June 04, 2009

Working Draft

Style Definition: TOC 1: Space Before: 0 pt, After: 0 pt, Tabs: 6.99", Right,Leader: ...

Deleted: May

Deleted: 20

A Program of the IEEE-ISTO

The Printer Working Group

The Printer Working Group (PWG)

Hardcopy Device Health Assessment Attributes

Status: Prototype

Abstract: This standard defines a set of attributes for Hardcopy Devices (HCD)s that may be used in the various network health assessment protocols to measure the fitness of a HCD to attach to the network.

This document is a PWG Candidate Standard. For a definition of a "PWG Candidate Standard", see: ftp://ftp.pwg.org/pub/pwg/general/pwg-process30.pdf

This document is available electronically at:
ftp://ftp.pwg.org/pub/pwg/ids/wd/wd-idsattributes10-20090520.pdf, .doc

Deleted: May

Deleted: 20

Title: *Hardcopy Device Health Assessment Attributes*

The IEEE-ISTO and the Printer Working Group DISCLAIM ANY AND ALL WARRANTIES, WHETHER EXPRESS OR IMPLIED INCLUDING (WITHOUT LIMITATION) ANY IMPLIED WARRANTIES OF MERCHANTABILITY OR FITNESS FOR A PARTICULAR PURPOSE.

The Printer Working Group, a program of the IEEE-ISTO, reserves the right to make changes to the document without further notice. The document may be updated, replaced, or made obsolete by other documents at any time.

The IEEE-ISTO and the Printer Working Group, a program of the IEEE-ISTO take no position regarding the validity or scope of any intellectual property or other rights that might be claimed to pertain to the implementation or use of the technology described in this document or the extent to which any license under such rights might or might not be available; neither does it represent that it has made any effort to identify any such rights.

The IEEE-ISTO and the Printer Working Group, a program of the IEEE-ISTO invite any interested party to bring to its attention any copyrights, patents, or patent applications, or other proprietary rights, which may cover technology that may be required to implement the contents of this document. The IEEE-ISTO and its programs shall not be responsible for identifying patents for which a license may be required by a document and/or IEEE-ISTO Industry Group Standard or for conducting inquiries into the legal validity or scope of those patents that are brought to its attention. Inquiries may be submitted to the IEEE-ISTO by e-mail at:

info@ieee-isto.org

The Printer Working Group acknowledges that the IEEE-ISTO (acting itself or through its designees) is, and shall at all times, be the sole entity that may authorize the use of certification marks, trademarks, or other special designations to indicate compliance with these materials.

Use of this document is wholly voluntary. The existence of this document does not imply that there are no other ways to produce, test, measure, purchase, market, or provide other goods and services related to its scope.

About the IEEE-ISTO
The IEEE-ISTO is a not-for-profit corporation offering industry groups an innovative and flexible operational forum and support services. The IEEE-ISTO provides a forum not only to develop standards, but also to facilitate activities that support the implementation and acceptance of standards in the marketplace. The organization is affiliated with the IEEE (http://www.ieee.org/) and the IEEE Standards Association (http://standards.ieee.org/).

For additional information regarding the IEEE-ISTO and its industry programs visit http://www.ieee-isto.org.

About the IEEE-ISTO PWG
The Printer Working Group (or PWG) is a Program of the IEEE Industry Standards and Technology Organization (ISTO) with member organizations including printer manufacturers, print server developers, operating system providers, network operating systems providers, network connectivity vendors, and print management application developers. The group is chartered to make printers and the applications and operating systems supporting them work together better. All references to the PWG in this document implicitly mean “The Printer Working Group, a Program of the IEEE ISTO.” In order to meet this objective, the PWG will document the results of their work as open standards that define print related protocols, interfaces, procedures, and conventions. Printer manufacturers and vendors of printer related software will benefit from the interoperability provided by voluntary conformance to these standards.

In general, a PWG standard is a specification that is stable, well understood, and is technically competent, has multiple, independent and interoperable implementations with substantial operational experience, and enjoys significant public support.

