
- Current effort is to generate a set of assessment attributes applicable to Imaging Devices

Ron noted that the published documents do not have much in the way of identified attributes at this point.

Jerry Thrasher noted that he recently received a document reference from Microsoft (available at: http://msdn2.microsoft.com/en-us/library/cc246924.aspx). The document title is: "Statement of Health for Network Access Protection (NAP) Protocol Specification"

4. Agenda Discussion – and Brainstorming

Peter Cybuck had developed a white paper that offered a proposed outline for the attribute discussion. It was reviewed by the group to get a sense of how they should attack the general problem of identifying attributes and/or characteristics of a device that can be used to determine whether it should be allowed on a network.

Peter explained that a scan for open ports on a printer or MFD device is sometime used (or perhaps should be used) to determine whether a device is allowed on a network or not. The discovered port configuration can be used for assessing acceptability. He wondered whether this is out of scope for the IDS effort. At this point, it doesn't seem to be.

Another item for screening that can be used is a driver check. Are the desired/required drivers available—and does the device support the required protocols?

Jerry mentioned the IEEE P802.1AR/D1.0 effort that is exploring the use of a [non-spoofable] Secure Device Identifier (SDI). He suggested that the SDI might also be a characteristic that could be used for assessing a device.

"Firmware things" could also be used as screening attributes. It was noted that firmware version is currently not reported in a standard manner across printers.

OS version was also mentioned as a possible screening attribute.

Bottom line goal: "I do not want a rogue device attached or bridged to this network. How can I avoid it?"

In answer to the question, "How far do we want to go on this?" it was suggested that we should initially target a simple or basic set of attributes/characteristics. Everyone agreed that the group could always add on later with a more complicated set of items. A suggestion was made that multiple levels of assessment would probably be useful for varying levels of security needs.

Peter's white paper suggested that the meeting should focus on the Cisco Network Access Control (NAC) architecture to create an initial example.

There is some debate as to whether the Microsoft and Cisco approaches are complementary.

It was noted that the NEA effort (in IETF) is co-chaired by individuals from both Cisco and Juniper.

Randy reported that the within the NEA (IETF) group, they are talking about the possibility of using NetConf (also an IETF working group) for network remediation.

Should we create something that can be used as an Application Type?

Randy believes that the attribute set the group identifies for HCDs will have overlap with other devices. In many senses, these devices look like computers to the network.

5. RSA Printer Security Presentation

Brian recalled that after an HP presentation at the RSA conference, one person asked if printers were providing NAC and NAP support. The HP speaker was generally vague in his response, but Brian mentioned the PWG IDS activity and the P2600 efforts that are currently active.

6. Cisco Attributes

Ron referenced a document he compiled that listed various Attribute Names being used by Cisco. It contained the following items:

Application-Posture-Token	Software-Name
System-Posture-Token	Software-ID
PA-Name	Version
PA-Version	Scan-Engine-Version
OS-Type	DAT-Version
OS-Version	DAT-Date
User-Notification	Protection-Enabled
OS-Kernel	Action
Kernel-Version	CSA-Version
Action	CSA-Operational-State
Machine-Posture-State	Last-Successful-Poll
Service-Packs	CSA-MC-Name
Hot-Fixes	CSA-Status
Host-FQDN	Last-Successful-Poll-Days
Package	

He explained that the list might not be completely accurate, because he has seen another document from Cisco that doesn’t completely agree with this list. Ron said he will need to investigate this inconsistency further.

The items above that are highlighted in green reflect the group’s identification of attributes that would likely be used for IDS. The discussion about which items should be required vs. optional was deferred.

Cisco’s attributes each have data type and value/format information identified that the IDS group would need to be consistent with—at least with Cisco’s protocol. The question remains about whether other protocols might have inconsistent type/value characteristics—and how IDS addresses that issue. Randy mentioned that the NEA [proposed] protocols should be examined for comparison purposes.

It was noted that each HCD vendor would need to [somehow] map whatever attributes they use into one or more of the above attributes, using the specified data type/format.

Bill pointed out that sometimes it is more important to identify a specific product model—rather than the OS version number.

To what level of granularity are changes to the system required to be tracked and reported?

ISSUE: The issue of describing which patches have been supplied to a given OS seems to be a difficult problem.

It was suggested that port configuration should also be considered as an attribute. The problem of encoding that information as a practical (and relatively small) value was deferred. Jerry suggested a hashed value of a set of entries in a table of port numbers could be used.

