PWG -Imaging Device Security (IDS) Working Group

April 6, 2011

Cupertino, CA

PWG F2F Meeting

Joe Murdock (Sharp)

Brian Smithson (Ricoh)

Agenda

9:00 – 9:15	Administrative Tasks
9:15 – 9:45	Discussion on NAC (Direction and Attributes)
9:45 – 10:15	TNC Binding Discussion
10:15 – 10:45	Common Criteria
10:45 – 11:00	Break
11:45 – 11:30	Common Log
11:30 – 12:00	IDS Charter Review
12:00 – 13:00	Lunch
13:00 – 13:45	IAA and Security Ticket
13:45 – 14:00	Wrap up and adjournment
14:00 – 15:30	Open Printing

Administrative Tasks

- Select minute-taker
- Introductions
- IP policy statement:
  "This meeting is conducted under the rules of the PWG IP policy". If you don't agree, the Winchester Mystery House is open, if you can find it.
- Approve Minutes from March 24 conference Call

IDS WG Officers

- 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: Ira McDonald (Samsung), Jerry Thrasher (Lexmark), Brian Smithson (Ricoh)
  - HCD-HR (Health Remediation): Joe Murdock (Sharp)
  - HCD-NAP-SCCM: Joe Murdock (Sharp)
  - IDS-Log: Mike Sweet (Apple)
  - IDS-IAA: Joe Murdock (Sharp)
  - IDS-Model: Ira McDonald, Joe Murdock, Ron Nevo

Action Items

Action Item #	Entry date	Assignee	Type	Action	Status	Disposition
33	12/10/2009	Randy Turner Ron Nevo	SHV	Randy Turner will contact Symantec (when appropriate) to encourage discussion with the PWG about a SHV.		
34	12/10/2009	Randy Turner Ron Nevo	Remediation	Randy Turner will investigate Symantec's products and their method(s) to "remediate noncompliant endpoints." Ron Nevo will take over this activity. Randy will pass on his contacts to Ron.		Need to indicate to Symantec that we really don't need too much proprietary information from them, but want to give them our information. Can we get Symantec to attend the April meeting in Cupertino?
44	3/11/2010	Jerry Thrasher Ira McDonald Brian Smithson	NEA Binding	TCG TNC Binding document		Make it a TCG document, not an IETF NEA document
58	6/11/2010	Joe Murdock and Ira McDonald	SCCM	Create a first draft SCCM binding spec based on the NAP binding specC	H	MS is releasing R3 of SCCM and also a beta of "R-next", while at the same time adding power management; WIMS group may also be interested. On hold due to priorities.
67	10/28/2010	Joe Murdock Ira McDonald	auth	Write IDS-Identification-Authentication-and-Authorization-Framework specification	P	direction is not "recommendations only", it is "requirements and recommendations" (pointing to existing standards) because there will be a conformance section
73	12/9/2010	Joe Murdock Ira McDonald Ron Nevo	reqts spec	start an IDS common requirements spec to include out-of-scope and terminology sections		Base on new PWG template
76	2/3/2011	Bill Wagner, Brian Smithson	MPSA	Data security article: Bill to draft, Brian to finish		
77	2/3/2011	Joe Murdock	NAP Binding	Needs a prototype		
79	2/3/2011	Joe Murdock	Common Reqts	Change name from IDS-CR to IDS-REQ		
80	2/3/2011	Joe Murdock, Brian Smithson	WG admin	Update the description of the IDS WG to include scope that is larger than just NAC/NAP/etc		do this after Mike makes the new PWG web site and wiki pages
81	2/3/2011	Joe Murdock	IDS-LOG	Find the user role definitions in the IA&A or schema documents and import them into the LOG document		
83	2/24/2011	Brian Smithson	2600.1 SD	Propose a schedule for teleconferences with NIAP	P	Alternate with SC meeting, Thursdays at 2pm-3pm EST
84	3/10/2011	Joe Murdock	WG Admin	Review IDS Charter to make sure it still reflect new directions. Add discussion as a F2F topic	P	
85	3/24/2011	Brian Smithson	2600.1 SD	Final review of project charter and send to SC for approval		make it initial draft in advance of F2F

Stable Documents

- HCD-Assessment-Attributes

  ftp://ftp.pwg.org/pub/pwg/ids/wd/wd-idsattributes10-20110127.pdf
  - Stable (needs a binding prototype)
- HCD-NAP Binding

  ftp://ftp.pwg.org/pub/pwg/ids/wd/wd-ids-napsoh10-20100930.pdf
  - Stable
- HCD-NAC Business Case White Paper

  ftp://ftp.pwg.org/pub/pwg/ids/white/tb-ids-hcd-nac-business-case-20100422.pdf
  - Final

