Imaging Device Security WG Minutes
August 15, 2014

Meeting was called to order at approximately 9am ET August 15, 2014.

Attendees

Danny Brennan (IBM)
Daniel Dressler
Till Kamppeter (Canonical/OpenPrinting)
Shane Lin (Monotype)
Daniel Manchala (Xerox - call in)
Ira McDonald (High North - call in)
Johannes Meixner (SuSE)
Joe Murdock (Sharp)
Brian Smithson (Ricoh)
Alan Sukert (Xerox - call in)
Mike Sweet (Apple)
Bill Wagner (TIC)
Rick Yardumian (Canon)
Carmen Aubry (Canon - call in)

Agenda Items

1. IP Policy and Minute Taker
    a. Policy accepted with Mike taking the minutes
2. Slides
    a. Alan volunteered to also edit the IDS Model and IDS IAA specifications
3. Common Criteria
    a. http://ftp.pwg.org/pub/pwg/ids/Presentations/2014-08-15-MFPTC-F2F.pptx
    b. Current drafts and issues, which require (free) CCUF membership - contact Brian Smithson as needed to gain access:
        - MFP-PP draft v0.8.1.pdf has change marks showing what changed since draft, 0.7.1 (changes for both v0.8 and v0.8.1):
            - https://ccusersforum.onlyoffice.com/products/files/doceditor.aspx?fileid=3808614
        - MFP-PP draft v0.8.1 diffs with v0.8.pdf has change marks only what changed since draft 0.8:
            - https://ccusersforum.onlyoffice.com/products/files/doceditor.aspx?fileid=3808612
        - MFP-PP draft v0.8.1 clean.pdf has no change marks and may be a bit easier to read for that reason:
            - https://ccusersforum.onlyoffice.com/products/files/doceditor.aspx?fileid=3808613
        - Open issues list:

- https://ccusersforum.onlyoffice.com/products/projects/messages.aspx?prjID=239468#sortBy=comments&sortOrder=descending&text=[issue]
  - c. Q: Useful to review comments at an upcoming IDS meeting?
    - A: Yes, use the August 25, 2014 meeting to review CC comments.
    - Start an hour early
    - Also could do next week: August 18, 2014
4. Review IDS Model
   - a. http://ftp.pwg.org/pub/pwg/ids/wd/wd-ids-model10-20140804-rev.pdf
   - b. Section 2.2:
     - Line 347: "and" instead of "an"
     - Also say what the System Account is less restricted than
     - Directory Service: Drop "organization or enterprise"
   - c. Section 3.1:
     - Approve new format for rationale
     - Action: MIke to update WD template for new rationale format
     - Item 2: Add Clients, Services and Subscriptions
     - Item 3: Add Clients
     - Item 4: Add Clients and Subscriptions
     - Add RFC 3995 to list of specs (Subscriptions, with definition)
   - d. Section 3.3:
     - Add to out-of-scope: Authentication of network-connected devices
   - e. Section 4:
     - Line 467: Fix reference to IAA spec
   - f. Section 4.1:
     - Reword
   - g. Section 4.1.2:
     - Reword
   - h. Section 4.1.3:
     - Complete
   - i. Section 4.5.1:
     - Capitalize User in all definitions
     - Proxy: A client or process that is acting as an intermediary on behalf of a user or service
   - j. Section 4.5.4:
     - Authentication SERVICE
     - Add Key Distribution Service, Authorization Service, Identification Service
   - k. Section 4.5.5:
     - Device Type for Proxy (for identification): Embedded Device
   - l. Confusing to have so many different terms with different meanings (Client, Server, etc.)
   - m. Section 4.5.6:
     - Mode -> Model
     - System Control -> SystemControl
     - Scan (drop "a")

- Fix transform (digital in and out)
- Combine with 4.5.4, maybe add "Service" to each name
n. Section 5:
- Protocol Bindings
- "are not defined by this document"
o. Section 5.1:
- "has not been compromised"
p. Q: What do do about identification of recipient/destination/output device?
- A: Should add something to Job Receipt and Document Receipt
- Also PIN printing - attach recipient to Job and Document Receipts
- Also subscriptions:
- Log of all recipients
- Plus per event delivered
- Also services:
- Audit log of all IDs, failed auth, etc. (everything common log picks up)
q. Section 6:
- What to do about securing (encrypting) document data for Cloud Print?
- Need to be able to do secure key exchange through the Cloud
- Need to re-add supported/request security elements
- Need to re-add operation for proxies (NegotiateSecurityElements?)
- Drop Send/GetSecurityAlerts (notifications takes care of those)
- Action: Alan, Ira, Joe, and Mike to think about proxied secure key exchange
r. Section 11:
- "encrypted end-to-end data path such as provided using TLS encryption..."
- Q: What about Fax?
- A: Need some "weasel words" for things like POTS and other communication medium that is accepted as secure
- Action: Ira and Mike to work on Fax weasel words for IDS Model and IPP FaxOut
- Add "Encryption of data in memory but not in use"
- Add "Access Control/Isolation of data in memory", both between processes, threads, functional units
s. References: add RFC 3275 for XML digital signatures
5. Review IDS IAA
a. http://ftp.pwg.org/pub/pwg/ids/wd/wd-ids-iaa10-20140804.pdf
b. Section 3.1:
- Title: Abbreviate to "IDS"
- Sync up with Semantic Model and IDS Model
c. Section 3.2, 3.3:
- Reference IDS Model use cases.
d. Section 3.4:
- Sync up with IDS Model

e. Section 3.5:
- Sync up with IDS Model
f. Section 4.1.1:
- Drop "actual human"
g. Add Scope for Tokens (as a capability)
h. Rename Cert to Certificate
i. Add Certificate Authorities as a capability (supported)
j. Add RFC 6350 for VCard format, RFC 6351 for XML VCard
k. Section 6.1.1.10: Title [RFCnnnn]
l. Section 6.2.1:
- Add MacAddress
- Add NetworkIdentifier (such as Wi-Fi SSID) + maybe GatewayMacAddress?
- IPAddr->IpAddress, make IPAddress multi-valued
m. Section 6.3.1:
- Add ClientCertificate plus any other User elements that apply
n. Section 6.4.1:
- Add ServiceCertificate
- Say something about connection information (which address, etc.) is part of the Device information
- Drop Location info
o. Add notion of virtual or logical devices (nesting of physical and logical devices on physical device) for virtual hosting
p. Section 8: New boilerplate to copy from template
q. Change Nancy Chen's affiliation in Authors section
r. Action: Mike to post description of CUPS policy/ACL capabilities to IDS list

Next Steps / Open Actions

- Next MFP-PP conference calls August 18, 2014 and August 25, 2014 at 1pm ET for 2 hours to review CC comments.
- Next IDS conference call September 15, 2014 at 2pm ET
- Action: Mike to update WD template for new rationale format (no IDS #)
- Action: Alan, Ira, Joe, and Mike to think about proxied secure key exchange (#152)
- Action: Ira and Mike to work on Fax weasel words for IDS Model and IPP FaxOut (#153)
- Action: Mike to post description of CUPS policy/ACL capabilities to IDS list (#154)