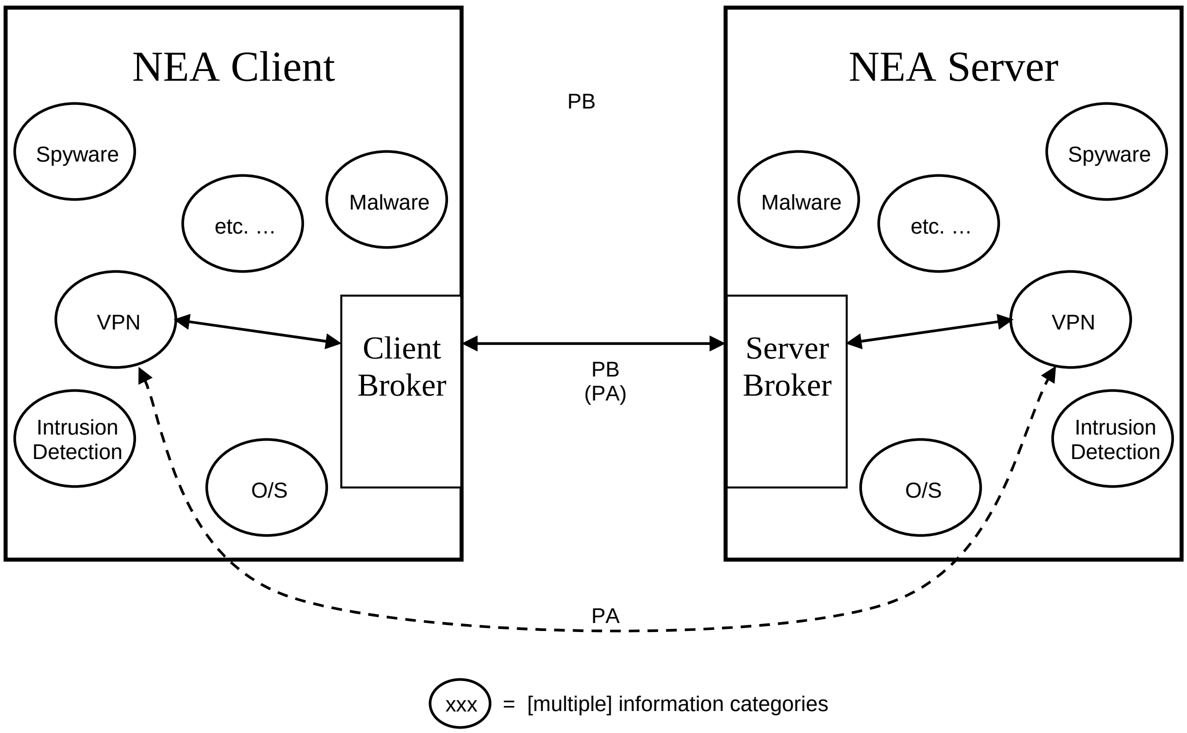
7. IDS – cont'd

On Thursday morning, the IDS group continued their discussions.

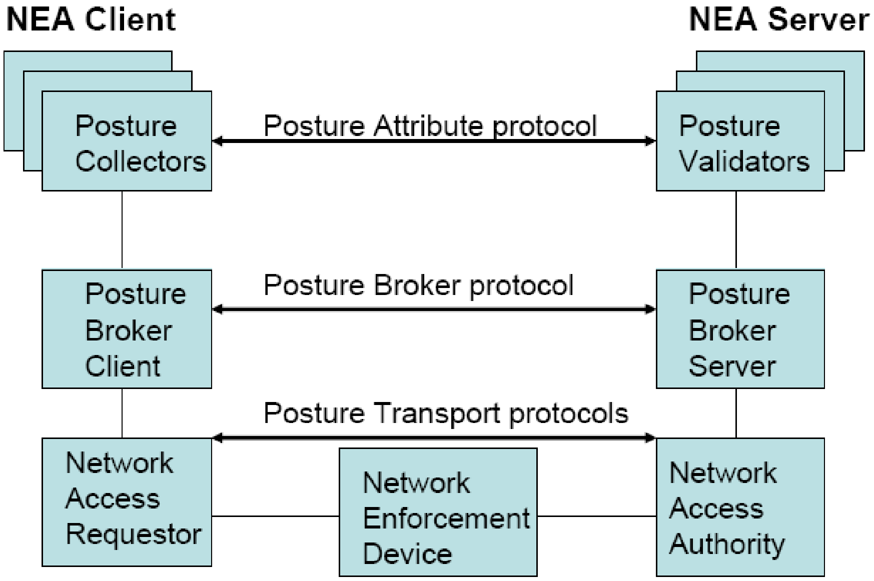
Ron commented that after examining the Microsoft document that was distributed, he feels that their technology is much further along than he previously thought.