For additional information regarding the Printer Working Group visit: http://www.pwg.org

Contact information:

The Printer Working Group
c/o The IEEE Industry Standards and Technology Organization
445 Hoes Lane
Piscataway, NJ 08854
USA

IDS Web Page:

http://www.pwg.org/ids

IDS Mailing List:

ids@pwg.org

Instructions for subscribing to the IDS mailing list can be found at the following link:

http://www.pwg.org/mailhelp.html

Those interested in this specification are encouraged to join the IDS Mailing List and to participate in any discussions clarifications or review of this specification. Not that, to reduce spam, the mailing list rejects mail from non-subscriber; you must subscribe to the mailing list to be able to send a question or comment to the mailing list.

Table of Contents

Deleted: May

Deleted: 20

Deleted:

Deleted: May

Deleted: 20

1. Introduction

Many corporate network and security administrators are beginning to deploy various security policy enforcement mechanisms that measure the “health” of a networked device being attached to the network infrastructure in addition to merely authenticating the user or device. The goal of these health assessment mechanisms is to provide a level of assurance that the device being granted access to network resources will do no harm to the network or other networked devices. For PCs, servers, etc.; these health assessment schemes allow the administrator to access the state of the device’s operating system, anti-virus program, personal firewall, and other attributes of the device to ensure that they are in compliance with the security policy for the network.

Deleted: condition

Currently, Hardcopy Devices do not participate in any of these protocols and are allowed to bypass health assessment when attaching to the network. In many health assessment schemes, this is merely the entry of the device’s MAC or IP address into an exception table. This, however, results in vulnerability in the network assessment scheme as it is fairly simple for the MAC or IP address of the excepted HCD to be spoofed by another device that would normally be subject to the health assessment.

Deleted: and other imbedded devices such as IP phones

Deleted: a vulnerability

Deleted: May

Deleted: 20

2. Terminology

This section defines terminology used throughout this document.

2.1 Conformance Terminology

Capitalized terms, such as **MUST, MUST NOT, REQUIRED, SHOULD, SHOULD NOT, MAY,** and **OPTIONAL**, have special meaning relating to conformance as defined in RFC 2119 [rfc2119].

2.2 Other Terminology

In addition, the following terms are imported or generalized from other source documents:

Hardcopy Device (HCD) – A system producing or utilizing a physical embodiment of an electronic document or image. These systems include printers, scanners, fax machines, digital copiers, multifunction peripherals (MFPs), multifunction devices (MFDs), all-in-ones, and other similar products. [IEEE2600]

Administrator – A user who has been specifically granted the authority to manage some portion or all of the HCD. Administrators may possess special privileges that provide capabilities to override portions of the security policy. [IEEE2600]

Comment [gwp1]: I do not understand how a Admin affect the policy. The policy is what the policy is. The Admin can enforce the policy. The Admin can make an exception to the policy (by his actions).

Deleted: and whose actions may affect the security policy

Application – An Application is computer instructions and data placed on the HCD, via download or additional hardware that are separate from, and not a part of, the base configuration. Applications are an addition to the base configuration that provide additional function beyond that provided by the base configuration.

Comment [gwp2]: This could be a chip, etc.

Deleted: Persistent

Deleted: (daughter card)

Deleted: Firmware

Deleted: Firmware

Deleted: Firmware

Deleted: ¶

Device administrator – A user who controls administrative operations of the HCD other than its network configuration (e.g., management of users and resources of the HCD). [IEEE2600]

Deleted: ¶

Firmware – Firmware is persistent computer instructions and data embedded in the HCD that provides the operational functions of that device. Firmware is only replaced during a specialized update process. [IEEE2600]

Deleted: P

Deleted: basic

Network administrator – A user who manages the network configuration of the HCD. [IEEE2600]

Resident Application - Resident applications are those applications that are downloaded via an offline administrative or maintenance update procedure and persist after a power cycle of the HCD. These types of applications augment the normal operation of the HCD and provide additional functions that are available to all users of the HCD.

User – An entity (human user or IT entity) outside the HCD that interacts with the HCD. [IEEE2600]

User Application - User applications are applications that are downloaded and executed as part of normal operation of the HCD and may be dynamically installed and executed by users. These applications do not include applications that are added via an offline administrative or maintenance update procedure. Examples of these types of applications include Java or Flash applications. User applications may or may not persist after a power cycle of the HCD.

