PWG -Imaging Device Security (IDS) Working Group

October 20, 2010

Lexington, KY

PWG F2F Meeting

Joe Murdock (Sharp)

Brian Smithson (Ricoh)

Agenda

09:00 – 09:15	Administrative Tasks
09:15 – 09:30	Review action items
09:30 – 09:45	Document status and Review
09:45 – 10:00	NEA and TCG Updates
10:00 – 10:30	Supporting Documents for Common Criteria Evaluation
10:30 – 10:45	Break
10:45 – 11:15	Supporting Documents for Common Criteria Evaluation (continued)
11:15 – 12:00	Identification and Authentication discussion
12:00 – 13:15	Lunch
13:15 – 14:00	Authorization Framework discussion
14:00 – 14:15	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, the Whiskey tour starts in 30 minutes…
- Approve Minutes from October 14 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 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?
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		Write an MPSA newsletter article for publication in November		Joe will work with Bill on articles, surveys, etc., to create and maintain a presence with MPSA. Planning to have something to review at the next F2F.
58	6/11/2010	Joe Murdock and Ira McDonald	SCCM	Create a first draft SCCM binding spec based on the NAP binding spec	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.
60	6/11/2010	Joe Murdock	auth	First draft of potential resource predicate values (objects, operations, etc.)	P	
63	8/6/2010	Bill Wagner	MPSA	Add the plan to a new section of the PWG wiki	P	Intro completed but no plan yet and not yet linked to the main page
64	9/30/2010	Joe Murdock		Outline an overview of IA&A		review at F2F

Document Status

- HCD-Assessment-Attributes
  ftp://ftp.pwg.org/pub/pwg/ids/wd/wd-idsattributes10-20100930.pdf
  - Stable (needs a binding prototype)
- HCD-NAP Binding
  ftp://ftp.pwg.org/pub/pwg/ids/wd/wd-ids-napsoh10-20100930.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-remediation10-20100930.pdf
  - Initial Draft
- HCD-NAP-SCCM Binding
  Mapping Spreadsheet:
  ftp://ftp.pwg.org/pub/pwg/ids/white/IDS-NAP-SCCM-Mapping_20090917.xls
  - Specification on hold
- 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
  ftp://ftp.pwg.org/pub/pwg/ids/white/Authorization-Framework-2010-10-15.xmind
  - 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
  Specification:
  ftp://ftp.pwg.org/pub/pwg/ids/wd/wd-ids-log10-20100803.pdf
  - Initial Draft
- HCD-Authentication
  mindMap:
  ftp://ftp.pwg.org/pub/pwg/ids/white/Cloud-and-Mobile-Authentication-2010-10-13.xmind
  - Specification under development

Document Review

- HCD-Remediation
  ftp://ftp.pwg.org/pub/pwg/ids/wd/wd-ids-standard-remediation10-20100930.pdf
- HCD-Log
  ftp://ftp.pwg.org/pub/pwg/ids/wd/wd-ids-log10-20100803.pdf

Reports/Discussions/Plans

- NEA Updates (Randy/Jerry)
- TCG Hardcopy Update (Ira/Brian)
- Supporting Documents for Common Criteria evaluation
- Authentication and Identification
- Authorization Framework for Hardcopy Devices

NEA Update

- NEA is not doing anything substantial

TCG Hardcopy WG - Status

- Unchanged since last meeting
  - 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)

Supporting Documents for Common Criteria Evaluation

- In 2009, the IEEE Std. 2600.1 protection profile was:
  - Published by the IEEE
  - Certified by NIAP at EAL3+ALC_FLR.2
  - Adopted by NIAP as the *US Government Protection Profile for Hardcopy Devices in Basic Robustness Environments*

- Two weeks later, NIAP changed their approach to PPs. They are:
  - Abandoning their "robustness" scale
  - Starting to make new PPs for all classes of products, some at EAL1 or EAL2
  - Refining or augmenting assurance requirements, tailored to each product class

