IEEE

IEEE Standard for Information Technology: Hardcopy Device and System Security

IEEE Computer Society

Sponsored by the
Information Assurance Committee

2600™

IEEE
3 Park Avenue
New York, NY 10016-5997, USA

30 June 2008

IEEE Std 2600™-2008

IEEE Standard for Information Technology: Hardcopy Device and System Security

Sponsor

Information Assurance Committee
of the
IEEE Computer Society

Approved 27 March 2008
IEEE-SA Standards Board

The following companies have agreed to make financial contributions to underwrite the cost of Common Criteria certification of some or all of the IEEE Std 2600-series Protection Profiles:

Canon Inc.; Fuji Xerox; The Hewlett-Packard Company; InfoPrint Solutions Company; Konica Minolta; Kyocera Mita Corporation; Lexmark International, Inc.; Océ; Oki Printing Solutions; Ricoh Company, Ltd.; Samsung Electronics Co., Ltd.; Sharp Corporation; Toshiba TEC Corporation; Xerox Corporation

Abstract: This standard defines security requirements (all aspects of security including but not limited to authentication, authorization, privacy, integrity, device management, physical security, and information security) for manufacturers, users, and others on the selection, installation, configuration, and usage of hardcopy devices (HCDs) and systems, including printers, copiers, and multifunction devices (MFDs), and the computer systems that support these devices. This standard identifies security exposures for these HCDs and systems, and instructs manufacturers and software developers on appropriate security capabilities to include in their devices and systems, and instructs users on appropriate ways to use these security capabilities.
Keywords: all-in-one, copier, facsimile, fax, hardcopy device, HCD, information security, MFD, MFP, multifunction device, multifunction product, printer, scanner

The Institute of Electrical and Electronics Engineers, Inc.
3 Park Avenue, New York, NY 10016-5997, USA

PDF: ISBN 978-0-7381-5750-4 STD95801
Print: ISBN 978-0-7381-5751-1 STDPD95801

IEEE Standards documents are developed within the IEEE Societies and the Standards Coordinating Committees of the IEEE Standards Association (IEEE-SA) Standards Board. The IEEE develops its standards through a consensus development process, approved by the American National Standards Institute, which brings together volunteers representing varied viewpoints and interests to achieve the final product. Volunteers are not necessarily members of the Institute and serve without compensation. While the IEEE administers the process and establishes rules to promote fairness in the consensus development process, the IEEE does not independently evaluate, test, or verify the accuracy of any of the information or the soundness of any judgments contained in its standards.

Use of an IEEE Standard is wholly voluntary. The IEEE disclaims liability for any personal injury, property or other damage, of any nature whatsoever, whether special, indirect, consequential, or compensatory, directly or indirectly resulting from the publication, use of, or reliance upon this, or any other IEEE Standard document.

The IEEE does not warrant or represent the accuracy or content of the material contained herein, and expressly disclaims any express or implied warranty, including any implied warranty of merchantability or fitness for a specific purpose, or that the use of the material contained herein is free from patent infringement. IEEE Standards documents are supplied "**AS IS**."

The existence of an IEEE Standard does not imply that there are no other ways to produce, test, measure, purchase, market, or provide other goods and services related to the scope of the IEEE Standard. Furthermore, the viewpoint expressed at the time a standard is approved and issued is subject to change brought about through developments in the state of the art and comments received from users of the standard. Every IEEE Standard is subjected to review at least every five years for revision or reaffirmation. When a document is more than five years old and has not been reaffirmed, it is reasonable to conclude that its contents, although still of some value, do not wholly reflect the present state of the art. Users are cautioned to check to determine that they have the latest edition of any IEEE Standard.

In publishing and making this document available, the IEEE is not suggesting or rendering professional or other services for, or on behalf of, any person or entity. Nor is the IEEE undertaking to perform any duty owed by any other person or entity to another. Any person utilizing this, and any other IEEE Standards document, should rely upon his or her independent judgment in the exercise of reasonable care in any given circumstances or, as appropriate, seek the advice of a competent professional in determining the appropriateness of a given IEEE standard.

Interpretations: Occasionally questions may arise regarding the meaning of portions of standards as they relate to specific applications. When the need for interpretations is brought to the attention of IEEE, the Institute will initiate action to prepare appropriate responses. Since IEEE Standards represent a consensus of concerned interests, it is important to ensure that any interpretation has also received the concurrence of a balance of interests. For this reason, IEEE and the members of its societies and Standards Coordinating Committees are not able to provide an instant response to interpretation requests except in those cases where the matter has previously received formal consideration. A statement, written or oral, that is not processed in accordance with the IEEE-SA Standards Board Operations Manual shall not be considered the official position of IEEE or any of its committees and shall not be considered to be, nor be relied upon as, a formal interpretation of the IEEE. At lectures, symposia, seminars, or educational courses, an individual presenting information on IEEE standards shall make it clear that his or her views should be considered the personal views of that individual rather than the formal position, explanation, or interpretation of the IEEE.

Comments for revision of IEEE Standards are welcome from any interested party, regardless of membership affiliation with IEEE. Suggestions for changes in documents should be in the form of a proposed change of text, together with appropriate supporting comments. Comments on standards and requests for interpretations should be submitted to the following address:

Secretary, IEEE-SA Standards Board
445 Hoes Lane
Piscataway, NJ 08854
USA

Introduction

This introduction is not part of IEEE Std 2600-2008, IEEE Standard for Information Technology: Hardcopy Device and System Security.

This standard defines the security requirements and guidance for manufacturers, information technology (IT) professionals, users, and others on the selection, installation, configuration, and usage of secure hardcopy devices (HCDs) and systems. The standard defines unique security requirements for HCDs in four different usage environments that map to most HCD installations.

This standard is part of a family of standards that are related to HCD and system security. IEEE P2600.1™ [B34],[a] IEEE P2600.2™ [B35], IEEE P2600.3™ [B36], and IEEE P2600.4™ [B37] provide Common Criteria protection profiles that can be used by manufacturers to create Common Criteria version 3.1 conformant Security Target documents for use in the Common Criteria certification program. Respectively, IEEE P2600.1, IEEE P2600.2, IEEE P2600.3, and IEEE P2600.4 are protection profiles that correspond to Operational Environments A, B, C, and D, as defined in this standard. The requirements for each environment listed in the compliance clause in this standard map directly to the required security objectives in the profile documents. This standard also defines additional security guidance and recommendations for non-IT security techniques that are beyond the scope of Common Criteria certification and for IT security techniques that cannot be exhaustively tested and verified in the Common Criteria certification program.

Notice to users

Laws and regulations

Users of these documents should consult all applicable laws and regulations. Compliance with the provisions of this standard does not imply compliance to any applicable regulatory requirements. Implementers of the standard are responsible for observing or referring to the applicable regulatory requirements. IEEE does not, by the publication of its standards, intend to urge action that is not in compliance with applicable laws, and these documents may not be construed as doing so.

Copyrights

This document is copyrighted by the IEEE. It is made available for a wide variety of both public and private uses. These include both use, by reference, in laws and regulations, and use in private self-regulation, standardization, and the promotion of engineering practices and methods. By making this document available for use and adoption by public authorities and private users, the IEEE does not waive any rights in copyright to this document.

Updating of IEEE documents

Users of IEEE standards should be aware that these documents may be superseded at any time by the issuance of new editions or may be amended from time to time through the issuance of amendments, corrigenda, or errata. An official IEEE document at any point in time consists of the current edition of the document together with any amendments, corrigenda, or errata then in effect. In order to determine

[a] The numbers in brackets correspond to those of the bibliography in Annex B.

whether a given document is the current edition and whether it has been amended through the issuance of amendments, corrigenda, or errata, visit the IEEE Standards Association Web site at http://ieeexplore.ieee.org/xpl/standards.jsp, or contact the IEEE at the address listed previously.

For more information about the IEEE Standards Association or the IEEE standards development process, visit the IEEE-SA Web site at http://standards.ieee.org.

Errata

Errata, if any, for this and all other standards can be accessed at the following URL: http://standards.ieee.org/reading/ieee/updates/errata/index.html. Users are encouraged to check this URL for errata periodically.

Interpretations

Current interpretations can be accessed at the following URL: http://standards.ieee.org/reading/ieee/interp/index.html.

Patents

Attention is called to the possibility that implementation of this standard may require use of subject matter covered by patent rights. By publication of this standard, no position is taken with respect to the existence or validity of any patent rights in connection therewith. A patent holder or patent applicant has filed a statement of assurance that it will grant licenses under these rights without compensation or under reasonable rates, with reasonable terms and conditions that are demonstrably free of any unfair discrimination to applicants desiring to obtain such licenses. Other Essential Patent Claims may exist for which a statement of assurance has not been received. The IEEE is not responsible for identifying Essential Patent Claims for which a license may be required, for conducting inquiries into the legal validity or scope of Patents Claims, or determining whether any licensing terms or conditions provided in connection with submission of a Letter of Assurance, if any, or in any licensing agreements are reasonable or non-discriminatory. Users of this standard are expressly advised that determination of the validity of any patent rights, and the risk of infringement of such rights, is entirely their own responsibility. Further information may be obtained from the IEEE Standards Association.

Participants

At the time this standard was submitted to the IEEE-SA Standards Board for approval, the P2600 Standard Working Group had the following membership:

Don Wright, *Chair*
Lee Farrell, *Vice Chair*
Brian Smithson, *Secretary*
Jerry Thrasher, *Editor*

Hiromasa Akamatsu
Carmen Aubry
Ron Bergman
Shah Bhatti
Nancy Chen
Peter Cybuck
Nick Del Re
David Freas
Fusayuki Fujita
Satoshi Fujitani
Tom Haapanen
Kazutaka Higo
Hiroshi Hosaka
Akihiko Iwasaki
Harry Lewis
Jean-Claude Longo
Daniel Manchala
Takanori Masui
Takeshi Nakamura
Ron Nevo
Wanda Nuckolls
Yusuke Ohta
Ken Ota
Glen Petrie
Stuart Rowley
Ole Skov
Alan Sukert
Yasuji Takeuchi
Hiroki Uchiyama
Shigeru Ueda
Brian Volkoff
Bill Wagner
Jan Walter
Craig Whittle
Sameer Yami
Liang Zhao

The following members of the individual balloting committee voted on this standard. Balloters may have voted for approval, disapproval, or abstention.

Danilo Antonelli
Carmen Aubry
Matthew Ball
Massimo Cardaci
Juan Carreon
Ying Chen
Keith Chow
John Cole
Geoffrey Darnton
Russell Dietz
Lee Farrell
Randall Groves
Tom Haapanen
Mark Henley
Eric Hibbard
Werner Hoelzl
Raj Jain
Piotr Karocki
Michael S. Newman
Charles K. Ngethe
Michael D. Rush
Brian Smithson
Thomas Starai
Walter Struppler
Jerry Thrasher
Thomas Tullia
Paul Work
Don Wright
Sameer Yami

When the IEEE-SA Standards Board approved this standard on 27 March 2008, it had the following membership:

Robert M. Grow, *Chair*
Thomas Prevost, *Vice Chair*
Steve M. Mills, *Past Chair*
Judith Gorman, *Secretary*

Victor Berman
Richard DeBlasio
Andy Drozd
Mark Epstein
Alexander Gelman
William R. Goldbach
Arnold M. Greenspan
Kenneth S. Hanus
Jim Hughes
Richard H. Hulett
Young Kyun Kim
Joseph L. Koepfinger*
John Kulick
David J. Law
Glenn Parsons
Ronald C. Petersen
Chuck Powers
Narayanan Ramachandran
Jon Walter Rosdahl
Anne-Marie Sahazizian
Malcolm V. Thaden
Howard L. Wolfman
Don Wright

*Member Emeritus

Also included are the following nonvoting IEEE-SA Standards Board liaisons:

Satish K. Aggarwal, *NRC Representative*
Michael H. Kelley, *NIST Representative*

Jennie Steinhagen
IEEE Standards Program Manager, Document Development

Michael D. Kipness
IEEE Standards Program Manager, Technical Program Development

Contents

IEEE Standard for Information Technology: Hardcopy Device and System Security

IMPORTANT NOTICE: This standard is not intended to assure safety, security, health, or environmental protection in all circumstances. Implementers of the standard are responsible for determining appropriate safety, security, environmental, and health practices or regulatory requirements.

This IEEE document is made available for use subject to important notices and legal disclaimers. These notices and disclaimers appear in all publications containing this document and may be found under the heading "Important Notice" or "Important Notices and Disclaimers Concerning IEEE Documents." They can also be obtained on request from IEEE or viewed at http://standards.ieee.org/IPR/disclaimers.html.

1. Overview

1.1 Scope

This standard defines security requirements (all aspects of security including but not limited to authentication, authorization, privacy, integrity, device management, physical security and information security) for manufacturers, users, and others on the selection, installation, configuration and usage of hardcopy devices (HCDs) and systems; including printers, copiers, and multifunction devices (MFDs). This standard identifies security exposures for these HCDs and systems, and instructs manufacturers and software developers on appropriate security capabilities to include in their devices and systems, and instructs users on appropriate ways to use these security capabilities.

1.2 Purpose

In today's information technology (IT) environment, significant time and effort are being spent on security for workstations and servers. However, today's HCDs (printers, copiers, MFDs, etc.) are connected to the same local area networks (LANs) and contain many of the same communications, processing and storage components, and are subject to many of the same security problems as workstations and servers. At this time, there are no standards to guide manufacturers or users of HCDs in the secure installation, configuration, or usage of these devices and systems.

The purpose of this document is to serve as such a standard and its goals are:

a) To provide guidance in the secure architecture, design, and out-of-box configuration of HCDs for manufacturers;

b) To provide guidance in the secure installation, configuration, and use of HCDs for end users and their supporting organizations.

