The Printer Working Group

Imaging Device Security

October 23-24, 2013

Cupertino, CA

Introduction

- IDS is investigating and defining standards for addressing general security attributes for imaging devices and services. Our general goals are to:
  - Define standard metrics and protocol bindings to assess the health of Hardcopy Devices to gauge if they should be granted access to a network.
  - Define a set of standard security and policy attributes and values for authorizing Hard Copy Devices, their services and users in a global workspace
  - Provide a general security model for other PWG standards to reference
- IDS is also providing an anonymous path for vendors to review and contribute to the definition of new Common Criteria MFP Protection Profiles

Officers

- Chair:
  - Joe Murdock (Sharp Labs)
- Vice-Chair:
  - Alan Sukert (Xerox)
- Secretary:
  - Alan Sukert (Xerox)
- Document Editors:
  - Ira McDonald (High North): HCD-TNC
    IDS-Model
  - Joe Murdock (Sharp Labs): HCD-Remediation
    IDS-Model
    IDS-IAA

Agenda

When	What
October 23	
9:00 – 12:00	Introductions, Agenda review
	Document Review
October 24	
9:00 – 12:00	Common Criteria MFP Technical Committee

Status

Active Documents

- HCD-TNC Binding (Prototype)

  ftp://ftp.pwg.org/pub/pwg/ids/wd/wd-idstnc10-20130910-rev.pdf

- IDS-Model (Interim)

  ftp://ftp.pwg.org/pub/pwg/ids/wd/wd-ids-model10-20120806-rev.pdf

- IDS-IAA (Interim)

  ftp://ftp.pwg.org/pub/pwg/ids/wd/wd-ids-iaa10-20111005-rev.pdf

- IDS-Remediation (Interim)

  ftp://ftp.pwg.org/pub/pwg/ids/wd/wd-ids-remediation10-20100930.pdf

  `

Document Review

- Errata for 5110.1 (IDS Attributes)

  ftp://ftp.pwg.org/home/pwg/pub/pwg/ids/wd/wd-idsattributes10-20131015.pdf

  ftp://ftp.pwg.org/home/pwg/pub/pwg/ids/wd/wd-idsattributes10-20131015.doc

  ftp://ftp.pwg.org/home/pwg/pub/pwg/ids/wd/wd-idsattributes10-20131015-rev.pdf

- HCD-TNC Binding (Health Assessment)

  ftp://ftp.pwg.org/home/pwg/pub/pwg/ids/wd/wd-idstnc10-20130910.pdf

  ftp://ftp.pwg.org/home/pwg/pub/pwg/ids/wd/wd-idstnc10-20130910.docx

  ftp://ftp.pwg.org/home/pwg/pub/pwg/ids/wd/wd-idstnc10-20130910-rev.pdf

- IDS Model

  ftp://ftp.pwg.org/pub/pwg/ids/wd/wd-ids-model10-20131020.pdf

  ftp://ftp.pwg.org/pub/pwg/ids/wd/wd-ids-model10-20131020.docx

  ftp://ftp.pwg.org/pub/pwg/ids/wd/wd-ids-model10-20131020-rev.pdf

ITU-T X.Series Security Standards (1 of 2)

- http://www.itu.int/ITU-T/recommendations/index.aspx?ser=X
- ITU-T INFORMATION AND NETWORK SECURITY
  - General security aspects – X.1000–X.1029
  - Network security – X.1030–X.1049
  - Security management – X.1050–X.1069
  - Telebiometrics – X.1080–X.1099
- ITU-T SECURE APPLICATIONS AND SERVICES
  - Multicast security – X.1100–X.1109
  - Home network security – X.1110–X.1119
  - Mobile security – X.1120–X.1139
  - Web security – X.1140–X.1149
  - Security protocols – X.1150–X.1159
  - Peer-to-peer security – X.1160–X.1169
  - Networked ID security – X.1170–X.1179
  - IPTV security – X.1180–X.1199

ITU-T X.Series Security Standards (2 of 2)

- ITU-T CYBERSPACE SECURITY
  - Cybersecurity X.1200–X.1229
  - Countering spam X.1230–X.1249
  - **Identity management X.1250–X.1279**
- ITU-T SECURE APPLICATIONS AND SERVICES
  - Emergency communications X.1300–X.1309
  - Ubiquitous sensor network security X.1310–X.1339
- CYBERSECURITY INFORMATION EXCHANGE
  - Overview of cybersecurity X.1500–X.1519
  - Vulnerability/state exchange X.1520–X.1539
  - Event/incident/heuristics exchange X.1540–X.1549
  - Exchange of policies X.1550–X.1559
  - Heuristics and information request X.1560–X.1569
  - Identification and discovery X.1570–X.1579
  - Assured exchange X.1580–X.1589

