PWG Plenary Status Report
IDS Working Group

June 10, 2010

Webster, NY, 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.

- Hardcopy Devices are currently allowed unfettered access to and storage of secure and controlled documents. There is no standard for controlling document access and defining usage behavior for protecting secure documents.

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

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 TCG TNC.
  - We are defining example "bindings" for how these metrics are used in the individual network assessment protocols.
  - We are defining standard attributes and values for authorizing Hard Copy Devices, their services and users to a secure network
  - We are defining standard attributes and values for specifying user and Hard Copy Device access to and operations on documents.

- 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:
  - Brian Smithson (Ricoh)

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

Current Status

- HCD Assessments Attributes document is stable.
  - XML Schema is under review
- HCD-NAP Binding Document is stable.
- HCD-TNC Binding Document is under development.
  - Target completion date of Q4 2010.
- HCD-Remediation Specification is under development
- SCCM mapping of IDS Attributes
  - Convert mapping proposal to a full fledged binding specification
- Investigating ways to get network management applications to support IDS attributes
  - Distributing IDS Business Use Case document
  - Microsoft System Center products
    - Forefront applications are being phased out in favor of SCCM
  - Symantec Endpoint Protection product line
    - Initiating contact with Symantec
- MPSA
  - Future focus group/survey with MPSA members for IDS use cases

Current Activities

- TNC Binding Specification – (Q4 2010)
  - Interaction with TCG Hardcopy Workgroup
- PWG IDS remediation specification (Q4 2010)
- Investigating Device and Document authorization attributes and parameters (TBD)
- Initiating investigation into defining standardize device log format for supporting security analysis (TBD)
- Seek adoption and support of IDS attributes by assessment protocol vendors