1.3 Document structure

Clause 1 provides the scope and purpose of the standard and an overview of the standard’s structure.

Clause 2 provides the definitions, special terms, acronyms, and abbreviations used in this standard.

Clause 3 describes the structure, architecture, and functions of a hardcopy device.

Clause 4 describes the various security environments of hardcopy devices considered by this standard.

Clause 5 describes the various assets of an HCD.

Clause 6 describes the threats against HCDs that are considered by this standard.

Clause 7 describes some of the mitigation techniques used to address each threat described in Clause 6. Mitigation techniques are provided for manufacturers, IT administrators, and users.

Clause 8 indicates specific security objectives, by operational environment, that are mandatory for compliance with this standard and provides example mitigation techniques that may be used to accomplish these objectives.

Annex A describes the best practices for various general security measures for HCDs. Best practices are provided for manufacturers, IT administrators, and users of HCDs.

Annex B provides additional references, which may add to the understanding of other parts of this document.

2. Definitions, special terms, acronyms, and abbreviations

2.1 Definitions

For the purposes of this document, the following terms and definitions apply. *The Authoritative Dictionary of IEEE Standards Terms* [B38][1] should be referenced for terms not defined in this clause.

2.1.1 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. *See also:* **multifunction device.**

2.1.2 multifunction device (MFD): An HCD that fulfills multiple purposes by using multiple functions in different combinations to replace several, single function devices.

2.2 Special terms

Terms used in this standard are defined as follows:

access control: Security service that controls the use of hardware and software resources and the disclosure and modification of stored or communicated data.

accountability: Property that allows activities in an IT system to be traced to the entity responsible for the activity.

actor: A role that a user plays with respect to an HCD.

administrator: A user who has been specifically granted the authority to manage some portion or all of the HCD and whose actions may affect the security policy. Administrators may possess special privileges that provide capabilities to override portions of the security policy.

applet: A program designed to be executed from within another program, e.g., a Java™ virtual machine program.[2] Applets cannot be executed directly from the operating system (OS).

application: The software or firmware that performs a major function of the HCD, e.g., authentication, copying, printing, scanning, and facsimile (fax).

asset: An entity upon which the owner, user, or manager of the device places value.

assurance: A measure of confidence that the security features of an IT system are sufficient to enforce its security policy.

attack: An intentional act attempting to violate the security policy of an IT system.

auditor: A user who reviews and maintains the audit trail recorded by the HCD.

[1] The numbers in brackets correspond to those of the bibliography in Annex B.

[2] Java is a trademark of Sun Microsystems, Inc. in the United States and other countries. This information is given for the convenience of users of this standard and does not constitute an endorsement by the IEEE of these products. Equivalent products may be used if they can be shown to lead to the same results.

authentication data: Information used to verify a claimed identity.

authorized administrator: A user who has been specifically granted permission by an entity authorized to do so to manage some portion or all of the HCD and whose actions may affect the security policy.

authorized user: An authenticated user who may, in accordance with the HCD's security policy, perform an operation.

back channel: Typically a low-speed or less-than-optimal transmission channel flowing opposite to the forward channel's direction. In many cases, the back channel is used mostly for acknowledgements of the validity of the forward channel's data (i.e., that the forward channel's data passes validity tests of some sort). *Contrast:* **forward channel.**

black list: A list of specific user credential values (e.g., login ID, e-mail addresses, phone numbers, URLs) that are explicitly prohibited from accessing all or specified functions of an HCD. *Contrast:* **white list.**

compromise: Type of incident where information is disclosed to unauthorized individuals or a violation of the security policy of a system in which unauthorized intentional or unintentional disclosures, modification, destruction, or loss of an object may have occurred.

copy control device: An entity external to the HCD, comprising hardware or software that enables and tracks copying.

copy control interface: An interface for connecting a copy control device to an HCD.

credential: A form of authentication data that specifies basic identifying information about a user or application. Credentials may be bound in some way to the individual to whom they were issued, or they may be bearer credentials. The former are necessary for identification, while the latter may be acceptable for some forms of authorization.

customer engineer: A person authorized to maintain an HCD at a customer site.

data: A representation of facts, concepts, or instructions in a manner suitable for communication, interpretation, or processing by humans or by automatic means

data interface: Any interface that transports print or scan data into or out of the HCD.

demilitarized zone (DMZ): A computer or small subnetwork that sits between a trusted internal network, such as a corporate private LAN, and an untrusted external network, such as the public Internet.

defense in depth: A security design strategy whereby layers of protection are utilized to establish an acceptable security posture for an IT system.

denial of service (DoS): The prevention of authorized access to a system resource or the delaying of system operations and functions.

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).

device interface: An electrical interface for connecting a device to control access to local operation of the HCD. Depending on the device and its purpose, access may be granted as a result of identifying the user or as a result of a payment. *See also*: **copy control interface.**

dictionary attack: An attack that tries all of the phrases or words in a dictionary, trying to crack a password or key. A dictionary attack uses a predefined list of words compared to a brute force attack that tries all possible combinations.

entity: A subject, object, user, or another IT device, which interacts with HCD objects, data, or resources.

external device interface*: See:* **device interface.**

firewall: A gateway that limits access between networks in accordance with local security policy.

firmware: Persistent computer instructions and data embedded in the HCD that provides basic functions of that device. Firmware is only replaced during a specialized update process.

forward channel: Communications channel used for the delivery of document data. *Contrast:* **back channel.**

identity: A representation (e.g., a string) uniquely identifying an authorized user, which can either be the full or abbreviated name of that user or a pseudonym.

information assurance: Information operations that protect and defend information and information systems by ensuring their availability, integrity, authentication, confidentiality, and non-repudiation. This includes providing for restoration of information systems by incorporating protection, detection, and reaction capabilities.

information technology (IT): The hardware, firmware, and software used as part of a system to collect, create, communicate, compute, disseminate, process, store, or control data or information.

local interface: An electrical, optical, or electromagnetic (EM) interface intended for use with close physical proximity (typically no more than 10 m) to the HCD. Examples include USB [B148], FireWire® (IEEE Std 1394™-1995 [B44]), IrDA®, parallel port (IEEE Std 1284™-2000 [B43]), serial port (e.g., EIA-232-1987 [B19]), memory card, diskette, and Bluetooth® (IEEE Std 802.15.1™-2005 [B42]). [3]

maintenance port: An electrical interface used for machine maintenance, service troubleshooting, or firmware updates.

man-in-the-middle attack: An active attack whereby a third party attempts to surreptitiously intercept, read, or alter information moving between two computing devices or users.

media: Objects on which data are or can be imaged. These include paper, transparencies, T-shirt transfers, etc.

network administrator: A user who manages the network configuration of the HCD.

network interface: An interface used to connect the HCD to a network. Examples include IEEE 802.3™, IEEE 802.5™, and IEEE 802.11™ interfaces.

non-repudiation: (A) The prevention of false denial of involvement in sending or receiving information. **(B)** A security policy pertaining to providing one or more of the following: to the sender of data, proof of delivery to the intended recipient; to the recipient of data, proof of the identity of the user who sent the data.

[3] FireWire is a registered trademark of Apple Inc. IrDA is a registered trademark of Infrared Data Association. Bluetooth is a registered trademark owned by the Bluetooth SIG, Inc. [B9]. This information is given for the convenience of users of this standard and does not constitute an endorsement by the IEEE of these products. Equivalent products may be useful if they can be shown to lead to the same results.

operational environment: The total environment in which an HCD operates, including the consideration of the value of assets and controls for operational accountability, physical security, and personnel.

operator panel: A local human interface used to operate the HCD. It typically consists of a keypad, keyboard, or other controls, and a display device.

password cracking: The process of attempting to ascertain secret passwords, often through algorithmic, dictionary, or automated procedures.

risk assessment: Assessment of threats to, impacts on, and vulnerabilities of information and information processing facilities and equipment including consideration of the likelihood of occurrence.

security objective: A statement of intent to counter identified threats or satisfy identified organization security policies or assumptions.

sniffing: Network wiretapping; passively monitoring and recording data that is flowing between two or more points in a communication system.

social engineering: Non-technical or low-technology means—such as deception, impersonation, tricks, bribes, blackmail, and threats—used to attack information systems.

spam: Unsolicited and unwanted electronic mail, instant messages, or other electronic communications.

stored data: Fonts, forms, and document data.

temporary data: The data, e.g., images, print file, that are temporarily buffered or stored in memory before or while the HCD performs application operations.

threat: Capabilities, intentions and attack methods of adversaries, or any circumstance or event, with the potential to violate the HCD's security policy.

threat agent: Any human user or IT product or system that may attempt to violate the HCD's security policy and perform an unauthorized operation with the HCD.

unauthorized user: A user who is not permitted to access or use an HCD for a defined purpose.

user: An entity (human user or IT entity) outside the HCD that interacts with the HCD.

User Document Data: The asset that consists of the information contained in a user's document. This includes the original document itself in either hardcopy or electronic form, image data, or residually stored data created by the HCD while processing an original document and printed hardcopy output.

User Function Data: The asset that consists of the information about a user's document or job to be processed by the HCD.

vulnerability: A weakness that can be exploited to violate the HCD's security policy.

white list: A list of specific user credential values (e.g., login ID, e-mail addresses, phone numbers, URLs) that are explicitly allowed access to all or specified functions of an HCD. *Contrast:* **black list.**

2.3 Acronyms and abbreviations

Abbreviations and acronyms used in this document are defined as follows:

3DES	“Triple DES” data encryption standard used three times
ADPU	active directory password utility
AES	advanced encryption standard
ANSI	American National Standards Institute
APOP	authenticated post office protocol
ASIS	American Society for Industrial Security
ATM	automated teller machine
BioAPI	Biometric Application Programmer Interface
CBC	cipher block chaining
CBEFF	common biometric exchange file format
CEN	European Committee for Standardization
CF	compact flash
CIFS	common Internet file system
CM	configuration management
COTS	commercial, off-the-shelf
CPU	central processing unit
CRC	cyclic redundancy check
C-SET	card secured electronic transactions
CSMA/CD	carrier sense multiple access/collision detection
CSN	card serial number (for compact flash)
DES	data encryption standard
DHS	U.S. Department of Homeland Security
DMZ	demilitarized zone
DoD	U.S. Department of Defense
DOE	U.S. Department of Energy

DoS	denial of service
DRAM	dynamic random access memory
DSA	directory service agent
DSL	digital subscriber loop
DSS	digital signature standard
EEPROM	electrically erasable programmable read-only memory
EIA	Electronic Industries Association
EM	electromagnetic
EMI	electromagnetic interference
EMSEC	emission security
EMV™	Europay-Mastercard®-Visa® [4]
EN	ISO language code for English, all dialects
EPROM	erasable programmable read-only memory
ESMTP	extended simple mail transfer protocol
ESP	encapsulating security payload
ETSI	European Telecommunications Standards Institute
EU	European Union
fax	facsimile
FIPS	Federal Information Processing Standards
FISMA	Federal Information Security Management Act of 2002 [B22]
FX	foreign exchange
GOST	GOsudarstvennyi STandard (Russian for “government standard”)
GSM	global system for mobile communications
HCD	hardcopy device
HDD	hard disk drive

[4] The EMV™ Mark is a trademark exclusively owned by EMVCo LLC. MasterCard is a registered trademark of MasterCard Worldwide. The Visa trademark is owned by Visa Inc. This information is given for the convenience of users of this standard and does not constitute an endorsement by the IEEE of these products. Equivalent products may be used if they can be shown to lead to the same result.

HIPAA	Health Insurance Portability and Accountability Act
HMAC	keyed-hash message authentication code
HMG	Her/His Majesty’s government
HPNA	Home Phoneline Networking Alliance
HTTPS	hypertext transfer protocol (secure)
I/O	input/output
IBIA	International Biometric Industry Association
ICC	integrated circuit card
ICMP	Internet control message protocol
ID	identification
IEC	International Electrotechnical Commission
IFD	interface device
IKE	Internet key exchange
INCITS	InterNational Committee for Information Technology Standards (USTAG to JTC1)
IP	Internet protocol version 4
IPP	Internet printing protocol
IPsec	Internet protocol security
IPv6	Internet protocol version 6
IrDA	Infrared Data Association
ISAKMP	Internet security association and key management protocol
ISO	International Organization for Standardization
ISP	Internet service provider
IT	information technology
ITL	information technology laboratory
kb/s	kilobits per second
KDC	key distribution center
LAN	local area network
LCD	liquid crystal display

LDAPS	lightweight directory access protocol (secure)
MAC	media access control
MD5	message-digest algorithm 5
METI	Japanese Ministry of Economy, Trade and Industry
MFD	multifunction device
MFM	modified frequency modulation
MFP	multifunction product/peripheral/printer
MIC	message integrity code
MICR	magnetic ink character recognition
NATO	North Atlantic Treaty Organization
NAVSO	Navy Staff Office
NIST	National Institute of Standards and Technology
NRC	Nuclear Regulatory Commission
OCR	optical character recognition
OCTAVE®	Operationally Critical Threat, Asset, and Vulnerability Evaluation℠ [5]
OS	operating system
OTS	off-the-shelf
PC	personal computer
PC/SC	proximity card/smart card
PDA	personal digital assistant
PDL	page description language
PHIPA	Personal Health Information Protection Act
PIN	personal identification number
PNA	Phoneline Networking Alliance
PSTN	public switched telephone network
RADIUS	remote authentication dial-in user service

[5] OCTAVE and Operationally Critical Threat, Asset, and Vulnerability Evaluation are trademarks and servicemarks owned by Carnegie Mellon University. This information is given for the convenience of users of this standard and does not constitute an endorsement by the IEEE of these products. Equivalent products may be used if they can be shown to lead to the same result.