Deleted: ¶

Formatted: Bullets and Numbering

2.3 Acronyms

DHCP – Dynamic Host Configuration Protocol

DNS – Domain Name System

FTP – File Transfer Protocol

HCD – Hardcopy Device

Deleted: May

Deleted: 20

HTTP – HyperText Transfer Protocol

Formatted: Font: Bold

HTTPS – HyperText Transfer Protocol Secure

Formatted: Font: Bold

IANA – Internet Assigned Numbers Authority

Formatted: Font: Bold

Deleted: **ISMS** – Information Security Management System¶

IETF – Internet Engineering Task Force

Formatted: Font: Bold

IP – Internet Protocol

IT – Information Technology

Formatted: Font: Bold

IPP – Internet Print Protocol

Formatted: Font: Bold

ISMS – Information Security Management System

LAA – Locally Administered Address

LDAP – Lightweight Directory Access Protocol

MAC – Media Access Control

NTP – Network Time Protocol

PA-TNC – Posture Attribute – Trusted Network Connect

Formatted: Font: Not Bold

PC – Personal Computer

Formatted: Font: Not Bold

PSTN – Public Switched Telephone Network

PWG – Printer Working Group

Formatted: Font: Bold

RTC – Real Time Clock

SMI – Structure of Management Information

SSL – Secure Socket Layer

Formatted: Font: Bold

TLS – Transport Layer Security

Formatted: Font: Bold

U – Unsigned

Formatted: Font: Bold

UAA – Universally Administered Address

URL – Universal Resource Locator

USB – Universal Serial Bus

UTF - Unicode Transformation Format

Formatted: Font: Bold

3. Requirements

3.1 Rationale for HCD Health Assessment Attributes

Hardcopy Devices generally do not include the same software infrastructure and patch management mechanisms as a PC or server, and don't currently include anti-virus programs or host-based firewalls. However there are attributes of a HCD that can be defined that can be used to gauge an HCD's compliance with a security policy.

3.2 Use Cases for HCD Health Assessment Attributes

3.2.1 Managed IT Environment using Health Assessment Protocols for Desktops and Laptops

A corporate IT department has decided to implement a network health assessment infrastructure as part of a rollout of laptop and desktop refresh for the company's employees. The motivation behind the decision to implement an assessment protocol was driven by the increasing number of laptops used by employees that were used away from the office on unmanaged networks and only occasionally attached to the corporate network. These laptops could not automatically have their security patches, antivirus definitions etc. updated since they were not on the network when the administrator's system management software executed batch updates.

Because Hardcopy Devices do not support the network health assessment protocols, the IP address of each HCD is manually entered into an exception table with the health assessment scheme's configuration tool. Industrious employees have discovered that they can program their laptops with the same IP address as the area's shared printer and access the corporate network without having to manually install operating system patches and antivirus updates before being allowed access. Having HCDs report attributes will remove the need for most exceptions and therefore decrease the chance of unprotected laptops spreading malware.

3.2.2 IT Environment that requires Common Criteria certification for networked devices

IT Security and Network administrators that follow specific Information Security Management System (ISMS) guidelines may require that ALL devices that attach to a network be certified via some external body, (e.g., Common Criteria). These certifications are usually only valid if the device is maintained in a particular configuration. For Hardcopy Devices, configuration parameters that may affect the status of a certification can include, but are not limited to:

- The specific level of firmware that is loaded into the HCD.
- The specific hardware ports that are enabled or disabled on the HCD.
- The specific network protocols that are enabled or disabled on the HCD.
- The specific port numbers that are enabled or disabled on the HCD.
- The specific services that are enabled on the HCD.

Any modification to these configuration parameters can result in the device no longer operating in its certified configuration.

3.2.3 IT Environment that requires Policy Enforcement Certification for networked devices

Organizations may have a set of internal policies that must be satisfied before a device is allowed on the network. Often these policy requirements are configuration requirements and may not seem directly related to "health." However, from the following example, it may be seen that configuration settings may be important elements for assessing the fitness of a device to attach to the network.

Users have discovered that they can gain access to the network by acquiring the address of a device on the exception list and statically assigning this IP address to their computer. Their computer is now on the exception list and is granted access. To mitigate this breach, IT administrators decide corporate policy is that ALL devices must acquire their IP addresses from a DHCP server. The configuration setting that enables/disables DHCP becomes part of the Policy Enforcement health assessment.

