PWG Imaging Device Security (IDS) Working Group

December 6, 2012

Irvine, CA

PWG F2F Meeting

Joe Murdock (Sharp Labs)

Agenda

IDS Session

1:00 – 5:00

Topics

- Administrative Tasks
- PWG Log
- HCD Attributes
- IDS Model
- NIAP/PP
- TNC/NEA

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 Auto Show is on all week.
- Approve Minutes from November 26 conference Call

IDS WG Officers

- IDS WG Chair
  - Joe Murdock (Sharp)
- IDS WG Vice-Chair
  - Vacant
- IDS WG Secretary:
  - Alan Sukert (Xerox)
- IDS WG Document Editors:
  - HCD-ATR: Jerry Thrasher (Lexmark), Joe Murdock (Sharp)
  - HCD-TNC: Ira McDonald (High North)
  - IDS-Model: Joe Murdock (Sharp), Ira McDonald (High North), Ron Nevo (Samsung)
  - IDS-Log: Mike Sweet (Apple)
  - IDS-IAA: Joe Murdock (Sharp)

Action Items

Action Item #	Entry date	Assignee	Type	Action	Status	Disposition
126	11/26/2012	Joe Murdock	Log, HCD-Attr, HCD-NAP	Send out PWG Last call announcement for IDS-Log, HCD-Attributes and HCD-NAP Specs.	C	

NAP Binding

HCD-NAP Binding Anonymous Prototype report

A PWG member company has prototyped the PWG HCD Health Attributes NAP Protocol Binding with the following reported results:

"We did a prototype of NAP on an MFP in 2009-2010. The most recent specs to which the prototype was developed were wd-idsattributes10-20100409.pdf and wd-ids-napsoh10-20100409.pdf.

We tested using 802.1x, not the other protocols. We implemented all of the mandatory attributes.

We didn't have any user apps or patches installed, there was no PSTN, and forwarding wasn't supported in the device, so we didn't test the conditionally mandatory attributes.

We didn't do any of the optional attributes.

It all worked well enough as a demonstration prototype.

However, we did find an issue with HCD_Default_Password_Enabled: which password (or passwords) should be checked?
If there are multiple administrative logins, should all be checked? What if some of them are not security-relevant? What if some could be considered security-relevant but do not administer any of the settings that are covered by the health check?

If there are different passwords for different administrative protocols (e.g., http, ssh, …), should all be checked?"

Cheers,
- Ira (PWG Secretary)

Documents in PWG Last Calls

- HCD-Assessment-Attributes
  ftp://ftp.pwg.org/pub/pwg/ids/wd/wd-idsattributes10-20121113.pdf

- HCD-NAP Binding
  ftp://ftp.pwg.org/pub/pwg/ids/wd/wd-ids-napsoh10-20121112.pdf

- PWG-LOG
  ftp://ftp.pwg.org/pub/pwg/ids/wd/wd-ids-log10-20121112.pdf
  "Apple has successfully prototyped support for PWG Common Log Format based on the current draft." - Email from Michael Sweet, July 27, 2012

PWG Last Call Comments

- HCD-Assessment-Attributes
  1. What kind of "administrator passwords or other credentials" are included? Only passwords for admin accounts that are security-relevant (e.g., not an administrator password that permits a device admin to change non-security settings)?
  2. What kind of credentials?
  3. Although not as important as the first clarification, it might be more clear to change the sense of the whole thing to "DefaultPasswordsChanged" (0 = not changed).

  During the updates to this HCD-TNC document based on
  IDS WG review on 6 June 2012, I discovered several mandatory changes
  to HCD-ATR (and therefore HCD-NAP) which were agreed but NOT
  implemented in the current versions out for PWG Last Call. See:
  ftp://ftp.pwg.org/pub/pwg/ids/minutes/ids-f2f-minutes-20120606.pdf
  - see especially decisions to change mandatory attributes

- HCD-NAP Binding

  See Assessment Attributes comments

PWG Last Call Comments

- PWG-LOG

  Section 3.3 Out of Scope

  While we're not specifying a standard for any of the mechanisms or functionality in section 3.3, we do include a statement that impacts:

  6. Data Protection Policies

  For instance, in section 6, "Conformance Requirements", #2 and #3 deal specifically with items that would be included in a data protection policy

  And in section 9 "Security Considerations", we again require integrity protection of the log information.

  We may want to modify the "out of scope" section to state that we are placing requirements on data protection policies, but not including recommendations for a "soup to nuts" data protection policy for logging information (of course, "soup to nuts" may not be appropriate for the actual text, but hopefully you get the idea)

  By the way, the sentence in section 9 I'm referring to above is written as:

  485. Device MUST provide protection from alteration both on the device and when distributed outside the device.

  IMHO, this wording should be more specific….something like:

  Imaging devices MUST provide integrity protection for log message data, both on the device, as well as when the log data is transported outside the device.