RAM	random access memory
RFC	request for comment
RIP	raster image processor
RLL	run length limited
ROM	read-only memory
S/MIME	secure/multipurpose Internet mail extensions
SANS	sysadmin, audit, network, security
SCADA	supervisory control and data acquisition
SCQL	structured card query language
SCSI	small computer system interface
SEIS	secure electronic information in society
SET	secure electronic transactions
SHA	secure hash algorithm
SIM	subscriber identity module
SMI	shared media interface
SMTP	simple mail transport protocol
SNMP	simple network management protocol
SOHO	small office/home office
SRAM	static random access memory
SSH	secure shell
SSL	secure sockets layer
STANAG	standardization agreement
TACACS	terminal access controller access control system
TCP	transmission control protocol
TE	terminal equipment
TLS	transport layer security
TWIC	transportation worker identification credential
UDP	user datagram protocol

USB	Universal Serial Bus
USENIX	Advanced Computing Systems Association
USM	user-based security model
VLAN	virtual local area network
VPN	virtual private network
VSITR	Verschluss-sachen-IT-Richlinien
WAN	wide area network
WEP	wired equivalent privacy
WPA2™	Wi-Fi® protected access 2 (an enhanced version of WPA™) [6]
WPA	Wi-Fi protected access

[6] Wi-Fi, WPA, and WPA2 are trademarks of the Wi-Fi Alliance [B151]. This information is given for the convenience of users of this standard and does not constitute an endorsement by the IEEE of these products. Equivalent products may be useful if they can be shown to lead to the same results.

3. Introduction to hardcopy devices

3.1 Hardcopy device overview

The HCDs that are considered in this standard are used for the purpose of converting hardcopy documents into digital form (scanning), converting digital documents into hardcopy form (printing), transmitting or receiving documents over telephone lines [public switched telephone network (PSTN) faxing], or duplicating hardcopy documents (copying). Typically, hardcopy documents are in paper form, but they can also take other forms (e.g., positive or negative transparencies or film).

HCDs can be implemented in many different configurations, depending on their intended purpose or purposes. Simple devices have a single purpose implemented by a single function, such as a printer or scanner. Other devices have a single purpose implemented by a compound function, such as a copier or fax machine. Complex MFDs fulfill multiple purposes by using multiple functions in different combinations to replace several, single function devices.

For the purposes of this standard, a generic MFD will be used as an example because it is composed of all of the individual purposes and functions of other HCDs; however, this standard can be applied to an HCD that is composed of any combination of these purposes and functions.

3.2 Generic architecture

HCD architecture and organization of functions vary widely depending upon specific functions, features, manufacturers, and other factors. For the purpose of illustration, a generic, composite architecture is shown in Figure 1, and its component parts are described subsequently.

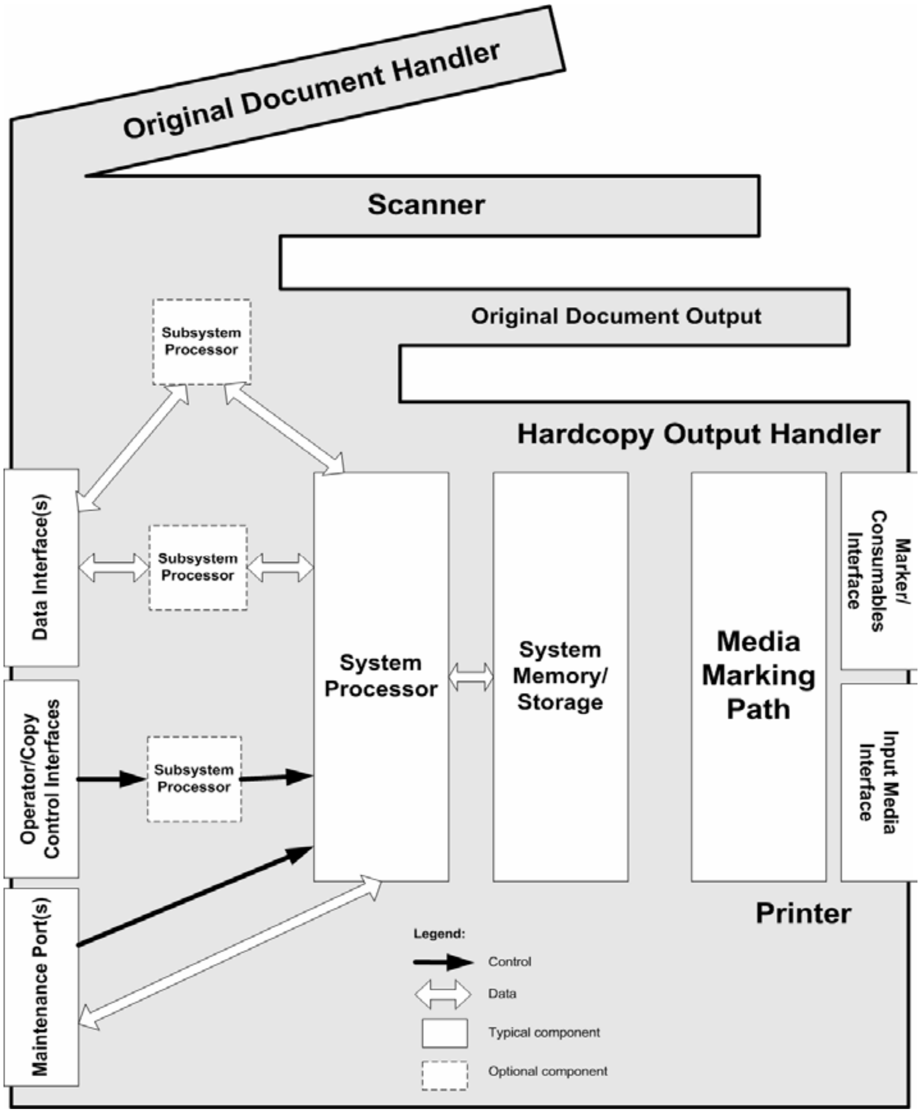

Figure 1—Generic architecture

3.2.1 Scanning function

3.2.1.1 Original document handler

The *original document handler* is the part of the HCD's media handling function that manipulates the input document into the proper position for scanning. Examples of Original Document Handler components include: flatbed glass window, single sheet feeder, or a multiple sheet input with duplexer.

3.2.1.2 Scanner

The *scanner* is an optical input device that uses light-sensing equipment to capture an image of a hardcopy document and translate it into a digital form that can be transmitted, stored, or be subsequently used to recreate the document.

3.2.1.3 Original document output

The *original document output* is the part of the HCD's media handling function that accumulates input documents after scanning.

3.2.2 Printing function

3.2.2.1 Input media interface

The *input media interface* includes any method for human access to the mechanisms that store and feed media (typically paper) to be marked on by an HCD. Examples of this interface would be the sliding drawers that hold paper for an office copier or the roll paper mechanism for a point-of-sale terminal.

3.2.2.2 Marker/consumables interface

The *marker/consumables interface* includes any method for human access to the user replaceable supplies (i.e., ink/toner/dye containers, developer roll, waste toner bottle) in an HCD. An example of this interface would be the doors and latches that are opened to replace a toner cartridge in a general-purpose laser printer.

3.2.2.3 Media marking path

The *media marking path* includes all paths in the printing function that the input media takes between the input media interface and the hardcopy output handler. This path may include certain intermediate media handling devices (e.g., duplexer) as well as the path through the marking mechanism.

3.2.2.4 Printer

The *printer* is the mechanism that applies ink, toner, or dye to create an image on the output medium. There are many different kinds of printers such as laser, LED, ink-jet, dot matrix, and dye sublimation. Depending on the kind of printer, they can create color output as well as black and white.

3.2.2.5 Hardcopy output handler

The *hardcopy output handler* is the part of the HCD's media handling function that holds or manipulates the media after it has exited the media marking path (print engine). The hardcopy output handler may also include certain post-printing processes (finishing options) such as stapling, folding, or hole punching. Examples include the exit tray of a printer, mailbox attachments to a MFD, and a stapler or collator attachment for a copier.

3.2.2.6 System processor and memory/storage

The *system processor* includes any microprocessor, digital signal processor, or microcontroller that has modifiable microcode or processes any type of user data or management information for the HCD. The *system memory* or *storage* includes any volatile or nonvolatile storage in the HCD. Examples include EEPROM, DRAM, SRAM, flash memory, and hard disk drive (HDD).

NOTE—Figure 1 shows the system processor or memory system as a single entity. In a typical HCD, many of the interfaces or components within a specific HCD may have their own microprocessor or memory subsystems. [7]

3.2.3 External interfaces

3.2.3.1 Data interface

The *data interface* of an HCD includes any interface that transports print or scan data into or out of the HCD's system processor and memory. Some data interface designs may include independent processor and memory subsystems. Examples include USB, parallel port (IEEE Std 1284-2000 [B43]), IEEE Std 802.3-2005 [B39], IEEE Std 802.5-1998 [B40], IEEE Std 802.11-2007 [B41].

NOTE—Some modular HCD architectures may include dedicated interfaces between specific functions of the device (e.g., scanner to print engine interface in an HCD, or a printing system where the system processor and memory are an external computer). These interfaces are not considered data interfaces in this standard.

3.2.3.2 Operator interface

The *operator interface* of the HCD is any physical human interface (e.g., touch screen LCD control panel) that allows access to the display or the modification of the state of the HCD. This interface can be as simple as a few lights and buttons on an inkjet printer to a full screen display with keyboard. This interface does not include remote or reflected user interfaces that may be implemented as part of a management application that accesses the device via one of the data interfaces. The remote management application and its host system are not within the scope of this standard.

3.2.3.3 Copy control interface

HCDs may include an electrical interface for external devices that are used for accounting, identification, or payment.

NOTE—This interface may also contain a software component as well.

3.2.3.4 Maintenance ports

Maintenance ports are interfaces used for machine maintenance, troubleshooting, and firmware updates.

3.3 Similarities and differences between HCDs and other IT devices

3.3.1 Basic security objectives for HCDs

Fundamentally, the security objectives for HCDs are the same as those for any kind of IT equipment that creates, stores, or processes information: protect the confidentiality, integrity, and availability of the defined assets.

HCD assets generally include but are not limited to the following:

[7] Notes in text, tables, and figures of a standard are given for information only and do not contain requirements needed to implement the standard.

a) The information being processed by the HCD

b) Data that is associated with processing that information

c) Data that is associated with configuring and securing the HCD

d) Use of the HCD itself

e) Physical assets associated with the HCD

See Clause 5 for complete definitions.

Security objectives also consider the confidentiality, integrity, or availability of the HCD's operating software and the data associated with authorizing HCD use and configuration, because their disclosure, alteration, or destruction can pose a threat to the HCD's assets. Additional security objectives consider the HCD's network services, because a misappropriated HCD could be employed to harm other IT devices on the same network.

See Clause 6 for more details.

3.3.2 Distinguishing characteristics

Many of the same administrative, physical, and logical security measures that are used to provide security for a general purpose computer can be applied to an HCD as well. However, HCDs are different from general purpose computers in the following ways:

a) HCDs not only process and store a user's data in electronic form, they also process or generate a user's data in physical form when the documents are scanned or printed.

b) HCDs have additional physical assets, such as toner or ink cartridges and blank media, intentionally designed for easy removal and replacement, which are required for the device to perform its intended function.

c) By virtue of their intended function, HCDs may be more physically accessible than either a desktop computer or a server computer in a given environment, and they are often available for use by a larger number of users.

d) HCDs are typically unattended, ownerless devices. Typically, desktop computers are placed in individual work areas and servers are placed in a controlled server room, but HCDs are often placed in common areas where they can be conveniently accessed by their users. In order to keep from disturbing people, HCDs are often placed out of sight from individual work areas and hence may be unmonitored for large periods of time.

e) HCDs are a temporary receptacle for their users' current documents of interest, and even if those documents are encrypted in transit and storage, they are not necessarily encrypted during scanning, printing, copying, and PSTN faxing.

Each of these distinguishing characteristics has security implications that further distinguish HCDs from general purpose computers, as follows:

1) Physical hardcopy documents are physically submitted to or retrieved from the HCD. There are a number of ways that the physical document can be misappropriated, ranging from social engineering to compromising the HCDs security functions. Physical controls to mitigate these threats can be inconvenient and costly.

2) Physical assets such as toners or media can be stolen for their monetary value, compromised to degrade or deny use of the HCD, or altered to compromise the integrity of physical document output. However, since these assets are consumable, they are accessible to make it easy to replenish them.

3) Widespread physical access to HCDs implies a variety of threats and makes it more difficult to determine responsibility for security-related events, but limiting physical access to an HCD reduces its utility and its economy.

4) Unattended, out-of-the-way operation means that physical presence at an HCD can go unnoticed, and the expectation that HCD users need to be present to submit and retrieve jobs means that such presence is unlikely to arouse suspicion. The lack of an owner who might watch over an HCD compounds the situation, because people may not feel the authority to question another's presence.

5) Users are most likely to print, scan, copy, or fax their most important and most current documents, making the HCD an ideal target for espionage. Since documents cannot be encrypted when printed, scanned, or PSTN faxed, an HCD can also be a target for accessing documents that would otherwise be encrypted in storage and in transit.