Policy Enforcement can encompass a wide range of configuration settings. The relevance of these settings may also vary between organizations. Some additional configuration elements that could be part of a policy statement include, but are not limited to:

- Secure Time Source
- Valid X.509 certificate signed by corporate Certificate Authority
- MAC addresses – Universally Administered Address (UAA) versus Locally Administrated Address (LAA)
- Enabled/Disabled protocols -- for example, no FTP daemon, or support for HTTPS but not for HTTP.
- Installed features – for example, disallow printers with hard disks unless they support disk wiping.
- Authentication settings – Kerberos/LDAP configuration
- Network proxy configuration
- DNS server address(es)

It is also important to note that some policy related settings, like disabled protocols and installed features, may overlap with other health related evaluations.

3.3 Design Requirements for Attributes

1) The PWG HCD Health Assessment Attribute design MUST NOT depend on the implementation of any specific network health assessment protocol.
2) The PWG HCD Health Assessment Attribute design MUST support mappings to multiple network health assessment protocols.
3) The PWG HCD Health Assessment Attributes design SHOULD be vendor extensible.

4. HCD Health Assessment Attributes

This section contains the definitions of the Health Assessment Attributes for Hardcopy Devices.

4.1 General Attribute Definitions

These attributes in the following table are the base set of attributes for HCDs that can be used to identify and measure the health of the HCD. The binding of these attributes into specific health assessment protocols is specified in other Printer Working Group documents.

HCD Health Assessment Attribute Name	(DataType)
Description	
HCD_Certification_State	(octet-array)
The HCD_Certification_State attribute is a vendor-specific variable length field that uniquely identifies the state of a particular set of configuration settings in the HCD that are included as part of a certification process (e.g., Common Criteria certification).	
HCD_Configuration_State	(octet-array)
The HCD_Configuration_State attribute is an administratively configured, vendor-specific variable length field that uniquely identifies the state of any configuration settings in the HCD that are included in creation of the attribute.	
HCD_Default_Password_Enabled	(boolean)
The HCD_Default_Password_Enabled attribute is a single bit-field that indicates that one or more of the devices' administrator passwords or other credentials are set to the factory defaults. (0 = no default passwords)	
HCD_Firewall_Setting	(octet-array)
The HCD_Firewall_Setting attribute is a variable length field that indicates the state (open/closed) of each IP protocol port on the device.	
HCD_Firmware_Name	(UTF-8 string)
The HCD_Firmware_Name attribute is a variable length string that specifies the name attributed to the firmware that is contained in the HCD.	
HCD_Firmware_Patches	(UTF-8 string)
The HCD_Firmware_Patches attribute is a variable length string that describes the patch(s) that have been applied to the firmware in the HCD. Note: Any firmware patches applied to the HCD MUST result in a change in the HCD_Firmware_Version attribute.	
HCD_Firmware_String_Version	(UTF-8 string)
The HCD_Firmware_String_Version attribute is variable length string that can uniquely describe the current version of firmware loaded in the device.	
HCD_Firmware_Version	(octet-array)
The HCD_Firmware_Version attribute is a 16 octet field that can uniquely describe the current version of firmware loaded in the device.	
HCD_Forwarding_Enabled	(boolean)
The HCD_Forwarding_Enabled attribute is a single bit-field that indicates whether any external-facing interface is being used as a bridge, route, or proxy from any other external-facing interface including itself.	

Deleted: May

Deleted: 20

Deleted: ¶

Formatted: Bullets and Numbering

Formatted Table

Deleted: A change to any configuration setting that is required for the device to maintain its certification status MUST cause a change, within the limits of information theory, in the attribute. Note: An example implementation of this attribute could be a cryptographically secure hash of the configuration (e.g., firmware version, port filter settings, protocols enabled/disabled etc.) that must be set to a specific state as part of the certification process.

Deleted: A change to any configuration setting that is included in the creation of the attribute MUST cause a change, within the limits of information theory, in the attributes value. The configuration settings included as part of this attribute SHOULD be administratively configurable. Note: An example implementation of this attribute could be a cryptographically secure hash of the configuration settings.¶
¶
Implementer Note:¶
The HCD_Configuration_State attribute is intended to provide a method for a system administrator (site local, device, etc.) to snap-shot a specific device configuration state. Examples of configuration information included in this attribute may include such items as default settings for duplex, media type, color mode, language, etc.; enabled or disabled services or features such as Fax, IPP, SSL support etc.; and encryption parameters for storage or network transports. In conjunction with a system health validation agent, this value can be used to determine if the configuration has changed in any way from the last snap-shot. No standardized values or behavior is defined by the PWG, only the ability to detect a change. Any access control restrictions that may be triggered by a change in this attribute are vendor or administrator define ... [1]

Deleted: Note: An example binding of this attribute follows the format for the Port Filter attribute type in [PA-TNC] section 4.2.6.

