PWG Plenary Status Report
IDS Working Group

December 10, 2009

Austin, TX, PWG F2F Meeting

Joe Murdock (Sharp)

Brian Smithson (Ricoh)

Purpose of the effort

- The industry is moving beyond basic authentication for access to corporate networks to a more detailed assessment of the "health" of devices before allowing them to access the network.
  - Examples of what's being measured for PC Clients:
    - OS Type, Version, Patch Level
    - Anti-virus Type, Version, Definition Level, Is Active

- Hardcopy Devices attach to networks, but there's no standard set of metrics that is used to assess an HCD.
  - As a result, HCDs are treated as an exception and are allowed to attach to the network based solely on a MAC address.

- Our goal is to provide the metrics and mechanisms that allow HCDs to fully participate in assessment-protected networks.

Purpose of the effort

- The IDS working group is chartered to enable Hardcopy Device support in the network assessment protocols that measure and assess the health of client computers and other devices that are attached to enterprise networks.

- The group will define a set of common assessment attributes for Hardcopy Devices and will liaison with the specific network assessment protocol efforts to include Hardcopy Device support in these protocols where necessary.

- In the future, the IDS WG charter may be revised to allow the working group to deal with other types of Imaging Devices (Network Projectors, Displays, etc.) in network assessment protocols or other security-related work items.

Work Items for the WG

- What We're Doing
  - We are defining a standard set of metrics that can be measured or assessed in Hardcopy Devices to gauge if they should be granted access to a network.

  - Current targets are MS NAP and IETF NEA.

  - We are defining example "bindings" for how these metrics are used in the individual network assessment protocols.

- What We're NOT Doing
  - We are NOT defining any new assessment protocols, nor assessment extensions to existing authentication protocols.

  - We are NOT endorsing any of the competing network assessment protocols (TNC, NAC, NAP, NEA). Our goal is to enable Hardcopy Devices to participate in any/all of them.

Administration

- IDS WG Chairs
    - Joe Murdock (Sharp)
    - Brian Smithson (Ricoh)

- IDS WG Secretary:
    - Lee Farrell (Canon)

- IDS WG Document Editors:
    - HCD-ATR: Jerry Thrasher (Lexmark)
    - HCD-NAP: Joe Murdock (Sharp), Brian Smithson (Ricoh)
    - HCD-NEA: Randy Turner (Amalfi), Jerry Thrasher (Lexmark)

Current Status

- HCD Assessments Attributes document was developed and it is in stable condition now.

- HCD-NAP Binding Document under development.
  - Target completion date of Q1 2010.

- HCD-NEA Binding Document has been started.
  - Target completion date of Q2 2010.

- Recent/ongoing discussions with assessment protocol designers (Microsoft/NEA) to finalize and endorse the IDS Binding documents.

- There is an issue about how to deploy HCD NAP in practice: how can we get MS's SHV to recognize and apply HCD_ATR?

Next steps

- Address final comments on attributes specification.
- Finish NAP binding specification – (Q1 2010)
- Develop NEA binding specification – (Q2 2010)
- Seek approval/adoption w.r.t. assessment protocol vendors.
- Possible interop (?)
- Address deployment issues
  - How to securely populate and update SHVs with HCD attributes and base values from vendors?
  - Should we first target the MS SCCM SHV by defining HCD responses that do not require SHV changes?
- Address remediation issues.
  - Should remediation mechanisms be vendor-specific? Or HCD-industry specific? Or can it be solved in a general way?