3.4 Determining the appropriate security strategy for an HCD

3.4.1 Environmental factors

As with any IT system, the appropriate security measures for protecting an HCD largely depend upon the value of and risk to the assets being protected. This is commonly expressed in terms of the business impact if the asset is lost or compromised as well as the likelihood of an attack against that asset. For example, it may not be necessary to implement any particular security measures to protect the printing of a recipe for fried chicken in a typical home office, but an enterprise might implement extensive organizational, physical and technical measures to secure the printing of a recipe for fried chicken if that enterprise is a fast food chain and that recipe is a core asset. Similarly, an HCD in the heart of a military installation may require no security measures to protect user documents if it is used only to print the daily cafeteria menu. Clause 4 describes several generalized operational environments on which the guidance, recommendations, and requirements of this standard are based.

3.4.2 Regulatory factors

Many parts of the world have adopted blanket legislation that requires the protection of personal information. The European Union has adopted EU 95/46/EC [B21] that requires that parties "must implement appropriate technical and organizational measures to protect personal data against accidental or unlawful destruction or accidental loss, alteration, unauthorized disclosure or access, in particular where the processing involves the transmission of data over a network and against all other unlawful forms of processing." An almost exact directive has been adopted in Japan as well via the METI Policy on the Protection of Personal Information [B79].

Other countries have passed directives dealing with specific types of personal or personally identifiable information as well as some types of non-personal information. Among these specific directives are, in the U.S., the Gramm-Leach-Bliley Act [B27], which deals with the protection of personal financial information, and the Sarbanes-Oxley Act of 2002 [B141], which deals with the control and protection of corporate financial and accounting records. The Health Insurance Portability and Accountability Act of 1996 (HIPAA) [B30] in the U.S., and the Personal Health Information Protection Act of 2004 (PHIPA) [B107] in Canada deal with the privacy and security of any type of personal "health related" information and details specific technical security measures, such as encryption, for protecting personal information in electronic form when transmitted or stored.

3.4.3 Typical approaches

3.4.3.1 General

For most operational environments, there is no global rule that defines which security measures are required or even warranted for an HCD. To help identify the appropriate security measures in a particular situation, the reader is directed to consult the following approach, which is most appropriate to their role.

3.4.3.2 For IT professionals

Each organization should perform a risk assessment that identifies assets, the threats to those assets, the probability of attack, and the business impact of a successful attack. Subsequently, the organization should compare the cost of mitigating each threat to the business impact of not mitigating the threat, and decide whether to mitigate, transfer, accept, or avoid that risk.

In some operational environments, specific procurement criteria, checklists, standards, or recommendations for securing IT equipment have been developed to aid in deciding what security measures to implement, thus reducing the need for a detailed risk assessment. Examples of some of these are provided in Clause 7, which may apply to HCDs if the assets of the HCD are sufficiently similar to the assets of the IT equipment.

3.4.3.3 For end users

If supported by an IT staff, end users should determine which of the operational environments in Clause 4 has been adopted by the IT staff, and then follow the appropriate guidance in Clause 7 and Annex A, regarding the use of their HCD. If unsupported, then end users should choose an appropriate security environment and follow its guidance.

3.4.3.4 For HCD manufacturers

The operational environments defined in Clause 4 are intended to be applicable to a variety of possible target markets. For a given target market, a manufacturer should choose the most applicable environment from the descriptions and examples given in Clause 4, and then should follow the guidance, recommendations, and requirements for that environment in Clause 7 and Clause 8, and in Annex A.

3.4.4 Use of this standard

3.4.4.1 Use by IT professionals

This standard is intended to help IT personnel determine an appropriate security strategy, but not to prescribe such a strategy. By identifying the operational environment in Clause 4 that most closely represents their particular HCD's environment, users of this standard will be guided to identify the appropriate assets described in Clause 5 and assess the relevant threats described in Clause 6, to perform their own risk analysis, and then consider the mitigation techniques described in Clause 7 and Annex A, to help decide how to handle their particular HCD security risks.

3.4.4.2 Use by end users

This standard is intended to help end users use HCDs in a secure manner through a combination of properly using the security features of their HCD and adopting secure behavioral practices, as described in Clause 7 and Annex A.

3.4.4.3 Use by HCD manufacturers

This standard is intended to help manufacturers design appropriately secure HCDs for a variety of operational environments. This standard will also help manufacturers provide default configuration settings and guidance to their customers to ensure that their HCDs are deployed and used in an appropriately secure fashion. By identifying the operational environments in Clause 4 that are most suitable to their customers, manufacturers will be guided to identify the appropriate assets in Clause 5, and design their products to protect those assets against relevant threats that are described in Clause 6.

4. Operational environments

4.1 Background

An organization's IT security needs depend on many factors, such as the value of its assets, the organizational impact of compromising those assets, the likelihood of a threat being carried out, various assumptions about the IT environment and about individuals in the organization, and externally mandated security requirements. The customary approach to evaluating a particular organization's IT security needs is to perform a risk analysis using those factors, and then a cost-benefit analysis to determine how (or whether) to mitigate each risk. There are many documented approaches to this process, including NIST Special Publication 800-30 [B82], ASIS International [B5], and ISO/IEC 27001:2005 [B71].

However, this standard is intended to apply to many different kinds of organizations, and so a conventional risk and cost-benefit analysis cannot be performed. Instead, four generalized classes of operational environments are defined. These environments are adapted from NIST Special Publication 800-70 [B102]. By choosing a generalized environment that most closely matches a particular organization's specific environment, the organization can identify the guidance and recommendations that are most applicable to its specific needs. Similarly, by choosing the generalized environment that most closely matches the requirements of a particular manufacturer's target customers, that manufacturer can identify the recommendations and requirements that are most applicable to that target market. Four operational environments (A, B, C, and D) are considered in this standard.

4.2 Operational Environment A

4.2.1 Description

Operational Environment A is generally characterized as a restrictive information processing environment in which enhanced document security, operational accountability, and information assurance are required. Typically, such systems process confidential information (e.g., personnel records, medical records, and financial information) or perform mission-critical and vital organizational functions (e.g., accounting, payroll processing, and insurance claims), and process supervisory control and data acquisition (SCADA) related documents or documents with high intellectual property value. HCDs in this environment might be targeted by third parties for exploitation, and they may be targeted by trusted parties inside the organization. This environment is not intended to support life-critical or national security applications, which are out of scope for this standard.

Operational Environment A may be appropriate for medium to large businesses, some governmental agencies, and organizations requiring tightly managed telecommuting systems and remote offices. These organizations typically have a group of IT professionals dedicated to supporting users and providing security. The combination of structure and skilled staff allows better security practices to be implemented during initial system deployment and in ongoing support and maintenance. The managed nature of typical enterprise environments gives administrators centralized control over various settings on workstations, servers, hardcopy and other types of devices, as well as the sharing of resources (e.g., file servers, printers). Environments like Operational Environment A enable only the services needed for normal business operations, with other possible avenues of exploit removed or disabled. Authentication, account, and policy management are administered centrally to maintain a consistent security posture across an organization.

This environment may include telecommuters who connect to an enterprise network from home or other remote locations and whose connection and equipment are tightly managed by the enterprise's IT department.

See Figure 2 for an infrastructure architecture typical of Operational Environment A. As an example, it would include networked printers and MFDs, managed workstations, and internal servers.

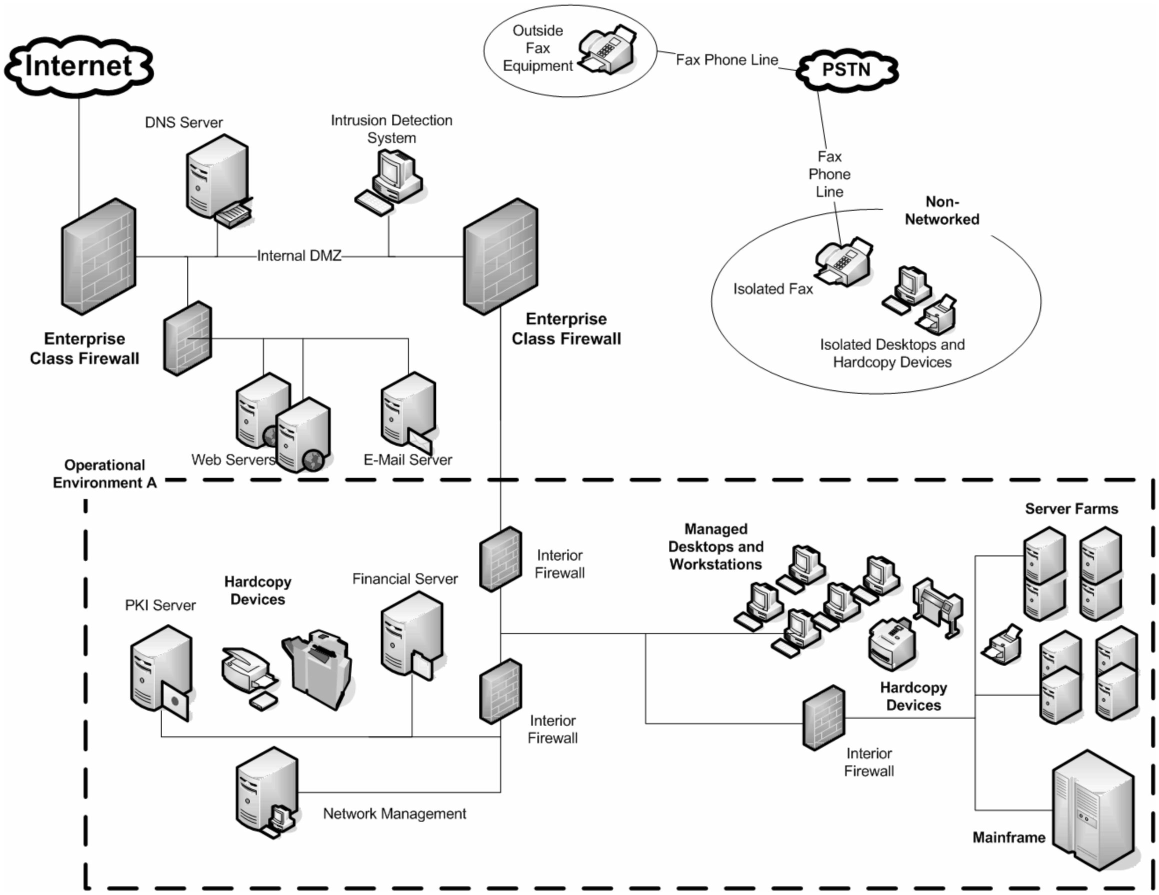

Figure 2—Operational Environment A example

Operational Environment A could also describe a subset of equipment located within another environment. For example, three desktops in a corporate enterprise that hold confidential employee data could be thought of as an Operational Environment A island within a typical enterprise (Operational Environment B) environment. Another example might include a laptop used by a mobile worker that is an Operational Environment A island within a typical small office/home office (SOHO) (Operational Environment D) environment. This environment might also be a self-contained environment outside any other environment, such as a credit card processing operation.

4.2.2 Typical security environment

Threats from insider attacks are equal to and often of greater concern than external attacks. Systems may have permanent, well-known IP addresses and name spaces with high visibility to attackers. Systems may be subject to automated intrusions and denial of service (DoS) attacks, as well as manual intrusions. Penetrations of firewalls and servers could lead to local attacks and intrusions. Local threats may be elevated if the systems are connected to large networks with many users or may be less if connected to smaller networks. Because of the risks and possible consequences of a compromise, this environment usually has the most functionally restrictive and secure configuration described in this standard. The suggested configuration provides the greatest protection with considerable tradeoffs to ease of use, functionality, and remote system management.

The following general practices and controls are likely to be found in Operational Environment A:

a) Systems generally process as few types of data as possible (i.e., do not combine multiple server applications on the same system)

b) Systems are stripped of all unnecessary services and applications

c) If possible, host-based firewall applications are used

d) Systems have as few users as possible

e) Strong authentication is used (e.g., authentication token, biometrics, smart cards)

f) Remote administration or access is restricted; if used, connections are encrypted

g) Security-related OS and application patches and updates are tested and applied as soon as possible

h) Systems are placed behind firewalls and other network security devices to restrict access and filter unnecessary protocols

i) Intrusion detection and other logs are monitored on a frequent basis

j) Vulnerability assessment tools are run against the systems on a frequent basis

k) System administrators are highly skilled in the appropriate technologies

l) Physical security is regularly assessed and updated

4.2.3 Examples

The examples that follow describe typical HCD environments that might be considered Operational Environment A.

Pharmaceutical research lab—Internet access is provided in these facilities with tightly controlled firewalls or proxies. E-mail may be provided. The research data produced, stored, and used is of high value. Internal networks may potentially be segregated from other internal networks and some of these segregated networks may not be connected to the Internet. Enhanced physical security is present. Employees may have been cleared through some screening process before given access to the high value information. Visitors are tightly controlled. There is a high potential for industrial espionage.

Bank/financial/stock broker—In this environment there is often moderate physical security and escorts are required when in the facility. There is often no Internet connection or the electronic assets may be segregated onto a private network. E-mail is provided although generally through a secure server that prevents the outflow of certain types of information and attachments. Foreign devices [personal computers (PCs), personal digital assistants (PDAs), etc.] are often not allowed on the network and a private wide area network (WAN) connection is used for electronic communication among remote offices. The assets, many individuals' private financial information, are subject to legislative privacy requirements.

Health insurance claims processing—This environment can include moderate physical security as there is little need for non-employees to be present. Outsiders can be controlled and escorted to prevent malicious acts. The IT environment may include multiple ports of electronic entry to support claim submissions from health care provides, e.g., fax, Internet, point-to-point. Funds transfer and other sensitive information will flow out of this office back to doctors, hospitals, pharmacies, and other heath care providers. Additionally, the production printing systems will generate substantial sensitive information in the form of claim acknowledgements and claim reports that will be mailed to the provider and the patient but is required to be reasonably protected before being given to the postal service. IT services are typically provided in-house or by an outsourced provider. These technicians are reasonably skilled and the network can be protected by appropriate firewalls and segmentation.