Deleted: Note: An example binding of this attribute may follow the format for the Numeric Version in [PA-TNC] section 4.2.3.

Deleted: (0 = no forwarding enabled) Note: An example of this may be a USB, Infrared, 802.11, Bluetooth, or PSTN Fax interface being bridged to the Ethernet interface allowing devices that have not been subject to the health assessm ... [2]

HCD Health Assessment Attribute Name	(DataType)	Description
HCD_Machine_Type_Model	(UTF-8 string)	The HCD_Machine_Type_Model attribute is a variable length string that indicates the particular machine type and model of the device. This attribute is generally common to all devices in a particular generation of that device. Example: "SomeCompany PhotoSmart 500"
HCD_PSTN_Fax_Enabled	(boolean)	The HCD_PSTN_Fax_Enabled attribute is a single bit-field that indicates if the PSTN fax interface or other modem interface on the device is enabled.
HCD_Resident_Application_Name	(UTF-8 string)	The HCD_Resident_Application_Name attribute is a variable length string that specifies the name attributed to a resident application that is currently installed on the HCD.
HCD_Resident_Application_Patches	(UTF-8 string)	The HCD_Resident_Application_Patches attribute is a variable length string that describes the patch(s) that have been applied to a resident application in the HCD.
HCD_Resident_Application_String_Version	(UTF-8 string)	The HCD_Resident_Application_String_Version attribute is variable length string that can uniquely describe the current version of an installed resident application in the device.
HCD_Resident_Application_Version	(octet-array)	The HCD_Resident_Application_Version attribute is a 16 octet field that can uniquely describe the current version of an installed resident application in the device.
HCD_Time_Source	(UTF-8 string)	The HCD_Time_Source attribute is a variable length string that indicates where the device acquires its time setting. Regardless of the time source, the HCD shall provide administrative protection for its internal time.
HCD_User_Application_Enabled	(boolean)	The HCD_User_Application_Enabled attribute is a single bit-field that indicates whether the HCD supports (or currently has enabled) the ability to download or execute applications intended to dynamically downloaded by users and executed on the device.
HCD_User_Application_Persistence_Enabled	(boolean)	The HCD_User_Application_Persistence_Enabled attribute is a single bit-field that indicates whether user-downloadable applications can persist outside the boundary of a single job.
HCD_User_Application_Name	(UTF-8 string)	The HCD_User_Application_Name attribute is a variable length string that specifies the name attributed to a dynamic user-downloadable and executable application that is currently installed on the HCD.
HCD_User_Application_Patches	(UTF-8 string)	The HCD_User_Application_Patches attribute is a variable length string that describes the patch(s) that have been applied to a user-downloadable application in the HCD.
HCD_User_Application_String_Version	(UTF-8 string)	The HCD_User_Application_String_Version attribute is variable length string that can uniquely describe the current version of an installed user-downloadable application in the device.

Deleted: May

Deleted: 20

Deleted: (1 = Fax enabled)

Deleted: Note: Any application patches applied to the HCD MUST result in a change in the HCD_Resident_Application_Version attribute.

Deleted: Note: An example binding of this attribute may follow the format for the Numeric Version in [PA-TNC] section 4.2.3.

Deleted: Examples of this attribute include: ("onboard" for a resident RTC or a Hostname or URL string for a network time source)¶
¶
Usage Considerations: Many security mechanisms rely on accurate time to enforce security. Examples include validity periods on X.509 certificates and Kerberos Tickets. As such, it is important to know that the device's internal clock(s) acquire time in a secure manner. If the time source is not secure, it could lead to denial of service (set time outside the validity period) and/or allow unauthorized access (set time to within validity period.) There are several ways to acquire the time including Network Time Protocol (NTP) and explicitly set by the user via some user interface. NTP has the ability to utilize encryption and integrity checks using pre-shared keys. The user interface to the clock can be protected using passwords. It is important to note that internal time of day clocks are often used in devices and may utilize a bus structure, such as I2C. In such cases, the bus used MUST NOT be accessible externally from the device.

