PWG -Imaging Device Security (IDS) Working Group

Seattle area, WA

IDS-Microsoft F2F Meeting

August 17, 2009

Ron Nevo

PWG IP Policy

- Meeting conducted under rules of PWG IP Policy

Agenda for the F2F 8/17/09 afternoon IDS-NAP/Microsoft Meeting

- Assign Scribe
- PWG IP Statement
- PWG Introduction
- IDS Introduction
- Short overview of NAP (Microsoft) (approx. 1 hr.)
- How the IDS group proposes to map attributes to the NAP protocol (IDS) (Ron/Jerry/Brian/Joe/Randy/???)
- Discuss the alignment of attributes
- Discuss questions- new and previously submitted to the NAP team
- Discuss remote attestation – how to make sure the remote device does not lie about its statement of health (without a TPM, how reliable can it be?) Is this an important concern of the NAP team?
- Discussion on SHVs
- Discussion on how NAP framework will transition to support non-Windows devices
- NAP Demo

List of New Questions

- Assuming that there is a PWG plug-in, how will end customers obtain it? Windows Update? Eventually, in the Windows Server 20XX distribution? Optional download from Microsoft? Download from PWG? Or?
- If there are vendor-specific extensions to the plug-in, how will end customers obtain those?
- Once customers have the attribute definitions for assessing HCDs, how will they obtain the appropriate values? (e.g., what is the current firmware revision for vendor X, product Y?). By what mechanism will those be maintained by vendors?
- How will customers be assured that the sources for the plug-in, extensions, and current values have not been spoofed, and that their contents have not been tampered with?

List of old Questions and Answers

- 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.

  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.

List of old Questions and Answers

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.

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.