- NIAP has been talking to the P2600 WG how to bring 2600.1 into line with the new approach (all other PPs are controlled by NIAP)
  - NIAP's first proposal was to downgrade 2600.1 to EAL2 and make it an "interim PP", awaiting rewrite
  - P2600 negotiated to leave it at EAL3 but start a PAR to rewrite it in the future
  - NIAP is now considering using IEEE 2600.2 (which is at EAL2) in some way, augmenting its SFRs so that they are consistent with those in 2600.1
  - It is unclear what would happen to 2600.1 or products evaluated outside the US
  - None of these approaches are satisfactory

Proposed new work area for IDS

- NIAP's real objective is for PP-conforming evaluations to be repeatable, consistent, and objective, across multiple labs and schemes, especially in ATE and AVA areas
- They like the SmartCard model for CC evaluations
  - Vendors, schemes, and customers collaborate to write PPs
  - Supporting Documents guide the evaluation process in ways that the CC language, SARs, and EAL packages, cannot

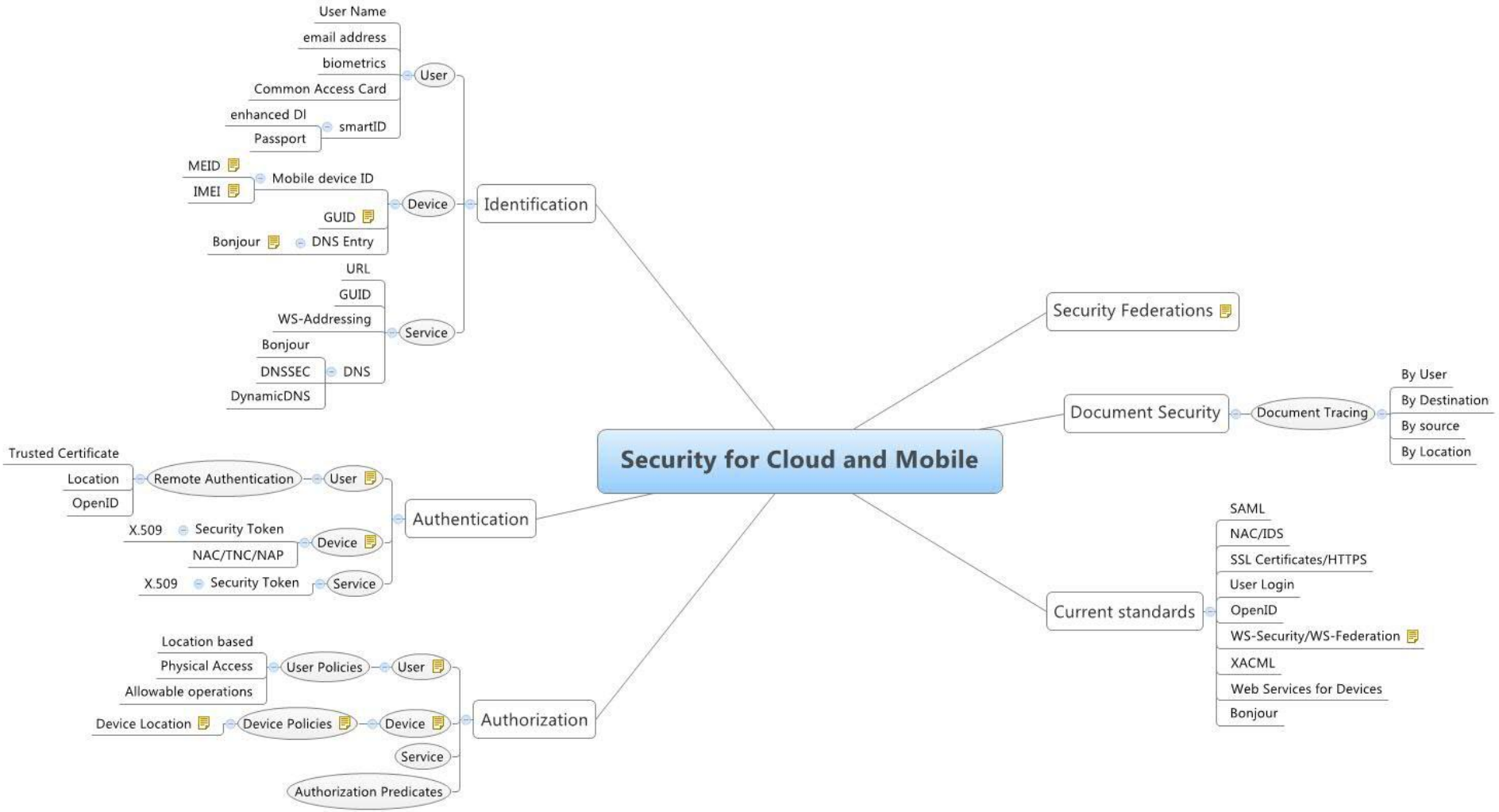
- We propose to create Supporting Documents within PWG-IDS
  - Fulfills NIAP's real objective, not the interim goal of EAL parity
  - Makes it possible to leave 2600.1 by justifying EAL3+ assurance
  - Might actually improve the repeatability, consistency, and objectivity of HCD evaluations

