PWG -Imaging Device Security (IDS) Working Group

Webster, NY- PWG F2F Meeting

June 11, 2010

Joe Murdock (Sharp)

Brian Smithson (Ricoh)

Agenda

09:00 – 09:15 Administrative Tasks
09:15 – 09:30 Review action items
09:30 – 10:00 Document status and Review
10:00 – 10:15 NEA and TCG Updates
10:15 – 10:30 SCCM Binding Document
10:30 – 10:45 Break
10:45 – 11:00 MPSA Survey/Focus
11:00 – 12:00 Standard Log File Discussion
12:00 – 13:00 Lunch break
13:00 – 14:45 Authorization Framework
14:45 – 15:00 Wrap up and adjournment

Administrative Tasks

- Select minute-taker
- Introductions
- IP policy statement:
  "This meeting is conducted under the rules of the PWG IP policy"
- Approve Minutes from June 3 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: Randy Turner (Amalfi), Jerry Thrasher (Lexmark)
  - HCD NAC Business Case: Joe Murdock (Sharp)
  - HCD-Remediation: Joe Murdock (Sharp)

Action Items

Action Item #	Entry date	Assignee	Type	Action	Status	Disposition
33	12/10/2009	Randy Turner	SHV	Randy Turner will contact Symantec (when appropriate) to encourage discussion with the PWG about a SHV.		No longer blocked waiting for AI #32 so we can send market rationale to Symantec.
34	12/10/2009	Randy Turner	Remediation	Randy Turner will investigate Symantec's products and their method(s) to "remediate noncompliant endpoints."		Symantec wants an NDA, but PWG cannot do an NDA; will do a generic version; should we invite Symantec to a PWG IDS teleconference?
38	2/11/2010	Joe Murdock	Binding docs	Investigate localization issue	C	Cannot find any information about this in MS documents; Joe will add a localization attribute to the NAP binding spec
41	2/25/2010	Joe Murdock	Remediation	look at providing a remediation URL(s?)		Joe has begun making an actual spec for remediation based on whitepaper
44	3/11/2010	Randy Turner	NEA Binding	Recast the NEA Binding document as a TCG TNC Binding document		Make it a TCG document, not an IETF NEA document
45	4/8/2010	Ira McDonald Pete Zehler	Attributes	Add HCD attributes to the system object in the MFD semantic model	P	Initial Schema has been written
47	4/8/2010	all	general	Take another look at SCAP and figure out what if anything to do in IDS		to be discussed at 6/10 f2f
48	4/8/2010	Randy Turner	auth	post to the IDS list the problem statement about authorization	C	
49	4/8/2010	all	auth	look at XACML and geoXACML (www.geoxacml.org)		
51	4/8/2010	Randy Turner	log format	compile wishlist for standard log content and format	C	
52	5/20/2010	all	log format	Look at LogFS (http://www.logfs.org) and syslog (http://datatracker.ietf.org/wg/syslog/ and optionally http://www.syslog.org/)		
53	5/20/2010	Joe Murdock and Brian Smithson		Do a brief overview and link to the market rationale for discussion/comment by MPSA (Jim Fitzpatrick)		

Document Status

- HCD_ATR
  ftp://ftp.pwg.org/pub/pwg/ids/wd/wd-idsattributes10-20100409.pdf
  - Stable (needs a binding prototype)
- HCD_NAP Binding
  ftp://ftp.pwg.org/pub/pwg/ids/wd/wd-ids-napsoh10-20100608.pdf
  - Prototype
- HCD_TNC Binding
  - Initial Draft still under development
- HCD NAC Business Case White Paper
  ftp://ftp.pwg.org/pub/pwg/ids/white/tb-ids-hcd-nac-business-case-20100422.pdf
  - Final
- HCD_Remediation

  URL TBD
  - Initial Draft

NAC Story

When the Trussville (Ala.) City Schools set out to keep non-Trussville assets off its production network – a common problem in public organizations – it originally went with a traditional Network Access Control (NAC) vendor.

Problem was, their issue required more than NAC – it wasn't just a matter of blocking non-Trussville assets, **as they found out when their NAC tool blocked devices such as printers and cafeteria cash registers**.

