

PWG Plenary Status Report IDS Working Group

April 7, 2010

Camas WA, 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.

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:
 - Brian Smithson (Ricoh)
- 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 is stable.
- HCD-NAP Binding Document is stable.
- HCD-NEA Binding Document is under development.
 - Target completion date of Q3 2010.
- Investigating ways to get network management applications to support IDS attributes
 - Developing IDS Marketing Rational document
 - Microsoft System Center/Forefront products
 - No recent contact with Microsoft
 - 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?
 - Symantec Endpoint Protection product line
 - Initiating contact with Symantec

Next steps



- Transform NEA Binding Specification – (Q3 2010)
 - Interaction with TCG Hardcopy Workgroup
- Seek approval/adoption with respect to assessment protocol vendors.
- Address deployment issues
 - How to securely populate and update SHVs with HCD attributes and base values from vendors?
 - Should we also consider supporting the MS SCCM SHV by defining HCD responses that do not require SHV changes?
- Address remediation issues.
 - Develop initial draft of PWG IDS remediation specification
- Other possible topics will be discussed during the IDS WG F2F meeting