ITU-T X.1254 Entity Authentication Assurance Framework (1 of 4)

- Scope – managing entity authentication assurance
  - Specifies four levels of entity authentication assurance
  - Specifies criteria and guidelines for achieving each of the four levels of entity authentication assurance
  - Provides guidance for mapping other authentication assurance schemes to the four LoAs;
  - Provides guidance for exchanging the results of authentication that are based on the four LoAs
  - Provides guidance concerning controls that should be used to mitigate authentication threats
- Terms
  - Assertion, Authentication, Claim, Context, Credential, Entity
  - Identity, Multifactor Authentication, Non-Repudiation
  - Identity Proofing, Mutual Authentication, Transaction
  - Trust Framework, Verification

ITU-T X.1254 Entity Authentication Assurance Framework (2 of 4)

- Levels of Assurance (LoAs)
  - 1 (Low) – little or no confidence in claimed or asserted identity
  - 2 (Medium) – some confidence in claimed or asserted identity
  - 3 (High) – high confidence in claimed or asserted identity
  - 4 (Very High) – very high confidence in claimed or asserted identity
- Actors
  - Entity – device, service, user, application, etc.
  - Credential Service Provider (CSP)
  - Registration Authority (RA)
  - Relying Party (RP)
  - Verifier
  - Trusted Third Party (TTP)

ITU-T X.1254 Entity Authentication Assurance Framework (3 of 4)

- Entity Authentication Assurance Framework Phases
  - Enrollment Phase
    – application and initiation (websites, badges, forms, etc.)
    – identity proofing and verification (entity identity attributes)
    – record-keeping (identity, verification, accept/deny/referral)
    – registration (during enrollment or later at first access)
  - Credential Management Phase
    – creation, binding to entity, issuance, activation
    – storage (secure handling, according to target LoA)
    – suspension, revocation, and/or destruction (CRLs, etc.)
    – renewal and/or replacement
    – record-keeping (creator, identity, entity, status)
  - Entity Authentication Phase
    – authentication (including LoA of each identity attribute)
    – record-keeping (service provision, compliance, accountability and/or legal requirements)

ITU-T X.1254 Entity Authentication Assurance Framework (4 of 4)

- Management and Organizational Considerations
  - Service establishment
  - Legal and contractual compliance
  - Financial provisions
  - Information security management and audit
  - External service components (i.e., third parties)
  - Operational infrastructure (i.e., trust frameworks)
  - Measuring operational apabilities
- Threats and Controls
  - Enrollment Phase – impersonation
  - Credential Management Phase – tampering, unauthorized creation, disclosure, unauthorized possession, unavailability, duplication, delayed revocation, repudiation
  - Authentication Phase – keystroke loggers, social engineering, guessing, duplication, phishing, eavesdropping, replay, session hijack, man-in-the-middle, theft, spoofing, masquerade

System Control Service Integration

- Discuss User/Group account access controls for PWG SM / IPP System Control Service
  - Updated tables in IDS-Model

ftp://ftp.pwg.org/pub/pwg/ids/wd/wd-ids-model10-20131020.pdf
ftp://ftp.pwg.org/pub/pwg/ids/wd/wd-ids-model10-20131020.docx
ftp://ftp.pwg.org/pub/pwg/ids/wd/wd-ids-model10-20131020-rev.pdf

Common Criteria

- Recap of the F2F meeting in Orlando
- Discussion of currently open issues and proposed resolutions
  https://ccusersforum.teamlab.com/products/projects/messages.aspx?prjID=239468#sortBy=comments&sortOrder=descending&text=[issue]
- Updates from NIAP and IPA (if any)
- Plans and schedules
- Open discussion

Future Activities

- Definition of core set of Policy Attributes
  - Addition to IAA specification
  - Harmonize with TCG TNC specifications
- Define access control values
- IDS model specification
- IDS health remediation
  - Integrate with TCG TNC Work Group

Wrap Up

- Review of new action items and open issues
- Conference call / F2F schedule
  - Next Conference Call December 2, 2013