Deleted: (0 = not enabled)

Deleted: (0 = not enabled)

Deleted: Note: Since these applications are dynamic, a re-assessment of the device may be required after each download.

Deleted: Note: Any user-downloadable application patches applied to the HCD MUST result in a change in the HCD_User_Application_Version attribute.

Deleted: May

Deleted: 20

HCD Health Assessment Attribute Name	(DataType)
Description	
HCD_User_Application_Version	(octet-array)
The HCD_User_Application_Version attribute is a 16 octet field that can uniquely describe the current version of an installed user-downloadable application in the device.	
HCD_Vendor_Name	(UTF-8 string)
The HCD_Vendor_Name attribute is a variable length string that indicates the name of the manufacturer of the HCD.	
HCD_Vendor_SMI_Code	(u-integer)
The Vendor_SMI_Code is a 24 bit unsigned integer that contains a globally unique SMI Network Management Private Enterprise Code of the vendor, as defined by IANA.	

Deleted: Note: An example binding of this attribute may follow the format for the Numeric Version in [PA-TNC] section 4.2.3.

Formatted: IEEEStds Paragraph

Formatted: IEEEStds Level 1

5. Conformance

Conformance: Any binding that supports the attributes defined in the table in section 4.1 MUST support multiple instances of the Name, Version, and Patch attributes related to user and resident applications.

5.1 andatory Attributes

HCDs that claim conformance to this specification MUST support the following set of attributes:

- HCD_Default_Password_Enabled
  - o The value of zero (0) SHALL imply "no default password". (0 = no default password)
- HCD_Firewall_Setting
  - o An example binding of this attribute follows the format for the Port Filter attribute type in [PA-TNC] section 4.2.6.
- HCD_Firmware_Name
- HCD_Firmware_Patches
  - o Any firmware patches applied to the HCD MUST result in a change in the HCD_Firmware_Version attribute.
- HCD_Firmware_String_Version
- HCD_Firmware_Version
  - o An example binding of this attribute may follow the format for the Numeric Version in [PA-TNC] section 4.2.3.
- HCD_Forwarding_Enabled
  - o The value of zero (0) SHALL imply "no forwarding enabled". (0 = no forwarding enabled)
  - o An example of this may be a USB, Infrared, 802.11, Bluetooth, or PSTN Fax interface being bridged to the Ethernet interface allowing devices that have not been subject to the health assessment measurement to access the Ethernet network.
- HCD_Machine_Type_Model
- HCD_User_Application_Enabled
  - o The value of zero (0) SHALL imply "user applications not enabled". (0 = not enabled)
- HCD_User_Application_Persistence_Enabled
  - o The value of zero (0) SHALL imply "user applications persistence not enabled". (0 = not enabled)
- HCD_Vendor_Name
- HCD_Vendor_SMI_Code

5.2 Conditionally Mandatory Attributes

HCDs MUST support the attributes in this section when the particular capability is implemented on the HCD.

5.2.1 User Application Attributes

The following attributes MUST be supported when the HCD supports user-downloadable applications.

- HCD_User_Application_Name
  - o Since these applications are dynamic, a re-assessment of the device may be required after each download.
- HCD_User_Application_Patches
  - o Any user-downloadable application patches applied to the HCD MUST result in a change in the HCD_User_Application_Version attribute.
- HCD_User_Application_String_Version
- HCDUser_Application_Version
  - o An example binding of this attribute may follow the format for the Numeric Version in [PA-TNC] section 4.2.3.

Deleted: May

Deleted: 20

Deleted: <#>¶
<#>Conformance: Any binding that supports the attributes defined in this table MUST support multiple instances of the Name, Version, and Patch attributes related to user and resident applications.
Page Break
¶
<#>Section Break (Continuous)
<#>Conformance¶

Formatted: IEEEStds Paragraph

Deleted: M

Formatted: Left

Formatted: Bullets and Numbering

Formatted: Bullets and Numbering

Formatted: Bullets and Numbering

Formatted: Bullets and Numbering

Formatted: Bullets and Numbering

Formatted: Bullets and Numbering

Formatted: Bullets and Numbering

Deleted: ¶

Formatted: Bullets and Numbering

Deleted: if

Deleted: , as described before each attribute,

Deleted: if

Formatted: Left

Formatted: Bullets and Numbering

Formatted: Bullets and Numbering

Formatted: Bullets and Numbering

Deleted: May

Deleted: 20

5.2.2 Resident Application Attributes

The following attributes MUST be supported when the HCD supports the addition of resident applications to the HCD's operating software.