Doctor's office—The office of a one or two doctor practice is typically located in a highly accessible, small or medium office building. With the exception of certain medicines and drugs, physical security is often minimal. A third party not located in the practice often provides support for the IT equipment. The skill level of these third-party providers can vary drastically. Connectivity to the Internet for e-mail, research, and insurance claim submission may be present. In some countries, all health providers are required to safeguard patient records (HIPAA in the U.S., PHIPA in Canada, and similar legislation in other countries). Improved guidance regarding HCD threats and risks may be required for small businesses processing valuable assets in environments with minimal physical security. Products with appropriately aggressive security features should be considered despite the scale of the business.

Hospital—The facility is typically a relatively large building or campus with a large population of networked HCDs. While there is some security, visitors are everywhere and there is constant outsider interaction with administrative and medical personnel. Nursing stations may have small exposed HCDs and temporary help in the form of volunteers with access to most areas is common. IT equipment may be provided and supported by a third party but large facilities typically have their own IT staff. The security savvy of the third-party providers can vary drastically, and IT staff awareness of HCD vulnerabilities is often low. Connectivity to the Internet for e-mail, research, diagnostic test results, and insurance claim submission may be present. In most countries, all health providers are required to safeguard patient records (HIPAA in the U.S., PHIPA in Canada and similar legislation in other countries) as well as confidential patient financial information, and ID information. Also at risk is audit and record information that frequently plays a role in court cases.

Local district attorney's office—As a government office, unescorted access to public areas within these offices is required. Therefore only a moderate level of physical security can be implemented. The assets contained in this office are printed material (or electronic versions of the same) related to criminal and civil legal proceedings, which may not be public and are generally highly confidential. Public access to public records of this office via the Internet is required so Internet connections are present. Non-public document processing resources are isolated since they meet the definition of assets in need of strong protection. Firewalls and proxies are generally used. E-mail is broadly available.

Social Security office—Similar to the preceding district attorney's office, many Federal government offices and agencies like the Social Security Office are open with easy access for all people. Additionally, to communicate with their clients, employees of the office have Internet e-mail capability. Information available on the Social Security office network is highly sensitive. This information includes personal information such as the salary history used to calculate benefits. It may also include medical information such as documentation necessary to support disability claims and other similar information.

Power and light company facilities—Recent U.S. Dept. of Homeland Security (DHS) initiatives counsel commercial enterprises that manage critical infrastructure to address weak links in their networks that might enable DoS attacks and impair the network's ability to respond in a timely fashion in emergency situations. Administrative areas supporting maintenance and operation of critical power and communication systems and controlling access and personnel availability and records pertaining to support systems are all processed by HCDs. Access to outside communication networks is often controlled and network vulnerabilities that might impact availability and response times are typical concerns. Additionally, those who manage nuclear power plants have areas that are required to follow Nuclear

Regulatory Commission (NRC)/U.S. Dept. of Energy (DOE) regulations and place their HCDs in the more secure, high asset value category described by Operational Environment A. IT staff typically seeks a uniform solution for the network; however, some policies and practices throughout the network require that all assets at risk be assigned a high value given their potential public impact.

Telephone network and switch company facilities—Similarly to the power and light company facility example, commercial organizations that may not be governed by current legislation from a security perspective may place their customer base at risk through the disclosure of personal communications records documents and by not taking adequate measures to assure that their administrative systems do not pose a threat to their ability to deliver critical public communication services at all times. Network DoS attacks and unauthorized access to configuration, management, support, and service documents processed by HCDs are issues of increasing concern. HCDs used in the communications support facilities that blanket the country face threats and deal with assets typical of Operational Environment A.

SCADA systems—The preceding power and communications user examples address high profile SCADA system threats. Commercial organizations involved in major public transportation systems, delivery and transport of critical fuels, and those who manage similar networks that might have widespread public impact if directed should consider deploying hardcopy document resources that meet the Operational Environment A requirements in areas where critical control and support systems might be jeopardized.

4.2.4 General security expectations for Operational Environment A

The security related expectations of an HCD that is used in Operational Environment A are necessarily high due to the expectation that the type of information that might be processed by the HCD is of significant value to the *user* or the *user's operational environment*. Even though the physical security expectations for this environment are also high, HCDs also are expected to provide robust security functions in this environment. These expectations include the following:

- All *users* and *administrators* of the HCD are identified and authorized before being able to use or access the capabilities of the HCD. This includes accessing via any type of network or local data connections, as well as any type of user interface. Note that inbound fax connections to an HCD may not be able to completely meet this expectation due to the fact that it is, by design, an unauthenticated, anonymous data connection.
- HCDs are expected to provide protection for user's documents from unauthorized disclosure, modification, or access. This expectation extends not only to the user's document while it is being processed or stored within the HCD, but also any electronic transmission of an authorized user's document to or from the HCD. Additionally, certain information about the user's document or the processing of that document, e.g., number of copies, duplex, color settings, is expected to be protected from unauthorized modification while both stored and in transit.
- HCDs are expected to provide protections against the disclosure of residual user document information that may reside in the HCD after the processing of that user document is completed.
- HCDs are expected to provide protection for any internal HCD configuration parameters, settings, logs, or other HCD specific security related information from unauthorized modification (and unauthorized access for certain types of security related information and logs). This expectation extends to any transmission of this information to or from the HCD as well as while it is resident in the HCD.
- HCDs are expected to provide protection for any internal HCD software, firmware, or other digital resources (e.g., downloadable fonts, images, forms) from unauthorized alteration (including deletion), while resident in the HCD.
- HCDs are expected to monitor and record, via protected logs, any security relevant events that occur within the HCD. Examples of these types of events might include: successful and

unsuccessful authentication attempts, changes in security relevant settings on the HCD, or changes in the content or state of the HCD's internal security or accounting logs.

— HCDs are expected to monitor and record, via protected logs, any use of HCD functions. Examples of these types of events might include: printing a document, scanning a document, receipt of a fax, etc.

— HCDs are expected to participate in networked and other shared-medium environments in a robust and orderly manner. This expectation includes resilience in the face of network-based DoS attacks as well providing mechanisms that reduce the likelihood that the HCD will interfere or obstruct the function of the network or other networked devices.

4.3 Operational Environment B

4.3.1 Description

Operational Environment B is generally characterized as an information processing environment in which a moderate level of document security, network security, and security assurance are required. Typically, this environment will handle the day-to-day proprietary and non-proprietary information needed to operate an enterprise. Figure 3 shows an example network architecture typical of Operational Environment B, which includes networked printers and MFDs, managed workstations, and internal servers.

Operational Environment B may be appropriate for medium to large businesses, some governmental agencies, and organizations requiring managed telecommuting systems and remote offices. These organizations typically have a group of IT professionals dedicated to supporting users and providing security. The combination of structure and skilled staff allows better security practices to be implemented during initial system deployment and in ongoing support and maintenance. The managed nature of typical enterprise environments gives administrators centralized control over various settings on workstations, servers, hardcopy and other types of devices, as well as the sharing of resources (e.g., file servers, printers). Environments like Operational Environment B enable only the services needed for normal business operations, with other possible avenues of exploit removed or disabled. Authentication, account, and policy management can also be administered centrally to maintain a consistent security posture across an organization. This environment includes telecommuters who connect to an enterprise network from home or other remote locations and whose connection and equipment are managed by the enterprise's IT department.

Environments described in this subclause may have a mixture of operational environments. It is common to have *islands* within all of the environments described that contain assets of high value and HCDs that process critical information requiring Operational Environment A precautions. The example in Figure 4 suggests an office such as a personnel department, a legal department, a research and development office, or a corporate executive office that require a higher degree of isolation and access control within a corporate enterprise typical of Operational Environment B. Islands of this type frequently have increased physical security restricting office access or building access. Also shown is a secured home office; this is an example of an Operational Environment A installation in a location that might usually be Operational Environment D.

