Charter of the PWG Imaging Device Security (IDS) Working Group (WG)

Status: Initial Draft

ftp://ftp.pwg.org/pub/pwg/ids/wd/ch-ids-charter-20150122.pdf

IDS WG Chair:

Joe Murdock (Sharp)

IDS WG Vice-Chair:

Alan Sukert (Xerox)

IDS WG Secretary:

Alan Sukert (Xerox)

IDS WG Document Editors:

Joe Murdock (Sharp), Ira McDonald (High North), Alan Sukert (Xerox)

Problem Statement:

Modern Imaging and Hardcopy Devices[1] and Services may be allowed unrestrained access to and storage of secure and controlled documents and resources exposing security and access considerations that are not fully addressed within current standards.

- Imaging Devices provide and use services outside of the traditional concept of a local user or server on a physical device. While current standards such as the IEEE 2600-2008 are focused on addressing issues related to securing local Hardcopy Device functionality, there are currently no suitable Imaging Device standards or recommendation for controlling or validating access to these extended services.

- Imaging Devices provide services to Imaging Clients[2] running on various operating systems and can extend these services as Cloud[3] resources. Imaging Devices and Imaging Clients also use resources and Imaging

[1] IEEE 2600-2008 defines the term Hardcopy Device as: A system producing or utilizing a physical embodiment of an electronic document or image. These systems include printers, scanners, fax machines, digital copiers, MFPs (multifunction peripherals), MFDs (multifunction devices), "all-in-ones," and other similar products.
The definition of an Imaging Device includes that of a Hardcopy Device, but also may include hardware devices such as projectors or displays and software services or processes that perform imaging functionality such as Character Recognition or document format transformations.

Services from the Cloud. There are no suitable Imaging Device standards or recommended methodologies for authenticating and securing the Imaging Devices, Imaging Clients, and Imaging Services in a Cloud environment.

- Imaging Devices and Imaging Services have no standard method to associate security information with an Imaging Job and ensure that the security information is maintained throughout the Job lifetime.

- Enterprise networks are deploying network endpoint attachment and compliance protocols and tools to measure and assess the health of devices on the network. These assessment protocols go beyond simply checking that the device possesses the correct credentials to access the network to also monitoring and assessing information such as operating system, security patches, antivirus definition levels etc. Hardcopy Devices (Network Printers, Multi-Function Devices, Network Scanners, etc.) have not been widely integrated into these new assessment protocol schemes, in part because there is no standardized set of attributes that a health assessment server can measure for Hardcopy Devices.

The goal of the Imaging Device Security Working Group is to address these issues by developing the following specifications and recommendations:

- TNC Binding for IDS Health Attributes – Define health attributes transport using TNC.
- Remediation specification – Define standard methods to perform remediation of detected device health and security defects.
- IDS Model – Define a common security model for PWG projects and working groups.
- IDS Identification, Authentication and Authorization – Define a set of standards and recommendations for providing the credentials and information required to provide secure access to Imaging Devices, Services and Clients.
- IDS Security Ticket schema – Define a standard schema for specifying, associating and maintaining security information with an Imaging Job, Imaging Device or Imaging Client.
- Liaison with the Common Criteria MFP Technical Community for Protection Profile

Our goal is to provide the metrics and mechanisms that allow Imaging Devices to fully participate in assessment-protected networks and provide secure, controlled access to Jobs, Documents and Imaging Services.

Out-of-scope:

- OOS-1 Define new encryption algorithms
- OOS-2 Define new transport protocols
- OOS-3 Define new application protocols
- OOS-4 Define new hash functions or digital signatures
- OOS-5 Define new network endpoint attachment protocols
- OOS-6 Define new security protocols
- OOS-7 Define new security token, or public key certificate formats

Objectives:

- OBJ-1 Define an extended set of attributes for Imaging Devices that may include device configuration attributes to be used for policy enforcement
- OBJ-2 Define a TNC transport binding for health assessment.
- OBJ-3 Define a common Security Model specification for reference by other PWG specifications.

---

[2] Terms such as “Imaging Device” and “Imaging Service” used in this document are defined in the PWG MFD Model and Common Semantics document. The term “Imaging Client” is synonymous with the PWG Model term “Client”

[3] The term “Cloud” is defined in the NIST Special Publication 800-145 (http://csrc.nist.gov/publications/drafts/800-145/Draft-SP-800-145_cloud-definition.pdf)

- OBJ-4 Define a set of recommendations for identifying, authenticating and authorizing Imaging Devices, Imaging Client, and Imaging Services.
- OBJ-5 Define a schema for security attributes and a Security Ticket to be associated with Imaging Jobs, Users, Services and Devices

Milestones:

Charter Stage:

- CH-1 Initial working draft of updated IDS WG charter – Nov. 2014 - DONE
- CH-2 Interim/Stable working draft of IDS WG charter
- CH-3 PWG Formal Approval of original IDS WG charter
- CH-4 Interim/Stable working drafts of IDS WG charter for new security work
- CH-5 PWG Formal Approval of revised IDS WG charter revision

Definition Stage:

- BIND-1 Prototype Working draft of the TNC binding of the Hardcopy Device Health attributes - TBD
- BIND-2 PWG Last Call of the TNC binding of the Hardcopy Device Health attributes – TBD
- REM-1 Initial working draft of Remediation specification - DONE
- SEC-1 Initial working draft of IDS Security Ticket Schema model - DONE
- MODEL-1 Initial working draft of IDS Model specification – DONE
- IAA-1 Initial working draft of IDS Identification, Authentication and Authorization specification – DONE
- REM-2 Prototype working draft of Remediation specification – TBD
- SEC-2 Prototype working draft of IDS Security Ticket Schema model – Q2 2015
- MODEL-2 Prototype working draft of IDS Model specification – Q2 2015
- IAA-2 Prototype working draft of IDS Identification, Authentication and Authorization specification – Q2 2015
- REM-3 PWG Last Call of Remediation specification – TBD
- SEC-3 PWG Last Call of IDS Security Ticket Schema model – TBD
- MODEL-3 PWG Last Call of IDS Model specification – TBD
- IAA-3 PWG Last Call of IDS Identification, Authentication and Authorization specification - TBD

Implementation Stage:

- INTEROP-1 Interoperability testing of the TNC Health Assessment - TBD
- INTEROP-2 Interoperability testing of the IDS Security Ticket – TBD
- INTEROP-3 Interoperability testing of the Remediation specification - TBD