Outline of work to create SDs

- Form an interest group within IDS
  - Not all current participants may be interested
  - Others who do not currently participate are interested
  - A separate teleconference time may be needed due to different people and international participation
- Discuss what can be obtained from actual product evaluations
  - What has been the experience to date?
  - How to sanitize company-proprietary information?
  - Are there IP restrictions from the labs, and how to handle them?
- As product evaluations are completed, collect test experience, with focus on the generic attack part
- Also consider other sources, such as vulnerability reports and analyses
- Produce SDs in a year or so?

- Next step is to propose this to NIAP

Mobile, Cloud and Device Security



Identification and Authentication

- Mindmap file:
  - ftp://ftp.pwg.org/pub/pwg/ids/white/Cloud-and-Mobile-Authentication-2010-10-13.xmind
- Document Security
- Identification
- Authentication
- Authorization
- Security Federations
- Current standards

Identification

- User
  - User Name
  - email address
  - biometrics
  - Common Access Card
  - smartID
    - enhanced Dl
    - Passport

Identification

- Device
  - Mobile device ID
    - MEID - CDMA Mobile Equipment Identifier
    - IMEI - GSM International Mobile Equipment Identifier
  - GUID
    - WS Device Profile GUID
  - DNS Entry
    - Bonjour

Identification

- Service
  - URL
  - GUID
  - WS-Addressing
  - DNS
    - Bonjour
    - DNSSEC
    - DynamicDNS

Authentication

- User
  - Is the user who they say they are?
  - Trusted Certificate
  - OpenID
  - Location information?
- Device
  - Do we know this device?
  - Security Token
  - NAC/TNC/NAP
- Service
  - Is the Service to be trusted?
  - Security Token

Authorization

- User
  - Is the user allowed to do what they're trying to do?
  - User Policies
    - Location based
      - What is a remote user allowed to do?
    - Physical Access
    - Allowable operations
- Device
  - Is the requested operation allowed on this device?
  - Device Policies
    - Location based
      - Is any device from this location (i.e. country) allowed?
- Service
  - Is the service allowed to do work?
  - Service Policies