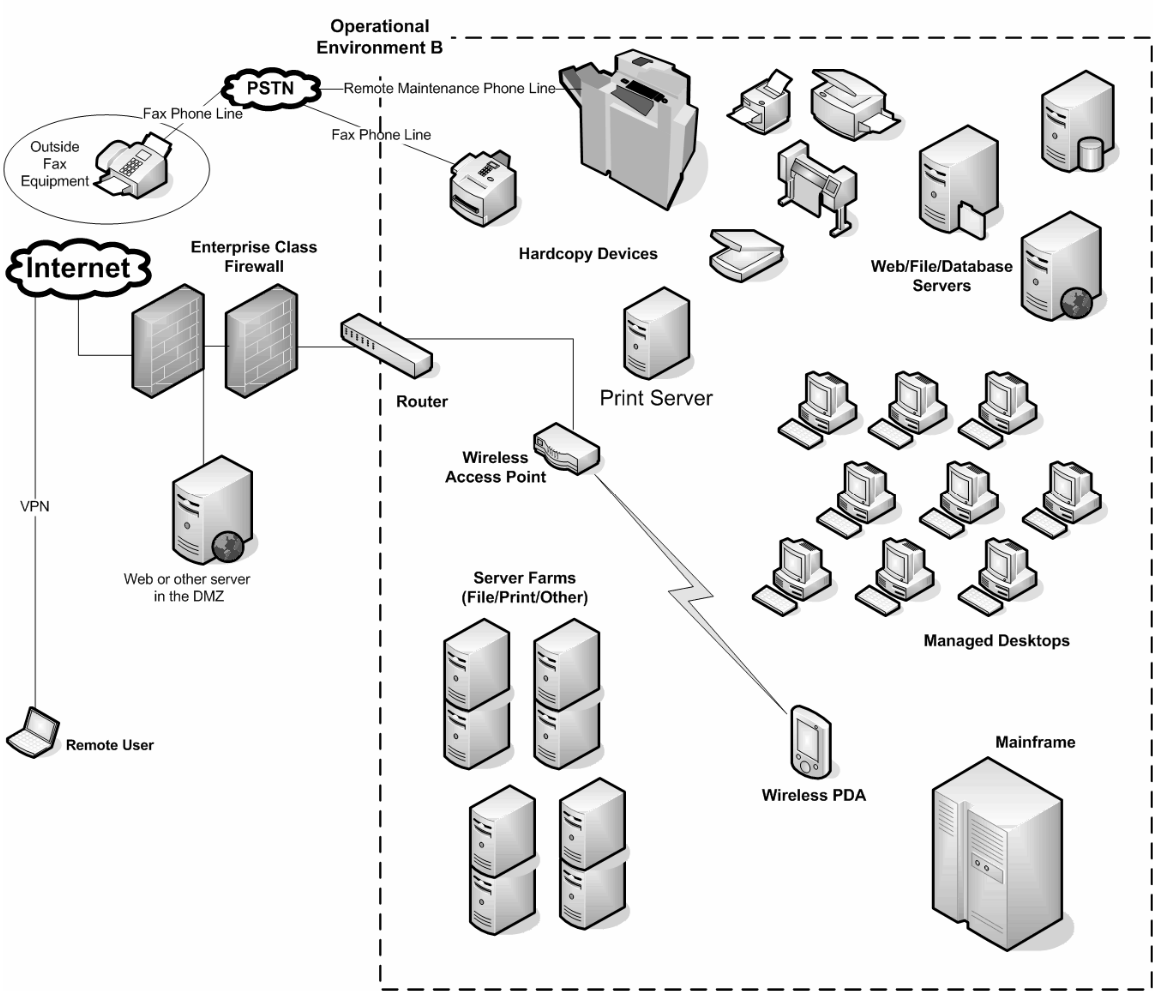

Figure 3—Operational Environment B example

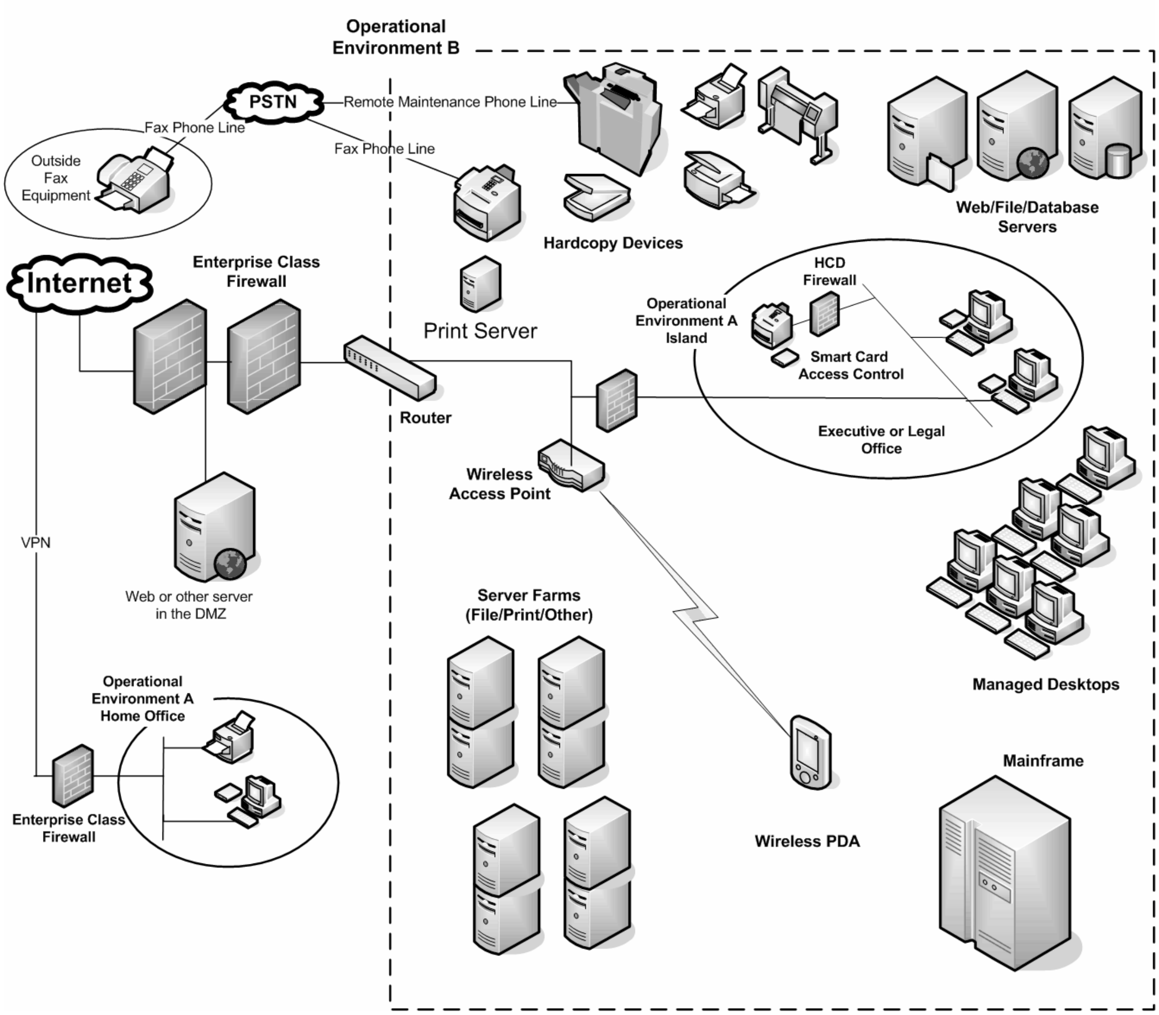
Operational Environment B
PSTN
Remote Maintenance Phone Line
Fax Phone Line
Fax Phone Line
Outside Fax Equipment
Hardcopy Devices
Web/File/Database Servers
Internet
Enterprise Class Firewall
Print Server
HCD Firewall
Operational Environment A Island
Smart Card Access Control
Router
Executive or Legal Office
Wireless Access Point
VPN
Web or other server in the DMZ
Server Farms (File/Print/Other)
Managed Desktops
Operational Environment A Home Office
Mainframe
Enterprise Class Firewall
Wireless PDA

Figure 4—Centrally managed Operational Environment B with Environment A islands

4.3.2 Typical security environment

Systems in this environment face many of the same threats as systems in Operational Environment A. Remote and local threats to Operational Environment B networks could have significant impacts to systems and applications. Enterprise organizations often have systems and devices with permanent, well-known IP addresses and name spaces with high visibility on the Internet to attackers. Most systems on enterprise networks are usually inward-facing—protected from direct exposure to the Internet by firewalls—but penetrations of those systems through other means could permit intruder access to internal networks. For example, viruses and worms could spread across homogenous networks in a short amount of time. Also, in these environments, the insider threat is generally greater due to the larger number of users and lower strength of authentication than one finds in Operational Environment A.

In environments like Operational Environment B, systems are typically susceptible to both local and remote threats. Local attacks, such as unauthorized usage of another department's workstations or HCDs, can often lead to unauthorized access to data, but may also lead to unauthorized data modification or consumption of resources. Remote threats may be posed not only by attackers outside the organization, but also by local users who are attacking other local systems from within the organization's network. Most security breaches caused by remote threats involve malicious payloads sent by external parties, such as viruses and worms acquired via e-mail or infected Web sites. Threats against network-based applications tend to affect a smaller number of systems and may be caused by internal or external parties. Both malicious payloads and network application attacks are most likely to affect availability (e.g., crashing the system or device, consuming all network bandwidth, breaking functionality) but may also affect integrity (e.g., infecting data files) or confidentiality (e.g., providing remote access to sensitive data). Data disclosure threats tend to come from internal parties who are monitoring traffic on local networks, and they primarily affect confidentiality.

Some commonly accepted security practices found in Operational Environment B are as follows:

a) Internal networks are segmented with internal firewalls and other defense-in-depth techniques

b) System management is centralized with restricted access to management functions

c) Security-related applications (e.g., antivirus) are centrally managed

d) Installation of system and application patches and updates is automated

e) Access to printer and MFDs and their features is restricted, and accounting features are enabled

f) Unnecessary ports and protocols are disabled

g) Backup and recovery facilities are centralized

4.3.3 Examples

The examples that follow describe typical HCD environments that might be considered Operational Environment B.

High-tech international company—Product plans, company intellectual property, printing, and scanning of documents to and from overseas manufacturing and support groups requires an increased focus on the security of document handling resources. Enterprise networks today link global sites and create new opportunities for attacks. Increased use of outsourced personnel with limited background data also raises the threat of internal attacks. While islands in large enterprises justify the use of Operational Environment A, the baseline for every large corporation with considerable assets at risk is Operational Environment B, which is intended to provide security recommendations applicable to all corporate enterprises with tangible assets.

Advertising agency/PR agency/photographic studios—Promotional and advertising companies today can be large global operations with numerous high profile clients. Typically, confidential information associated with product and events not yet disclosed to the public that might have significant financial repercussions are disclosed in detail to these organizations. Specifications are copied and product information printed, scanned, and exchanged with project teams. Corporate project teams in foreign locations review and exchange hardcopy materials associated with the products and projects. Industrial, corporate, and international espionage threats can be mitigated by prudent and more secure use of office resources such as the HCDs that process all the documents at risk.

Cable television company—Broadcast media companies have also become communication companies providing two-way data services and even audio-video services over their networks. Client financial information and access information for thousands of subscribers may be processed by office HCDs. Care should be taken to eliminate the possibility of remote access to the office document handling systems since the cable network itself will likely have a large number of sophisticated potential attackers linked to the servers providing public access. Personally identifiable information providing access to Internet-based services may be at risk.

Large retail firm—Retail operations today frequently provide their own credit services and manage a large database of customer personal and financial Information. This is especially true of companies dealing with larger, frequently financed items such as furniture outlets and large electronics retailers. Customer financial information is frequently processed by the company hardcopy resources that have the potential to put client information at risk.

College campus—The college campus environment is a special case of Operational Environment B and includes broad access to and from the Internet; however, there are several unique differences. First, because of academic freedom issues, there tends to be less content filtering and other protections in use. Students and staff need to be able to accomplish a wide range of tasks that are difficult to characterize and therefore configuration of protection devices and systems have to allow for a broad range of usage. Second, due to the age and maturity levels of some college students, the campus IT environment is often viewed as a challenge. These students are often very motivated insider attackers who constantly search for systems to compromise. A college's HCDs may be accessible to a large number of unscreened individuals in work-study programs and other volunteer work.

4.3.4 General security expectations for Operational Environment B

Although not as high as the expectations for Operational Environment A, the security related expectations of an HCD in Operational Environment B still require the HCD to provide a robust level of security for the types of information being processed. These expectations include the following:

- All users and administrators of the HCD are identified and authorized before being able to use or access the capabilities of the HCD. This includes accessing via any type of network or local data connections, as well as any type of user interface. Note that inbound fax connections to an HCD may not be able to completely meet this expectation due to the fact that it is, by design, an unauthenticated, anonymous data connection.
- HCDs are expected to provide protection for user's documents from unauthorized disclosure, modification, or access while it is being processed or stored within the HCD. Additionally, certain information about the user's document or the processing of that document, e.g., number of copies, duplex, color settings, is expected to be protected from unauthorized modification while stored in the HCD.
- HCDs are expected to provide protections against the disclosure of residual user document information that may reside in the HCD after the processing of that user document is completed.
- HCDs are expected to provide protection for any internal HCD configuration parameters, settings, logs, or other HCD specific security related information from unauthorized modification (and unauthorized access for certain types of security related information and logs). This expectation extends to any transmission of this information to or from the HCD as well as while it is resident in the HCD.
- HCDs are expected to provide protection for any internal HCD software, firmware, or other digital resources (e.g., downloadable fonts, images, forms) from unauthorized alteration (including deletion), while resident in the HCD.
- HCDs are expected to monitor and record, via protected logs, any security relevant events that occur within the HCD. Examples of these types of events might include: successful and unsuccessful authentication attempts, changes in security relevant settings on the HCD, or changes in the content or state of the HCD's internal security or accounting logs.
- HCDs are expected to monitor and record, via protected logs, any use of HCD functions. Examples of these types of events might include: printing a document, scanning a document, receipt of a fax, etc.

- HCDs are expected to participate in networked and other shared-medium environments in a robust and orderly manner. This expectation includes resilience in the face of network-based DoS attacks as well providing mechanisms that reduce the likelihood that the HCD will interfere or obstruct the function of the network or other networked devices.

4.4 Operational Environment C

Operational Environment C is generally characterized as a public-facing environment in which document security is not guaranteed, but access control and usage accounting are important to the operator of the environment. A retail copy center, public library, Internet café, and hotel business center are typical examples of this environment.

4.4.1 Typical environment

These organizations typically have a group of IT professionals dedicated to supporting users and providing security. The combination of structure and skilled staff allows better security practices to be implemented during initial system deployment and in ongoing support and maintenance. The managed nature of these environments gives administrators centralized control over various settings on workstations, servers, hardcopy and other types of devices, as well as the sharing of resources (e.g., file servers, printers). Environments like Operational Environment C should enable only the services needed for normal business operations, with other possible avenues of exploit removed or disabled. Authentication, account, and policy management can also be administered centrally to maintain a consistent security posture across an organization. This environment does not typically include telecommuters who connect to an enterprise network from home or other non-business remote locations.

The typical Operational Environment C environment is a business or public sector operation that provides some combination of wired and wireless Internet connectivity, desktop computers, and HCDs, for general use by transient patrons, members, customers who pay a service rental fee, or the general public. This environment is likely to have some or all of the following characteristics:

a) Due to its public nature, it is difficult to provide physical security.

b) Since the users of these services are transient, it is impractical to manage user identities and accountability in the way one would in Operational Environment A or B.

c) There may be requirements that usage is granted to those who have some kind of permission, that device and security settings are controlled, and for which resource usage is accounted.

d) This environment may also have some connection to a more controlled environment that manages access control, performs billing functions, supplies read-only access to databases, or performs other functions.

e) There may be a high risk of, and associated controls for, local injection of viruses or worms and other uses that violate terms of service.

f) Because of its public nature, the typical instance of Operational Environment C may not assure any kind of document security. However, its operator may wish to add value by providing some level of document security and should therefore consider adopting some of the security objectives of Operational Environment B.

4.4.2 Examples

The examples that follow describe typical HCD environments that might be considered Operational Environment C.

Public library—One example of Operational Environment C is a public library, as shown in Figure 5. Patrons in the public library are able to use the public computers as well as the public copiers, printers, and scanners. This is public space with no physical security during business hours. Internet access and e-mail are often available both to the public and to the employees. Libraries are not liable for disclosure of copied, scanned, or printed content. Accurate charge-back and payment information is required to recover the costs of fair use duplication of material. No credit card information is retained by the HCD after a transaction.

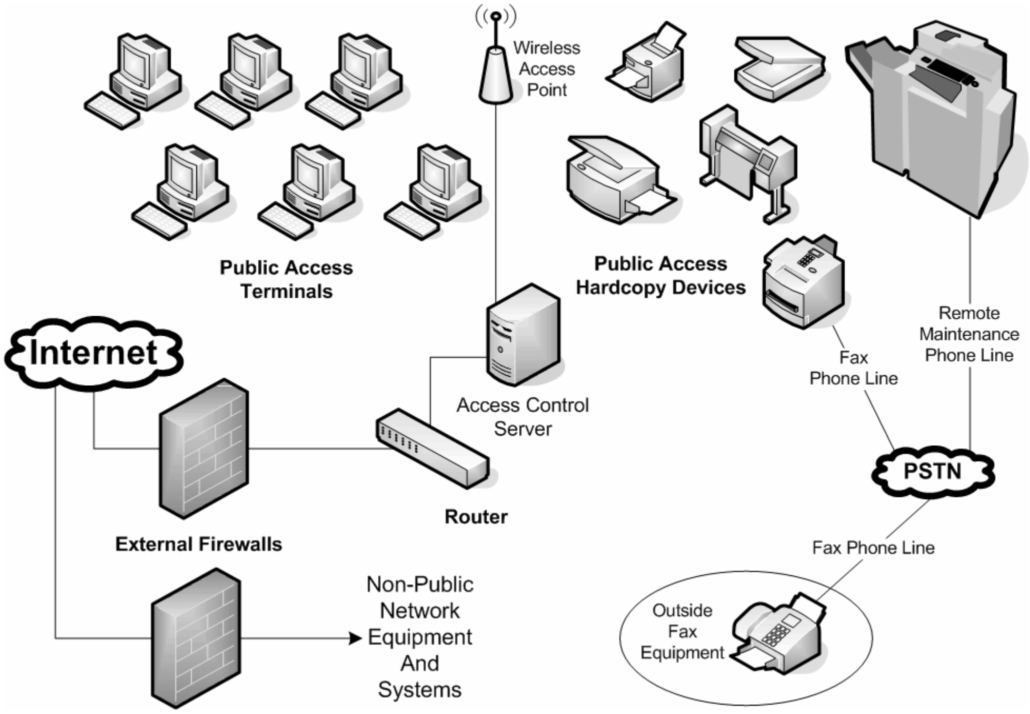

Figure 5—Operational Environment C example—public library

Hotel business center—Many large hotel chains provide visitor access to HCDs with print, copy, fax, and scan capabilities. Some provide remote access from hotel rooms to these resources. Typical users are business travelers with the need to process hardcopy based information that might be confidential company information or personal information.