8. Network Endpoint Assessment (NEA)

Randy started the session by discussing the IETF NEA WG status. He drew the following diagram:



Randy’s diagram can be compared to the architecture diagram that has been published by the NEA:



A “Posture” is defined in the NEA Requirements document to be the “configuration and/or status of hardware or software on an endpoint as it pertains to an organization's security policy.”

A proposal for the Posture Broker protocol has been submitted for review. Each broker is responsible for aggregating attributes as well as distributing them to multiple Posture Collectors.

The primitive attributes include the following items, and can be used in multiple categories for policy determination:

- Product information
- Numeric version
- String version
- Operational status
- Port filter
- Installed packages

As an example for the VPN category, he gave the following list of attributes that could be used:

- installed packages
- numeric version
- string version

The numeric version could be defined by the following set of items:

- Major version
- Minor version
- Build number
- Service pack major version

- Service pack minor version

Randy explained that he expects the above list to expand in the future, but said that these attributes are intended as "the basic meat" (i.e., fundamental attributes) of the technology. It was noted that they are very similar to the items identified in the Cisco attributes above.

Each of the attributes can be extended, including in vendor-specific (or organization-specific—such as PWG) methods.

Randy noted that over the wire, the NEA protocols are compatible/interoperable with the Trusted Computing Group's Trusted Network Connect (TNC) technology.

9. Proposed List of Attributes for IDS – Brainstorm

Ron encouraged the group to identify a preliminary set of suggested attributes that should be considered for use in the IDS activity. The following list was generated:

- Product name
- Product version
- Vendor name (ID)
- O/S name
- O/S version
- O/S installed date/time
- System application name [multiple entries]
  - Application version
  - Application type
  - Application installed date/time
- Certification state (token or opaque block)
- Configuration state
- Port filter (firewall setting)
- Build date
- Authorized accessibility state
- Services configuration
- Patches installed (hot fixes) [multiple entries]
- Bridging or forwarding enabled?
- Fax enabled? (modem, PSTN)
- Admin password = default? (or not enabled?)

There was some discussion about the significance or benefit of the installation date/time. It was suggested that the build date/time (and/or build number) would be more relevant.

There was some debate about whether the distinction of O/S vs. Applications is necessary or appropriate. For some printer devices, it could be argued that there is no Operating System. However, the debate was deferred.

After a while, the group was concerned that they might be generating a lot of system characteristics that aren't necessarily applicable or relevant to a "security posture."

One person observed that the list above had very few (zero?) attributes that were unique to imaging devices.

The above list was then reorganized into the following:

- Product
  - Product name
  - Product version
- Vendor
  - Vendor name
  - Vendor ID
- O/S
  - O/S name
  - O/S version and patches (hot fixes)
  - O/S installed date/time
- Applications (software packages)
  - Application name
  - Application version and patches (hot fixes)
- Firewall setting (port filter)
- Certification/configuration state (token?) [placeholder – multiple entries]
  - Bridging or forwarding enabled?
  - Fax enabled? (modem, PSTN)
  - Admin password = default? (or not enabled?)
  - Secure Time used?
  - Secure Time service trusted? [multiple entries]
  - Minimal security levels acceptable?
  - Minimal encryption key length?
  - Security algorithm specified?

10. Next Steps

Ron listed a few tasks for future work:

- Review and determine IDS attribute mappings to each:
  - Microsoft documentation
  - NEA documentation
- Start a Definition of Terms list (i.e., some documentation)
- Protocol mappings - what level of support do we include?

The following Action Items were assigned:

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

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

The following teams were identified to focus on the IDS attribute mappings:

Microsoft Team	NEA Team
Joe Murdock	Shah Batti
Peter Cybuck	Brian Smithson
Nancy Chen	Ron Bergman

The following target dates were established:

Review and IDS attribute mappings	June 23-27
Definition of Terms (first draft)	August
Protocol mappings	August
Level of support	October

Ira suggested that the IDS attributes should be made consistent with (or included in) the PWG Semantic Model. Randy disagreed, saying that they should be independent—although they could reference each other. The decision was deferred.

IDS Meeting adjourned.