Document Security

- Document Tracing
  - By User
  - By Destination
  - By source
  - By Location

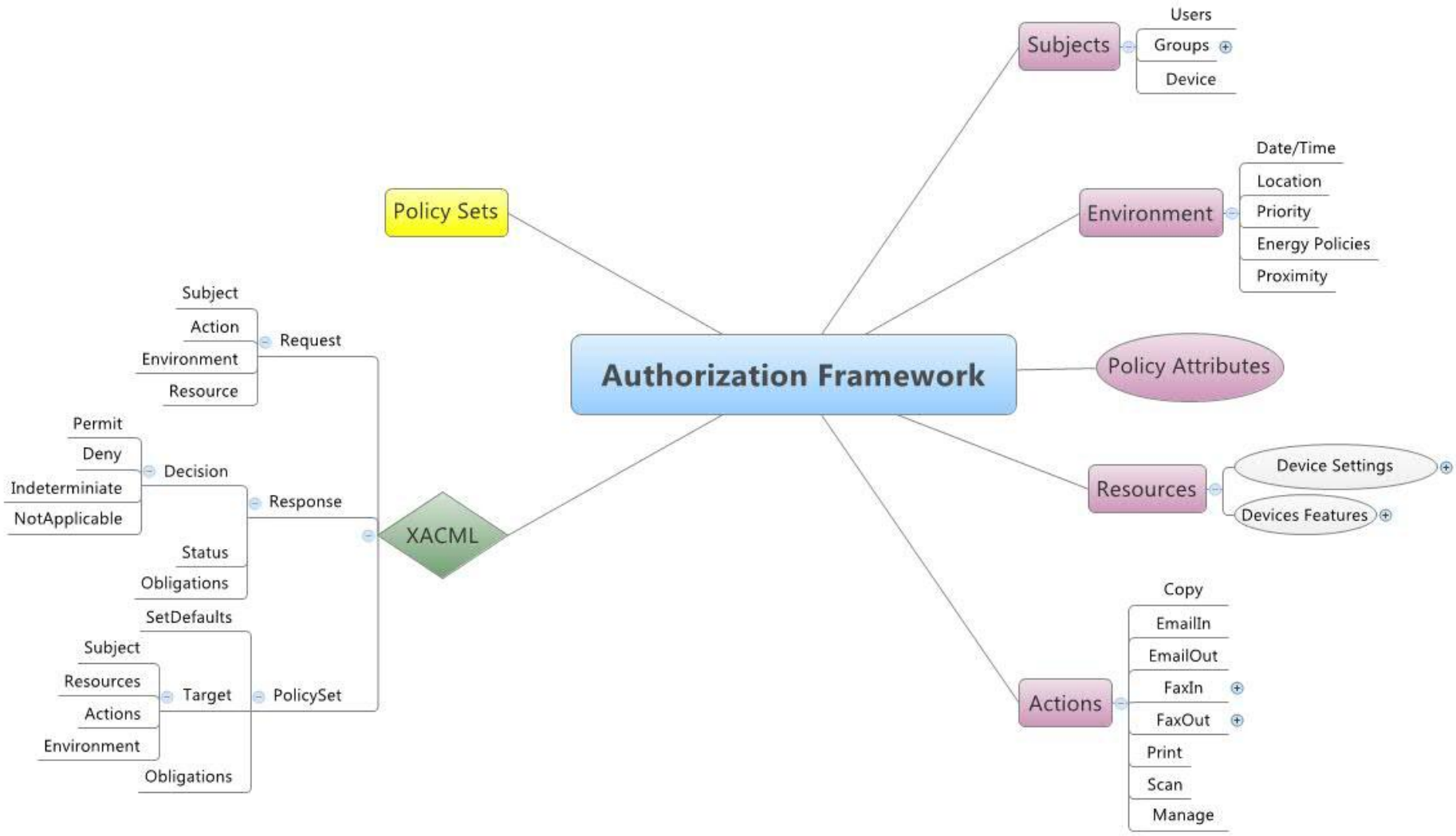
Security Federations

- If the service trusts the device, then it will trust a user vouched for by the device
- If the Service trusts the user, then it doesn't necessarily matter what device is being used
- Override by device policy
- Override by user device list

Current standards

- Identification
- User Login
- OpenID
- Web Services for Devices
- Bonjour
- WS-Security/WS-Federation
  - SAML
  - NAC/IDS
  - SSL Certificates/HTTPS
  - User Login
- Authentication
  - NAC/IDS
  - SSL Certificates/HTTPS

Authorization Framework



Authorization Framework

- Mind Map file:
  - ftp://ftp.pwg.org/pub/pwg/ids/white/Authorization-Framework-2010-10-15.xmind

Wrap up

- Review of new action items and open issues
- Conference call / F2F schedule
  - Next Conference call November 4, 2010
- Adjournment