PWG -Imaging Device Security (IDS) Working Group

May 26, 2011

Webster, NY

PWG F2F Meeting

Joe Murdock (Sharp)

Brian Smithson (Ricoh)

Agenda

9:00 – 9:15	Administrative Tasks
9:15 – 9:40	IDS IAA
9:40 – 10:00	IDS Model
10:00 – 11:00	Common Criteria
11:00 – 11:15	Short Break
11:15 – 12:00	IDS Model and Use Cases (NAC/IDS Attributes)

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 May 12 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	Investigate Symantec's products and their method(s) to "remediate noncompliant endpoints."		Need to indicate to Symantec that we really don't need too much proprietary information from them, but want to give them our information.
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 Ira McDonald	SCCM	Create a first draft SCCM binding spec based on the NAP binding specC	H	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 "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	P	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		
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		
85	3/24/2011	Brian Smithson	2600.1 SD	Final review of project charter and send to SC for approval		Delayed until after NIAP coordination conference
86	4/6/2011	Ira McDonald	HCD-ATR	Inquire with S. Hanna about the importance (or lack) of having attributes for authentication service, log URI, and log enabled		
87	4/6/2011	Ira McDonald	TNC Binding	Inquire with S. Hanna about whether flat binding is appropriate for embedded systems like MFPs, referring to IF-TLV document		
88	4/6/2011	Brian Smithson	2600.1 SD	Post a reminder to the list to read the whitepaper ftp://ftp.pwg.org/pub/pwg/ids/white/2600sd-20110223.pdf		
89	4/6/2011	Brian Smithson	2600.1 SD	Outline ideas/proposals for SD		
90	4/6/2011	Michael Sweet	IDS-LOG	Change the title so as to PWG Common Log Format		
92	4/6/2011	Michael Sweet	IDS-LOG	Update the rational section to higher-level statements		see 4/6/2011 minutes
93	4/6/2011	Brian Smithson	IDS-LOG	Send a message to the list to solicit use cases for the log spec		
94	5/12/2011	Joe Murdock	reqts spec	Placement of alerts in the semantic model document		

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
- IDS Charter

  ftp://ftp.pwg.org/pub/pwg/ids/charter/ch-ids-charter-201100503.pdf
  - Updated charter approved by Steering Committee

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
- 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-iaa10-20110524.pdf
  - Draft
- IDS-Model

  ftp://ftp.pwg.org/pub/pwg/ids/wd/wd-ids-model10-20110524.pdf
  - Draft

IDS IAA

- IDS-IAA Specification
  ftp://ftp.pwg.org/pub/pwg/ids/wd/wd-ids-iaa10-20110524.pdf

IDS Model

- IDS-Model Specification Review
  ftp://ftp.pwg.org/pub/pwg/ids/wd/wd-ids-model10-20110524.pdf

IEEE 2600.1 Supporting Documents

- Project status on hold pending the call with NIAP
- Conference call with NIAP

IEEE 2600.1 Supporting Documents

Source	Content	Purpose	Notes and examples
Vendors, labs, and schemes	Clarifications and errata	Specify PP intent; correct errors	The P2600 PP Guide http://grouper.ieee.org/groups/2600/PP%20Guide/P2600%20PP%20Guide%20v1.1.pdf is both a source and a destination for this information. Comments received by vendors or by NIAP are discussed in an internal P2600 mailing list.
Labs and schemes	Evaluation experience	Consistent interpretation, easier evaluation, case studies	Evaluation experience would require some sanitization and permission from both vendor and lab
Vulnerability databases	Historical vulnerability reports for HCDs	Refine AVA to be more applicable to this technology	http://web.nvd.nist.gov/view/vuln/search-results?query=mfp&search_type=all&cves=on, http://secunia.com/advisories/search/?search=mfp, http://osvdb.org/search?search[vuln_title]=mfp&search[text_type]=titles
"Top N" documents	Current "top" security issues for all technologies	Identify those that may apply to this technology, and refine AVA	https://www.owasp.org/index.php/Category:OWASP_Top_Ten_Project, http://www.sans.org/critical-security-controls/, http://cwe.mitre.org/top25/, http://www.sans.org/top-cyber-security-risks/
Research reports and demonstrations	Threats and mitigations that may not have been considered in the PP	Additional items for AVA	http://www.ipa.go.jp/security/fy21/reports/mfp/documents/20100830report.pdf, http://www.shmoocon.org/speakers#printerpwnd, http://www.shmoocon.org/speakers#printerwild
SPANSTIG and other STIGs	Technical requirements, and capabilities required for administrative requirements	Guidance for products being sold into US DoD market	Only deal with STIG requirements that the TOE can actually control and deliver
NIST SP800 series		General guidance or specific guidance for US Govt market	Some are general; others are US specific
Various sources (?)	Best implementation practices for particular SFRs	Identify and require currently appropriate crypto algorithms, key sizes, protocols, protocol versions, etc.	This should ensure that relatively static high-level SFRs are implemented in products using relatively dynamic best practices
National governments	National policies, especially crypto (e.g., FIPS 140-2)	Guidance for products being sold into national markets	Government procurement/use policies, crypto import restrictions, etc.

IDS Model

- IDS-Model Specification Review
  ftp://ftp.pwg.org/pub/pwg/ids/wd/wd-ids-model10-20110524.pdf
- IDS Use Cases

NAC

- Final decision:
  - Do we update the HCD NAC Attributes specification or create a new IDS NAC Attributes specification?
- New NAC Attributes
  - HCD_SecurityLog_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_SecurityLog_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.
  - IDS_Authentication_Service_URI Attribute
    - The HCD_SysLog_Enabled attribute is a variable length string that identifies the server(s) or service(s) the HCD will use to authenticate itself, users and remote devices or services.
- TCG Input on above attributes?

IDS IAA

- 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.

Cloud Considerations 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 June 16, 2011
- Adjournment