Retail copy shop or Internet café—This is intended to be used by the public; therefore no physical security is present during business hours. Wireless Internet access may be provided to patrons for a nominal fee or no fee. PCs and HCDs with wired access may also be provided. The business' operations network (non-public) will be segregated or firewalled from the public network. Credit card information is present on the operation's network but not generally through any HCD. The openness of these environments suggests that they are high risk with minimal security. Deployment of security tools typical of, for example, Operational Environment A would constrain user access and is generally not feasible: user caution is advised.

4.4.3 General security expectations for Operational Environment C

The security related expectations of an HCD in Operational Environment C focus on the integrity and security of the configuration and function of the machine and not necessarily the security of the information being processed by the HCD. This narrowing of expectations centers on the fact that this environment is focused on publicly accessible and publicly used HCDs where a user should not expect robust protection of the information being processed. These expectations include the following:

- All administrators of the HCD are identified and authorized before being able to access the administrator functions of the HCD. This includes accessing via any type of network or local data connections, as well as any type of user interface.
- HCDs are expected to provide protections against the disclosure of residual user document information that may reside in the HCD after the processing of that user document is completed.
- HCDs are expected to provide protection for any internal HCD configuration parameters, settings, logs, or other HCD specific security related information from unauthorized modification (and unauthorized access for certain types of security related information and logs). This expectation extends to any transmission of this information to or from the HCD as well as while it is resident in the HCD.
- HCDs are expected to provide protection for any internal HCD software, firmware, or other digital resources (e.g., downloadable fonts, images, forms) from unauthorized alteration (including deletion), while resident in the HCD.
- HCDs are expected to monitor and record, via protected logs, any security relevant events that occur within the HCD. Examples of these types of events might include: successful and unsuccessful authentication attempts, changes in security relevant settings on the HCD, or changes in the content or state of the HCD's internal security or accounting logs.
- HCDs are expected to participate in networked and other shared-medium environments in a robust and orderly manner. This expectation includes resilience in the face of network-based DoS attacks as well providing mechanisms that reduce the likelihood that the HCD will interfere or obstruct the function of the network or other networked devices.

4.5 Operational Environment D

4.5.1 Description

Operational Environment D is generally characterized by a small, private information processing environment in which many elements of security are provided by the physical environment. Some level of network security is needed to protect the device and its network from misuse originating outside of the environment. Small offices and home offices are typical examples of this environment. Figure 6 shows a typical Operational Environment D environment.

The following are typical characteristics of the target end-user audiences and configurations:

a) Home users with stand-alone systems, generally with dial-up or high-speed access to the Internet, possibly using wired or wireless home networks, possibly sharing resources across the networks.

b) Telecommuters using stand-alone systems who work from a home office but who are not operating under the control of an enterprise IT department, i.e., not Operational Environment A or B islands.

c) Small businesses, typically with small networks of stand-alone desktop systems and small office servers, protected from direct Internet access by a firewall, but possibly including some small centrally managed networks of desktop systems and products, and typically not maintaining publicly accessible servers.

d) HCDs may be directly connected using IEEE 1284, Universal Serial Bus (USB), or other local connectivity, to desktop computers, general purpose servers, or print servers. Devices connected to one system can be shared with other systems. In some environments, these HCDs are directly connected to the network using Ethernet, IEEE 802.11, HomePNA™,[8] or similar networking technologies.

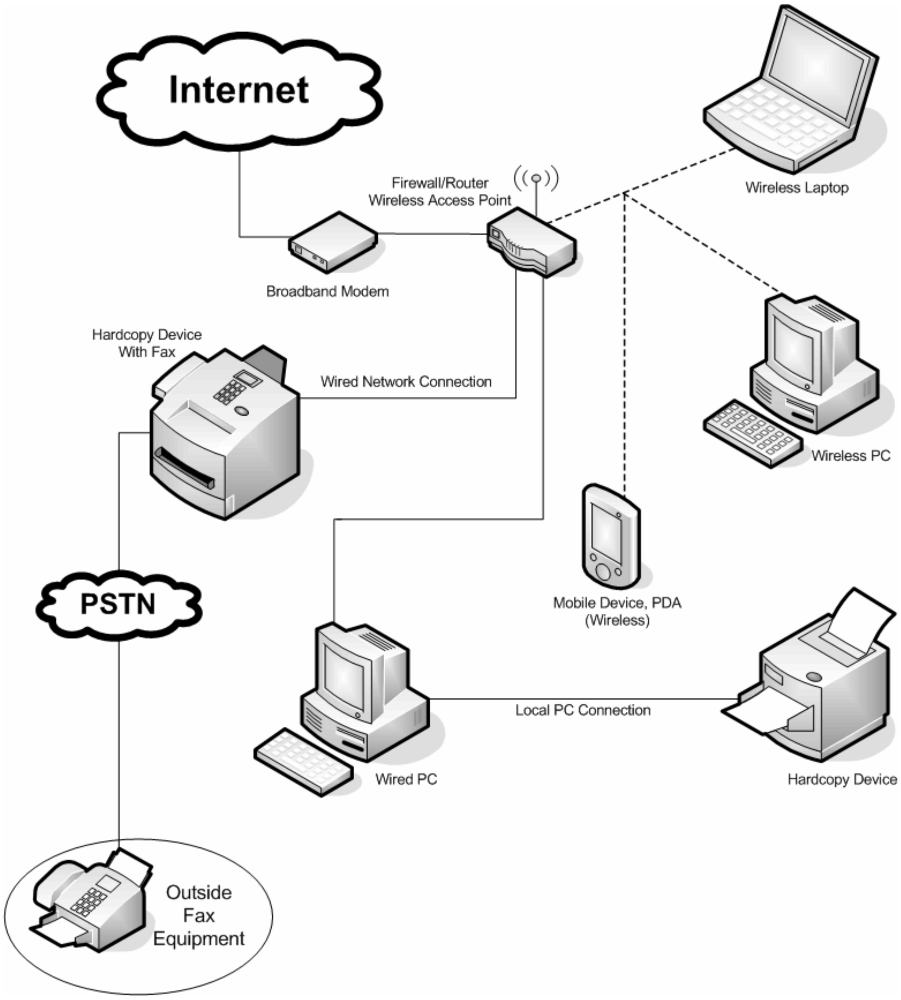

Figure 6—Operational Environment D example

4.5.2 Typical security environment

Operational Environment D is typically the least secured of the environments considered in this standard. The individuals performing small office or home office system administration are assumed to be less knowledgeable about security than enterprise system administrators. This often results in environments that

[8] HomePNA is a trademark of the HomePNA Alliance [B32]. This information is given for the convenience of users of this standard and does not constitute an endorsement by the IEEE of these products. Equivalent products may be used if they can be shown to lead to the same results...

are less secure than they should be because the system administrator's focus is on functionality. There may be no network-based security controls such as firewalls, or those present may be out-of-date or ineffective, thereby directly exposing the network and devices to external attacks. These environments are frequently targeted for exploitation to acquire information through keystroke logging or other phishing methods, to perform distributed DoS attacks on other computers, to deliver spam e-mail messages, or to propagate viruses or worms. Systems in this environment may themselves be infected by viruses or worms, or suffer collateral damage resulting from malicious software installation and use.

Because the primary threats in this environment are external, and the HCD devices deployed generally have less restrictive security policies than those in Operational Environment A or B, they tend to be most vulnerable to attacks from remote threat categories. Local threats are often less significant because few people typically have local access to personal or small business systems; however, it is still important to protect against local and other threats. Systems for Operational Environment D are typically exposed to attacks against network services and by malicious payloads (e.g., viruses, worms). These attacks are most likely to affect availability (e.g., crashing the system, consuming all network bandwidth, breaking functionality) but may also affect integrity (e.g., infecting data files) and confidentiality (e.g., providing remote access to sensitive data, e-mailing data files to others).

Operational Environment D networks often have the following characteristics:

a) Consumer-class hardware Internet firewall appliances are used to block inbound connections and possibly to also filter outbound traffic.

b) Some systems may have host-based firewalls.

c) Computers are likely to have antivirus software and possibly anti-spyware software. The engines and definition files associated with these programs may be out-of-date.

d) There may be a mixture of OSs present; including some that may be no longer supported with security updates. OS updates or patches, if available, may not necessarily be applied in a timely fashion.

e) Systems are likely to be left in their out-of-box configuration, which can mean that unnecessary applications, services, and protocols remain enabled and not configured beyond their original state.

f) Network encryption is seldom used.

g) Wireless LANs may be unsecured, may use older, less secure protocols, may use weak keys, or may use default configurations that can easily be compromised.

h) User accounts, if used at all, may have weak or no password protection.

i) Shared resources are likely to have few access controls.

4.5.3 Examples

The examples that follow describe typical HCD environments that might be considered Operational Environment D.

Real estate broker—These are generally in small-to-medium office buildings located in highly accessible locations. There is no substantial physical security. E-mail and Web access are required and often with only minimal firewalls on the Internet connection. The susceptible assets are generally land and building contracts and other agreements. Some may have accounting considerations. Few, if any, legislative privacy or other controls are required or observed.

Architect's office—These offices are generally in small-to-medium office buildings with no substantial physical security. Internet access and e-mail are available often with only minimal firewalls on the Internet connection. The susceptible assets usually do not include private information but do include business information such as cost estimates, schedules, plans and drawings, supplier and contractor contact information, customer lists, and other confidential business information.

Home—Only trivial physical security, such as door locks, is present. The assets could be confidential and consist of personal and financial information. Internet access and e-mail are commonly present through dial-up or increasingly through always-on broadband connections. Wireless networks are increasingly common and often not protected with WEP, WPA, IEEE 802.11i™, or any other security techniques. Firewalls and proxies are often not present. There are no legislative mandates to protect one's own information from attack.

4.5.4 General security expectations for Operational Environment D

The security related expectations of an HCD in Operational Environment D focus on the integrity and security of the configuration and function of the machine and not the security of the information being processed by the HCD. These expectations include the following:

- All administrators of the HCD are identified and authorized before being able to access the administrator functions of the HCD. This includes accessing via any type of network or local data connections, as well as any type of user interface.
- HCDs are expected to provide protection for any internal HCD configuration parameters, settings, or other HCD specific security related information from unauthorized modification (and unauthorized access for certain types of security related information) while stored in the HCD or in transit.
- HCDs are expected to provide reasonable protection for any internal HCD software or firmware from unauthorized alteration while resident in the HCD. At a minimum, the HCD is expected is indicate to the administrator or user that change has occurred.
- HCDs are expected to participate in networked and other shared-medium environments in a reasonably robust and orderly manner. This expectation includes providing at least minimal protections that reduce the likelihood that the HCD will interfere or obstruct the function of the network or other networked devices.

4.6 Choosing the most applicable operational environment

When choosing the most applicable environment to use as a guide for particular security needs, the reader should look beyond the simple description of the environment and instead consider both the totality of the operational environment and the value of the most valuable assets to be protected. Table 1 summarizes those factors for each environment.

Table 1—Factors affecting security

	Effect on security requirements			
Operational Environment	**A**	**B**	**C**	**D**
Element of security				
Value of asset	High	Moderate	Moderate–Low	Low
Physical security	High	Moderate	Low	Low
Network protection	High	Moderate	Moderate	Low
Laws and regulations (see Note)	High	Moderate–Low	Low	Low
Personnel trust	High	Moderate	Low	Low
NOTE—Laws and regulations include privacy and governance laws, industry-specific standards, etc.				

Here are some examples of how an appropriate operational environment might be chosen:

Home appliance service company—This business typically has a network of computers to run their operation, which includes taking orders, dispatching trucks, general bookkeeping, and providing access to service documentation. Operational Environment B is the most applicable environment description. However, a few of the company's routine functions involve private information such as credit card processing for customers and payroll and health insurance records for its employees. Systems that perform those functions are likely to be regulated by laws and would therefore need to be considered as Operational Environment B with islands of Operational Environment A.

Publicly traded pharmaceutical manufacturer—This business performs many functions that are regulated or involve highly valuable competitive information. For example, their bookkeeping is regulated by governance laws, their clinical trial data is regulated by privacy laws, and their research and patent data is so valued that its disclosure could result in the loss of significant future revenue. All of these activities would clearly require the precautions typical of Operational Environment A. However, there are many other functions in the company that are not regulated nor involve trade secrets. For example, they have an in-house corporate travel service, cafeteria food service for employees, fleet management for company vehicles, and a worldwide distribution center.

Home user—A typical home network often consists of two desktop computers and an HCD, which is connected via USB to one of the computers but its use is shared. Such a home network is often connected to the Internet by a combined DSL modem, firewall, and wireless access point. This environment is typical of Operational Environment D. However, one of the family members uses their laptop computer at home to connect to their employer's corporate network so that they can work at home on product launch plans for the aforementioned pharmaceutical company. The laptop, the wireless connection, and the HCD and its host computer would need to be able to operate as an Operational Environment A island within this typical Operational Environment D environment.

5. Hardcopy device assets

5.1 Overview

In this clause, HCD assets are defined and their relative importance in each operational environment is discussed.

5.2 HCD asset definitions

5.2.1 User Document Data

Minimally, the HCD processes User Document Data. User Document Data consists of all the information in the users' documents processed by the HCD, including the original hardcopy media being scanned or copied, electronic files to be printed, image data from scanning or fax, printed hardcopy output, and deliberately or residually stored data in hard disks or other memory devices.

5.2.2 User Function Data

Depending on the function and design of a particular device, an HCD may also have User Function Data. User Function Data consists of the information about the job that is to be processed. This information includes job instructions and job status.