  The original text doesn't explicitly state what might be altered.

Active Documents

- HCD-TNC Binding
  ftp://ftp.pwg.org/pub/pwg/ids/wd/wd-ids-tnc10-20121202-rev.pdf
- IDS-Model
  ftp://ftp.pwg.org/pub/pwg/ids/wd/wd-ids-model10-20120806-rev.pdf
- IDS-IAA
  ftp://ftp.pwg.org/pub/pwg/ids/wd/wd-ids-iaa10-20111005-rev.pdf

Document Review

- HCD-TNC Binding
  ftp://ftp.pwg.org/pub/pwg/ids/wd/wd-ids-tnc10-20121202-rev.pdf

New MFP Protection Profile

- Kicked-off of the Multifunctional Printer (MFP) Technical Community (TC) to create a MFP Protection Profile on 9/12/12
  - Will be a replacement for IEEE 2600.2 which is currently approved NIAP Protection Profile for MFPs
  - Will also be a replacement for IEEE 2600.1 which is used internationally and is approved by NIAP as an alternative to IEEE 2600.2 for evaluations performed outside of the US
  - Joint IPA (Japanese CC* Scheme) and NIAP (US CC Scheme) effort, with IPA as the lead
  - Vendors from the US and Japan joined in person or by telephone

*Common Criteria

New MFP Protection Profile

- Status:
  - Initial draft of Software Problem Definition (SPD) - threats, assumptions, security objectives - prepared by IPA
  - NIAP with help from a small group of vendors created an alternate draft SPD which was reviewed and commented on by IPA
  - Full MFP Technical Committee working with both NIAP and IPA to finalize SPD and start work on Security Functional Requirements (SFRs) and Security Assurance Requirements (SARs)
- Proposed NIAP/IPA Schedule at MFP TC Kickoff:
  - Complete SPD by end of December 2012
  - Complete PP by end of March 2013
- In actuality we may have a draft PP by Sep 2013 for ICCC 2013 if we are very lucky

New MFP Protection Profile

- SPD Major Issues Still to be Resolved:
  - Scope of PP: Apply to MFPs only or apply also to network printers/scanners
  - Address specifics (such as RFCs) for standardized security protocols and their versions (e.g., TLS 1.2) versus provide general secure protocol requirements
  - Whether or not to require self-test on start-up and/or self-test associated with repair/trusted updates

Proposed IDS activity to provide input to MFP TC

- The MFP Technical Community is an open, international working group
- Although it has an active discussion forum on the CC Users Forum collaboration site (https://ccusersforum.teamlab.com/), it has had few face-to-face or teleconference meetings.
- The PWG IDS could serve as a useful forum for vendors to be informed of progress and discuss current issues from the MFP TC
- As a vendor group, the PWG IDS could also provide collaborative input to the MFP TC -- similarly to the JBMIA in Japan
- A few notes:
  - The MFP PP will be published by the US and JP CC schemes; it would not be a PWG document
  - Participation in the proposed IDS activity is not a substitute or alternative to directly participating in the MFP TC; the IDS activity is intended to enhance participation in the MFP TC.
- To participate in the MFP TC, join the CC Users Forum (https://ccusersforum.teamlab.com/) if you are not already a member, and then send an email to bsmithson@ricohsv.com with a request to join the MFP TC

TCG Update

- Summary - publication of last three NEA WG documents as RFCs is expected in early 2013.
- Current status of the last three IETF NEA WG documents:
  - NEA Asokan Attack Analysis
    - http://datatracker.ietf.org/doc/draft-ietf-nea-asokan/
    - approved by IESG for Informational RFC on 19 October
  - PT-TLS: A TLS-based Posture Transport (PT) Protocol
    - http://datatracker.ietf.org/doc/draft-ietf-nea-pt-tls/
    - second IESG last call for standards-track RFC started 5 November
    - second LC due to late IPR disclosure from Cisco
  - PT-EAP: Posture Transport (PT) Protocol For EAP Tunnel Methods
    - https://datatracker.ietf.org/doc/draft-ietf-nea-pt-eap
    - final draft for IESG last call as standards-track RFC on 12 November
    - also affected by late IPR disclosure from Cisco
- TCG has a "fast track" arrangement with ISO so that these TNC core specs could become ISO specs quickly.
- TNC is currently coordinating with XACML and OASIS for access policy statements

Future Activities

- Resume Health Remediation specification
  - TNC community has expressed interest in health remediation
- Possible collaboration with MFP Technical community on Protection Profile work
- Definition of core set of Policy Attributes with XACML, SAML and WS-Policy, etc. bindings
  - Addition to IAA specification
  - Industry preference for XACML – SAML is too verbose with unacceptable performance

Wrap up

- Review of new action items and open issues
- Conference call / F2F schedule
  - Next Conference call January 7, 2012