Deleted: if

- HCD_Resident_Application_Name
- HCD_Resident_Application_Patches
  - Any application patches applied to the HCD MUST result in a change in the HCD_Resident_Application_Version attribute.
- HCD_Resident_Application_String_Version
- HCD_Resident_Application_Version
  - An example binding of this attribute may follow the format for the Numeric Version in [PA-TNC] section 4.2.3.

Formatted: Left

Formatted: Bullets and Numbering

Formatted: Bullets and Numbering

5.2.3 Other Conditionally Mandatory Attributes

The attributes in the following table MUST be supported if the condition described after each attribute is present in the HCD.

Attribute	Condition
HCD_PSTN_Fax_Enabled	MUST be supported when the HCD implements a PSTN Fax interface. o The value of one (1) SHALL imply "Fax is enabled". (1 = Fax enabled)
HCD_Time_Source	MUST be supported when the HCD implements any protocol or feature that requires a time source. o Examples of this attribute include: ("onboard" for a resident RTC or a Hostname or URL string for a network time source) o ***Usage Considerations:*** Many security mechanisms rely on accurate time to enforce security. Examples include validity periods on X.509 certificates and Kerberos Tickets. As such, it is important to know that the device's internal clock(s) acquire time in a secure manner. If the time source is not secure, it could lead to denial of service (set time outside the validity period) and/or allow unauthorized access (set time to within validity period.) There are several ways to acquire the time including Network Time Protocol (NTP) and explicitly set by the user via some user interface. NTP has the ability to utilize encryption and integrity checks using pre-shared keys. The user interface to the clock can be protected using passwords. It is important to note that internal time of day clocks are often used in devices and may utilize a bus structure, such as I2C. In such cases, the bus used MUST NOT be accessible externally from the device.

Formatted: Left

Formatted Table

Formatted: Left

Deleted: if

Formatted: Left, Indent: Left: -0.01", Hanging: 0.13", Tabs: Not at 1"

Formatted: Bullets and Numbering

Formatted: Left

Formatted: Left

Deleted: if

Formatted: Left, Indent: Left: -0.01", Hanging: 0.13", Bulleted + Level: 2 + Aligned at: 0.75" + Tab after: 1" + Indent at: 1", Tabs: Not at 1"

Formatted: Left

Formatted: Font: Bold, Italic

Formatted: Indent: Left: -0.01", Hanging: 0.13", Bulleted + Level: 2 + Aligned at: 0.75" + Tab after: 1" + Indent at: 1", Tabs: Not at 1"

Deleted: May

Deleted: 20

Deleted: Section Break (Continuous)

Formatted: Bullets and Numbering

5.3 Optional Attributes

Support for the following attributes is OPTIONAL for an HCD.

- HCD_Configuration_State
  - A change to any configuration setting that is included in the creation of the attribute MUST cause a change, within the limits of information theory, in the attributes value.
  - The configuration settings included as part of this attribute SHOULD be administratively configurable.
  - An example implementation of this attribute could be a cryptographically secure hash of the configuration settings.
  - ***Implementer Note:*** The HCD_Configuration_State attribute is intended to provide a method for a system administrator (site local, device, etc.) to snap-shot a specific device configuration state. Examples of configuration information included in this attribute may include such items as default settings for duplex, media type, color mode, language, etc.; enabled or disabled services or features such as Fax, IPP, SSL support etc.; and encryption parameters for storage or network transports. In conjunction with a system health validation agent, this value can be used to determine if the configuration has changed in any way from the last snap-shot. No standardized values or behavior is defined by the PWG, only the ability to detect a change. Any access control restrictions that may be triggered by a change in this attribute are vendor or administrator defined. While a specific vendor may wish to provide mediation support for this attribute, no remediation support is defined or required by this standard.
- HCD_Certification_State
  - A change to any configuration setting that is required for the device to maintain its certification status MUST cause a change, within the limits of information theory, in the attribute.
  - An example implementation of this attribute could be a cryptographically secure hash of the configuration (e.g., firmware version, port filter settings, protocols enabled/disabled etc.) that must be set to a specific state as part of the certification process.