Review

- NAP Binding

  ftp://ftp.pwg.org/pub/pwg/ids/wd/wd-ids-napsoh10-20100608.pdf
- XML Schema

  ftp://ftp.pwg.org/pub/pwg/mfd/white/health-20100525.xsd

Reports/Discussions/Plans

- NEA Updates
- TCG Hardcopy Update (Ira/Brian)
- SCCM Binding Document
- MPSA Survey/Focus Group
- Standard Log File Formats for Printers and MFDs
- Authorization Framework for Hardcopy Devices

TCG Overview

- TCG Website
  - http://www.trustedcomputinggroup.org/
- TCG Developer Resources
  - http://www.trustedcomputinggroup.org/developers
- TCG Description
  - The Trusted Computing Group (TCG) is a not-for-profit organization formed to develop, define and promote open, vendor-neutral, industry standards for trusted computing building blocks and software interfaces across multiple platforms
- TCG Membership Levels
  - TCG Promoter Member ($55,000/year) – voting
  - TCG Contributor Member ($16,500/year) – voting
  - TCG Adopter Member ($8,250/year) – non-voting

TCG Workgroups

- Authentication
- Hardcopy
- Infrastructure
- Mobile Phone
- PC Client
- Server Specific
- Storage
- Trusted Network Connect (TNC)
- Trusted Platform Module (TPM)
- TCG Software Stack (TSS)
- Virtualized Platform

TCG Hardcopy WG - Status

- Current focus
  - Datatypes (applications, firmware, resources, logs, etc.)
    - Threats against Hardcopy Device (e.g., disclosure, modification)
    - Threats against other network devices via compromised HCD (e.g., unauthorized usage, distributed denial-of-service)
    - Defenses (e.g., strong authentication, digital signatures)
- Next steps
  - Use Cases (trusted startup, trusted services, etc.)
    - Use TCG standards (e.g., TNC, TPM, Opal secure drives)
    - Use PWG standards (e.g., PWG Scan Service w/ WS-Security)
  - Requirements (for HCD and mobile/PC clients)
    - Use TCG standards and technologies
    - Use PWG Semantic Model terminology (e.g., storage, interface, console, interpreter, marker, scanner)

SCCM Binding

- Suggestion that we make a separate binding document for SCCM
  - Start with the existing SCCM mapping paper

    ftp://ftp.pwg.org/pub/pwg/ids/white/IDS-NAP-SCCM-Mapping_20090917.xls
  - Produce a formal document to map IDS Attributes to existing SCCM attributes

MPSA IDS Liason

- Need to write intro
- Submit with Business Case document

Log File Formats

- Standard Log File Formats for Printers and MFDs
  - Randy's Log document

    ftp://ftp.pwg.org/pub/pwg/ids/white/ids-logging.pdf
  - Discuss Brian's Log Standards Summary

    ftp://ftp.pwg.org/pub/pwg/ids/white/IEEE2600.1_audit_events.pdf

Authorization Framework

- Define an Authorization Framework for Hardcopy Devices
- Randy's authorization document
  ftp://ftp.pwg.org/pub/pwg/ids/white/ids-authorize.pdf
- Anything we can use from P2600?
- Limit initial scope to defining a set of policy definitions and values
  - Then provide "bindings"
- Policies can be applied to a device, document or user
- Need to be able to define override precedence
  - who overrides who
  - what over what
  - Who overrides what
  - What overrides who

Authorization Framework

- Define basic MFP operation policy definitions
  - can scan
  - can print
  - can copy
  - can fax
  - can access external data
  - document repository control
  - cannot use mobile device
  - will not accept from wireless
  - etc.
- Do we want to cover general policies like use color, must duplex?
- Define Document Policies?
  - No Print
  - No Copy
  - No Scan
  - etc.

Authorization Framework

- Cloud Printing
  - What special authorization issues might arise from a cloud printing model
  - Printer registration in the cloud?
    - Policies for cloud user
- Mobile
  - Specific device policies
  - Location conditions

Wrap up

- Review of new action items and open issues
- Conference call / F2F schedule
  - Next Conference call June 24, 2010
- Adjournment