

# PWG -Imaging Device Security (IDS) Working Group

Bagsværd, Denmark- PWG F2F Meeting

August 6, 2010

Joe Murdock (Sharp)

Brian Smithson (Ricoh)

# Agenda

---



- 12:30 – 12:45 Administrative Tasks
- 12:45 – 13:00 Review action items
- 13:00 – 13:15 Document status and Quick Review
- 13:15 – 13:45 NEA and TCG Updates
- 13:45 – 14:30 MPSA Liaison discussion
- 14:30 – 14:45 Break
- 14:45 – 15:30 Remediation Specification
- 15:30 – 16:30 Standard Log File discussion
- 16:30 – 16:45 Break
- 16:45 – 17:30 Authorization Framework discussion
- 17:30 – 17:45 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"  
If you don't agree, Legoland is open...*
- Approve Minutes from July 22 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)
  - HCD-NAP-SCCM: Joe Murdock (Sharp)
  - HCD-Log: Mike Sweet (Apple)
  - HCD-Authorization: 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?
41	2/25/2010	Joe Murdock	Remediation	look at providing a remediation URL(s?)	C	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
53	5/20/2010	Joe Murdock and Bill Wagner		Do a brief overview and link to the market rationale for discussion/comment by MPSA (Jim Fitzpatrick)		Joe will work with Bill on articles, surveys, etc., to create and maintain a presence with MPSA
58	6/11/2010	Joe Murdock and Ira McDonald	SCCM	Create a first draft SCCM binding spec based on the NAP binding spec		
59	6/11/2010	Michael Sweet	log format	Create a first draft of a common logging specification	C	
60	6/11/2010	Joe Murdock	auth	First draft of potential resource predicate values (objects, operations, etc.)		

# Document Status

---



- HCD-Assessment-Attributes  
<ftp://ftp.pwg.org/pub/pwg/ids/wd/wd-idsattributes10-20100712.pdf>
  - Stable (needs a binding prototype)
- HCD-NAP Binding  
<ftp://ftp.pwg.org/pub/pwg/ids/wd/wd-ids-napsoh10-20100712.pdf>
  - Stable
- 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

# Document Status



- HCD-Remediation

<ftp://ftp.pwg.org/pub/pwg/ids/wd/wd-ids-standard-remediation10-20100730.pdf>

- Initial Draft

- HCD-NAP-SCCM Binding

Mapping Spreadsheet:

[ftp://ftp.pwg.org/pub/pwg/ids/white/IDS-NAP-SCCM-Mapping\\_20090917.xls](ftp://ftp.pwg.org/pub/pwg/ids/white/IDS-NAP-SCCM-Mapping_20090917.xls)

- Specification under development

- HCD-Authorization

White Paper:

<ftp://ftp.pwg.org/pub/pwg/ids/white/ids-authorize-20100608.pdf>

<ftp://ftp.pwg.org/pub/pwg/ids/white/ids-authorization-predicates-20100805.xlsx>

- Specification under development

- HCD-Log

White Papers:

<ftp://ftp.pwg.org/pub/pwg/ids/white/ids-logging-20100608.pdf>

[ftp://ftp.pwg.org/pub/pwg/ids/white/IEEE2600.1\\_audit\\_events.pdf](ftp://ftp.pwg.org/pub/pwg/ids/white/IEEE2600.1_audit_events.pdf)

Specification:

<ftp://ftp.pwg.org/pub/pwg/ids/wd/wd-ids-log10-20100803.pdf>

- Initial Draft

# Quick Document Review

---



- NAP Binding

<ftp://ftp.pwg.org/pub/pwg/ids/wd/wd-ids-napsoh10-20100712.pdf>

- IDS Attributes

<ftp://ftp.pwg.org/pub/pwg/ids/wd/wd-idsattributes10-20100712.pdf>



# Reports/Discussions/Plans

---



- NEA Updates (Randy/Jerry)
- TCG Hardcopy Update (Ira/Brian)
- 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
  - 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)
  - 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
  - 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)

# MPSA IDS Liason

---



- Group Discussion (WIMS and IDS)
- Develop proposed schedule
  - Articles
  - Surveys
  - Focus Groups
- Submit with NAC Business Case document

# Review/Discussion

---



- HCD-Remediation

<ftp://ftp.pwg.org/pub/pwg/ids/wd/wd-ids-standard-remediation10-20100730.pdf>

- HCD-Log

<ftp://ftp.pwg.org/pub/pwg/ids/wd/wd-ids-log10-20100803.pdf>

- HCD-Authorization

<ftp://ftp.pwg.org/pub/pwg/ids/white/ids-authorization-predicates-20100805.xlsx>

# HCD-Remediation

---



- HCD-Remediation

<ftp://ftp.pwg.org/pub/pwg/ids/wd/wd-ids-standard-remediation10-20100730.pdf>

# 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>
  - Specification  
<ftp://ftp.pwg.org/pub/pwg/ids/wd/wd-ids-log10-20100803.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>
- Predicate worksheet  
<ftp://ftp.pwg.org/pub/pwg/ids/white/ids-authorization-predicates-20100805.xlsx>
- 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
  - User Location (phone, laptop)
  - MFP Location conditions
    - Presumed valid for MFP
    - HCD Health Attribute for Location settings
      - Boolean Value similar to Admin Password
      - Actual Location value
    - Geo Location
    - Office location (not just for mobile)
      - Organizational Unit

# Wrap up

---



- Review of new action items and open issues
- Conference call / F2F schedule
  - Next Conference call August 19, 2010
- Adjournment