Formatted: Bullets and Numbering

Formatted: Font: Not Italic

Formatted: Bullets and Numbering

6. Internationalization Considerations

The attributes that are defined in this specification are intended to be used as part of a network assessment protocol and conform to the IETF Policy on Character Sets and Languages [RFC2277] in that all string attributes are UTF-8 encoded.

7. Security Considerations

This specification does not define any specific security mechanism for the protection of the confidentiality and integrity of the attributes, however, assessment protocols that use these attributes SHOULD provide integrity protection and confidentiality of the attributes.

8. Normative References

None.

9. Informative References

[IEEE2600]	IEEE 2600-2008 IEEE Standard for Information Technology: Hardcopy Device and System Security
[PA-TNC]	A Posture Attribute Protocol (PA) Compatible with TNC: draft-ietf-nea-pa-tnc-02.txt
[RFC2119]	Key words for use in RFCs to Indicate Requirement Levels
[RFC2277]	IETF Policy on Character Sets and Languages
[RFC3766]	Determining Strengths for Public Keys Used For Exchanging Symmetric Keys
[RFC4086]	Randomness Requirements for Security

10. Contributors

Randy Turner – Amalfi Systems
Lee Farrell – Canon
Rick Landau – Dell
Glen Petrie – Epson
Harry Lewis – InfoPrint
Dave Whitehead – Lexmark
Nancy Chen – Oki Data
Ron Bergman – Ricoh
Brian Smithson – Ricoh
Shah Bhatti – Samsung
Peter Cybuck – Sharp
Joe Murdock – Sharp
Ron Nevo – Sharp
Craig Whittle – Sharp
Bill Wagner – TIC
Sameer Yami – Toshiba
Pete Zehler – Xerox

11. Authors Addresses

Jerry Thrasher
Lexmark International
740 New Circle Road
Lexington, KY 40550
Email: thrasher@lexmark.com

Annex A Change Log (informative)

Note: This section will be removed after PWG Last Call completion.

A.1 Changes from November 13, 2008

- Application of changes identified at the 12/03/2008 IDS Face to Face meeting.
- Update of the informative references.

A.2 Changes from January 06, 2009

- Global change of HCD_Secure_Time_Enabled to HCD_Authenticated_Time_Enabled.

A.3 Changes from February 02, 2009

- Accepted all changes, created new base for review.

A.4 Changes from February 10, 2009

- Changes from the 02/18/09 Face to Face meeting.

A.5 Changes from February 18, 2009

- Accepted changes and applied changes (none) from WG last call.

A.6 Changes from April 15, 2009

- Changes from the 04/30/2009 Face to Face meeting. Note: this an interim working draft showing results of current last call comments.

Page 10: [1] Deleted Glen W Petrie 6/4/2009 11:32:00 AM

A change to any configuration setting that is included in the creation of the attribute MUST cause a change, within the limits of information theory, in the attributes value. The configuration settings included as part of this attribute SHOULD be administratively configurable. Note: An example implementation of this attribute could be a cryptographically secure hash of the configuration settings.

Implementer Note:

The HCD_Configuration_State attribute is intended to provide a method for a system administrator (site local, device, etc.) to snap-shot a specific device configuration state. Examples of configuration information included in this attribute may include such items as default settings for duplex, media type, color mode, language, etc.; enabled or disabled services or features such as Fax, IPP, SSL support etc.; and encryption parameters for storage or network transports. In conjunction with a system health validation agent, this value can be used to determine if the configuration has changed in any way from the last snap-shot. No standardized values or behavior is defined by the PWG, only the ability to detect a change. Any access control restrictions that may be triggered by a change in this attribute are vendor or administrator defined. While a specific vendor may wish to provide mediation support for this attribute, no remediation support is defined or required by this standard.

Page 10: [2] Deleted Glen W Petrie 6/4/2009 11:36:00 AM

(0 = no forwarding enabled) Note: An example of this may be a USB, Infrared, 802.11, Bluetooth, or PSTN Fax interface being bridged to the Ethernet interface allowing devices that have not been subject to the health assessment measurement to access the Ethernet network.