Active Document Status

- HCD-TNC Binding
  - Initial Draft still under development
- HCD-Health Remediation

  ftp://ftp.pwg.org/pub/pwg/ids/wd/wd-ids-remediation10-20100930.pdf
  - Initial Draft
- HCD-NAP-SCCM Binding
  - On hold
- IDS Charter

  ftp://ftp.pwg.org/pub/pwg/ids/wd/wd-ids-charter-20110331.pdf
- IDS-Log

  ftp://ftp.pwg.org/pub/pwg/ids/wd/wd-ids-log10-20110326.pdf
  - Draft
- IDS-Identification-Authentication-Authorization

  ftp://ftp.pwg.org/pub/pwg/ids/wd/wd-ids-iaa10-20110402.pdf
  - Draft
- IDS-Model

  ftp://ftp.pwg.org/pub/pwg/ids/wd/wd-ids-model10-20110402.pdf
  - Draft

NAC

- HCD Remediation specification
  - Rename to HCD Health Remediation to limit scope to NAC Health attributes? Remediation may spill out to other aread of IDS work. These should probably be in a separate document?
  - The current spec is driven by health assessment, but the larger function of remediation also includes things like monitoring and enforcing site policy that isn't strictly related to system health
- NAC discussions at RSA seem to indicate that NAC is being used not just (or even to) authenticate systems onto a network, but is now being used as a means to kick systems off the network. This is not necessarily associated with any particular bad set of health attributes, but just "you're misbehaving, get off my network."
  - Does this have any effect of our current thinking of NAC for Imaging devices?

NAC

- New NAC Attributes
  - HCD_SysLog_URI (string)
    - The HCD_SysLog_URI attribute is a variable length string that specifies the location(s) where the HCD's system log is to be stored. Locations are provided as a URI and MUST conform to RFC 2396. When multiple locations are provided, the log is to be written to locations in the order indicated by the list, starting with the first provided location. If no explicate HCD_SysLog_URI locations have been defined by a system administrator, the system default internal log location MUST be returned
  - HCD_SysLog_Enabled (boolean)
    - The HCD_SysLog_Enabled attribute is a Boolean value that indicates if system logging is enabled for the device. If system logging is disabled (HCD_SysLog_Enabled = FALSE) then any value set for HCD_SysLog_URI is ignored.
  - NAC IDS Authentication Service Attribute
  - Additional IDS Security Attributes?

HCD-TNC Binding

- Real-time document editing

IEEE 2600.1 Supporting Documents

- NIAP CC Status
- Common Criteria Support Documents Project Charter
  ftp://ftp.pwg.org/pub/pwg/ids/wd/wd-ids2600sd-charter-20110324.pdf
- 2 Week review period
- Send to Steering Committee for acceptance

IDS Log

- Document Review

  ftp://ftp.pwg.org/pub/pwg/ids/wd/wd-ids-log10-20110326-rev.pdf
  ftp://ftp.pwg.org/pub/pwg/ids/wd/wd-ids-log10-20110326.pdf
  ftp://ftp.pwg.org/pub/pwg/ids/wd/wd-ids-log10-20110326.docx

IDS Charter Review

ftp://ftp.pwg.org/pub/pwg/ids/wd/wd-ids-charter-20110331.docx
ftp://ftp.pwg.org/pub/pwg/ids/wd/wd-ids-charter-20110331.pdf

IDS IAA

- XML Schema
  ftp://ftp.pwg.org/pub/pwg/ids/white/ids-security-20110402.xsd
- IDS-IAA Specification
  ftp://ftp.pwg.org/pub/pwg/ids/wd/wd-ids-iaa10-20110402.docx
  ftp://ftp.pwg.org/pub/pwg/ids/wd/wd-ids-iaa10-20110402.pdf
- IDS-Model Specification
  ftp://ftp.pwg.org/pub/pwg/ids/wd/wd-ids-model10-20110402.docx
  ftp://ftp.pwg.org/pub/pwg/ids/wd/wd-ids-model10-20110402.pdf
- IDS-IAA Bindings
  - IPP*
    - Security Ticket in JPS3?
  - PWG Cloud
  - Registration/Discovery Bindings?
- Advertisement of supported security capabilities?
  - Add a supported security element to the security ticket?
  - Overload of xxxSecurity?
  - A separate element in the system or service capabilities?
  - In the semantic model, the system object would provide all supported methods, while each service (system, print, etc.) would list only those used by the service.
- Physical hardware security requirements (e.g. encrypted disk, etc.)

Cloud Consideration in the Security Ticket

- How does the printer advertise it's public key?
  - How best to pass the public key through a cloud manage/provider directly to the user?
  - Do we add public key to the identity element?
- Need to consider what to encrypt
  - Can’t just encrypt the whole data stream
  - In a cloud environment, want to provide end-to-end encryption of job data, but the job ticket (or at least the security ticket) needs to be readable by the cloud print provider and manager so they can match security requirements between the user, devices and services.
- Cloud Job privacy
  - How to avoid tracking of a job or partial interception.
  - Provide a way to explicitly hide job origination information?
    - Runs contrary to the IDS logging assumptions, but is this appropriate for the cloud use model?

Wrap up

- Review of new action items and open issues
- Conference call / F2F schedule
  - Next Conference call April 21/28, 2011
- Adjournment