5.2.3 HCD Protected Data

HCD Protected Data is information for which alteration by a user who is neither an administrator nor the owner of the data would have an adverse effect on the operational security of the HCD, but for which disclosure is acceptable. It may be stored in flash memory, on an HDD, or by using other means. Examples of HCD Protected Data include the following:

a) HCD device job and usage logs, scan and fax address books, and device configuration

b) Network management data such as IP addresses

c) An HCD's digital resources and other resident data that is not necessarily part of User Document Data or HCD software such as fonts or stored forms

5.2.4 HCD Confidential Data

HCD Confidential Data is information for which either disclosure or alteration by a user who is neither an administrator nor the owner of the data would have an adverse effect on the operational security of the HCD. It may be stored in flash memory, on an HDD, or by using other means. Examples of HCD Confidential Data include the following:

a) User and administrator passwords

b) Device management data such as security event audit log data

5.2.5 HCD Physical Resources

An HCD's *physical resources* include components of the HCD and consumable items such as paper, ink, and toner.

5.2.6 HCD Availability

The ability to use the HCD can be considered an asset. In some operational environments, it is important to ensure that authorized users have timely access to the HCD. In other environments, it is important to prevent unauthorized users from using the HCD.

5.2.7 Software

The software that controls the function of the HCD is an asset that typically has two forms: *firmware* and *applets*.

5.2.7.1 Firmware

Firmware is any persistent instructions and data in the HCD that provides basic functions of the HCD, is developed by the manufacturer, is embedded in the device, and is infrequently updated.

5.2.7.2 Applets

Applets are HCD application software designed to be executed from within another application that provide additional capabilities for customer- or industry-specific purposes, sometimes developed by the customer or a third party, and possibly installed on demand.

5.2.8 External Environment

Although not part of the HCD itself, the External Environment consists of other IT equipment that is interconnected or interoperates with the HCD and can be threatened by certain kinds of exploits against the HCD. However, exploits against external IT devices that might threaten the HCD are beyond the scope of this standard.

5.3 Asset values in the operational environments

Based on the operational environment descriptions in Clause 4, Table 2 lists the relative value or importance of HCD asset categories in each of the environments:

Table 2—Asset values in each operational environment

Asset Operational environment	User Document Data	User Function Data	HCD Protected Data	HCD Confidential Data	HCD Physical Resources	HCD Availability	Software	External Environment
A	High	High	High	High	Low	Moderate	High	Moderate
B	Moderate	Moderate	Moderate	High	Moderate	Moderate	Moderate	Moderate
C	Low	Low	Moderate	High	High	High	Moderate	Moderate
D	Low	Low	Low	High	Moderate	Moderate	Low	Low

6. Hardcopy device threats

6.1 Overview

This clause defines the various threats to an HCD's assets that were defined in Clause 5. This is done by defining a threat vector for HCDs that accounts for threats related to any entry point of an HCD that might provide access to the HCD assets.

Each threat is given a risk rating for each of the four environments that are defined in this standard. These ratings are listed in Table 52 in 6.4.

6.1.1 Threat ID naming convention

While there is nothing special about the particular ID names that are given to each threat, the threat IDs were created using the following general rules:

a) Each threat ID begins with the letter T.

b) The next portion of the ID relates to the asset being attacked. (e.g., T.DOC.xxx is a threat to the User Document Data asset)

c) The remaining portions of the ID tag relate to the general access or attack method and the resulting effect of the threat. (e.g., T.DOC.TRANSIT.DIS is a threat that the User Document Data asset while in transit to or from the HCD on a shared communications media will be disclosed to an unauthorized person.)

This naming convention is aligned with the example threat ID naming used in ISO/IEC TR 15446:2004 [B70].

6.2 Threat summaries

Table 4 lists the threat identifiers or names, a short description for each threat, and a reference to the full vector description.

Table 3—HCD threat summaries

Threat ID	Description	Vector
T.CONSUMABLES.EXHAUST	An HCD’s consumable items may be intentionally exhausted as a result of jobs being submitted by unauthorized persons.	Table 20
T.CONSUMABLES.THEFT	An HCD’s consumable items may be intentionally removed by unauthorized persons.	Table 19
T.CONF.CAMERA.DIS	HCD Confidential Data may be disclosed to unauthorized persons by capturing this data with an external camera as it is entered into the HCD.	Table 38
T.CONF.GUESS.DIS	HCD Confidential Data may be disclosed to unauthorized persons by guessing or by observing the data as it is entered into the HCD.	Table 39
T.CONF.REST.ALT	HCD Confidential Data in the HCD may be altered by unauthorized persons.	Table 40
T.CONF.REST.DIS	HCD Confidential Data in the HCD may be disclosed to unauthorized persons.	Table 41
T.CONF.TRANSIT.ALT	HCD Confidential Data in transit over a shared communications medium may be altered by unauthorized persons.	Table 42
T.CONF.TRANSIT.DIS	HCD Confidential Data in transit over a shared communications medium may be disclosed to unauthorized persons.	Table 43
T.CONF.TRANSIT.EM.DIS	HCD Confidential Data in transit over a shared communications medium may be disclosed to unauthorized persons by capturing the EM radiation from the communication medium.	Table 44
T.DOC.ANALYZE.DIS	User Document Data may be disclosed to unauthorized persons by using an electron microscope or other equipment to read residual image on copier belt or drum.	Table 21
T.DOC.CAMERA.DIS	User Document Data may be disclosed to unauthorized persons by capturing this data with a hidden camera as it is processed by the HCD.	Table 22
T.DOC.DELETED.SAL	Deleted User Document Data in a nonvolatile storage medium that has been removed from the HCD may be salvaged by unauthorized persons.	Table 23
T.DOC.EM.DIS	User Document Data may be disclosed to unauthorized persons by capturing EM radiation from HCD.	Table 24
T.DOC.FAX.ALT	User Document Data may be altered by unauthorized persons via a man-in-the-middle attack on the PSTN interface.	Table 25
T.DOC.FAX.DIS	User Document Data may be disclosed to unauthorized persons by tapping into a phone line to sniff fax traffic on the PSTN interface.	Table 26
T.DOC.INPUT.DIS	User Document Data may be disclosed to unauthorized persons by examining the document while in the original document handler or removing the document from the original document handler.	Table 27
T.DOC.OUTPUT.DIS	User Document Data may be sent to the output handler and disclosed to unauthorized persons.	Table 28
T.DOC.RETRIEVE.ALT	User Document Data that are retrievable from the HCD may be altered by unauthorized persons.	Table 29
T.DOC.RETRIEVE.DIS	User Document Data that are retrievable from the HCD may be disclosed to unauthorized persons.	Table 30
T.DOC.REST.SAL	User Document Data in a nonvolatile storage medium that has been removed from the HCD may be salvaged by unauthorized persons.	Table 31
T.DOC.TRANSIT.ALT	User Document Data in transit over a shared communications medium may be altered by unauthorized persons.	Table 32

Table 3—HCD threat summaries (continued)

T.DOC.TRANSIT.EM.DIS	User Document Data in transit over a shared communications medium may be disclosed to unauthorized persons by capturing EM radiation from the communication medium.	Table 33
T.DOC.TRANSIT.DIS	User Document Data in transit over a shared communications medium may be disclosed to unauthorized persons.	Table 34
T.DOS.FAX.HOOK	HCD Availability may be interrupted by unauthorized persons by inserting an off-hook telephone in the fax line to prevent incoming or outgoing faxes.	Table 5
T.DOS.FAX.LOOP	HCD Availability may be interrupted by unauthorized persons by continuously sending grayscale fax pages at low speed to or from the HCD.	Table 6
T.DOS.FAX.TRAIN	HCD Availability may be interrupted by unauthorized persons by generating an incoming fax connection that forces the fax modem to continuously train (negotiate fax connection parameters).	Table 7
T.DOS.FAX.VOLUME	HCD Availability may be interrupted by unauthorized persons by continuously sending excessive scanned document volume to the HCD to prevent its normal use.	Table 8
T.DOS.HCD.ALTER	HCD Availability may be interrupted by unauthorized persons by mechanically or electrically altering or damaging the HCD or its components.	Table 9
T.DOS.HCD.INTERFERE	HCD Availability may be interrupted by unauthorized persons by mechanically or electrically interfering with the HCD or its components.	Table 10
T.DOS.PRT.CHANNEL	HCD Availability may be interrupted by unauthorized persons by submitting page description language (PDL) or print protocol data to generate a back-channel message flood.	Table 11
T.DOS.PRT.CRASH	HCD Availability may be interrupted by unauthorized persons by submitting PDL or print protocol data to cause print controller failure or code execution loop.	Table 12
T.DOS.PRT.PRIORTY	HCD Availability may be interrupted by unauthorized persons by intentionally, continuously sending print jobs that de-prioritize other types of jobs.	Table 13
T.DOS.SMI.CONNECT	HCD Availability may be interrupted by unauthorized persons by opening all available connections on a shared communication media and keeping them open to prevent legitimate connections.	Table 14
T.DOS.SMI.CRAFT	HCD Availability may be interrupted by unauthorized persons by sending crafted packets over the shared communication media to cause interface crash or failure.	Table 15
T.DOS.SMI.FLOOD	HCD Availability may be interrupted by unauthorized persons by flooding packets over the shared communication media to cause a sustained interface interruption or failure.	Table 16
T.ENV.DOS	The External Environment may be interrupted by unauthorized persons by creating a DoS attack on the local network using the HCD’s interface.	Table 49
T.ENV.FAXBRIDGE	The External Environment or the HCD’s internal components and software may be accessed by unauthorized persons via the fax connection.	Table 50
T.ENV.PROXY.DOS	The External Environment may be interrupted by unauthorized persons by propagating an attack to the local network through a network service on the HCD.	Table 51
T.FUNC.REST.ALT	User Function Data in the HCD may be altered by unauthorized persons.	Table 35
T.FUNC.TRANSIT.ALT	User Function Data in transit over a shared communications medium may be altered by unauthorized persons.	Table 36
T.FUNC.TRANSIT.DIS	User Function Data in transit over a shared communications medium may be disclosed to unauthorized persons.	Table 37

Table 3—HCD threat summaries (continued)

T.HCD.AVAIL.COPY	HCD Availability may be misappropriated to unauthorized persons by using a rogue copy control device to bypass copy control or accounting.	Table 17
T.HCD.AVAIL.BYPASS	HCD Availability may be misappropriated to unauthorized persons by circumventing HCD security or accounting controls.	Table 18
T.PROT.TRANSIT.ALT	HCD Protected Data in transit over a shared communications medium may be altered by unauthorized persons.	Table 46
T.PROT.REST.ALT	HCD Protected Data in the HCD may be altered by unauthorized persons.	Table 45
T.SW.APPLET.ALT	HCD software applets in the HCD may be altered by unauthorized persons.	Table 47
T.SW.FIRMWARE.ALT	HCD firmware in the HCD may be altered by unauthorized persons.	Table 48

6.3 Threat vectors and descriptions

6.3.1 Threat vector model

Details of the threats summarized in the previous subclause are contained in 6.3.2 and are described in terms of a threat vector model that generally follows the threat profile structure used in the OCTAVE approach for information security risk evaluation [B105]. Each threat vector is modeled according to the vector definitions listed in Table 4.

Table 4—Threat vector definitions

Vector category	Vector subcategory	Description
Asset	**User Document Data**	Information that is part of the user's document being processed by the HCD (see 5.2.1, also 2.2).
	User Function Data	Information that is about the user's job or document (see 5.2.2, also 2.2).
	HCD Confidential Data	Security relevant information that is disclosed only to administrators (see 5.2.4).
	HCD Protected Data	Security relevant information that is altered only by administrators (see 5.2.3).
	HCD Physical Resources	Physical resources or consumables used by the HCD (see 5.2.5).
	HCD Availability	The use of or the capability to use the HCD (see 5.2.6).
	Software	The underlying control software of the HCD (see 5.2.7).
	External Environment	Includes other networked devices that are external to the HCD (see 5.2.8).
Actor	**Anonymous**	Machine or person, may be anonymous.
	Authorized	Machine or person, authorized for some degree of HCD use.
	Present (physically)	Physical attack that requires the presence of the attacker during the attack.
	Remote (physically)	Physical attack that may be remotely operated.
Skill	**Layman**	An attacker with no previous or specialized training relating to the execution of the attack.
	Proficient	An attacker with general knowledge regarding the execution of an attack.
	Expert	An attacker with very specific, specialized training or knowledge that is directly related to the execution of an attack
Equipment	**Standard**	Equipment that is generally available to the public [e.g., a personal computer (PC)]
	Specialized	Equipment that is not generally available to the public and may require some specialization to use (e.g., a network packet sniffer or a PC with specialized program).
	Bespoke	Equipment that is specially designed to perform a specific attack (e.g., an EMI receiver that decodes laser emissions).
Access	**Network**	Access to the HCD over a shared communication media (e.g., Ethernet, Token Ring, wireless).
	Local	Access to the HCD over a local port or connection [e.g., parallel, serial, USB, compact flash (CF) card.]
	Physical	Physical access to the device
	Telephone	Access to the HCD over the public telephone network.
Outcome	**Interruption**	Loss of availability
	Corruption	Loss of integrity
	Disclosure	Loss of confidentiality
	Loss (theft) of service	Unauthorized use
	Loss (theft) of resource	Unauthorized removal of supplies, etc.
Impact	**Direct**	The result of a successful attack directly threatens the specified assets.
	Indirect	The result of a successful attack indirectly provides opportunity to directly threaten the specified assets.
Manufacturers observe	Symptoms of the attack that an HCD manufacturer may experience.	
IT providers observe	Symptoms of the attack that the HCD's IT provider may experience.	
Users observe	Symptoms of the attack that an HCD's user may experience	

6.3.2 Threat descriptions

This subclause contains the descriptions, a possible threat scenario, and threat vector for each threat. Each entry also includes a list of what manufacturers, IT providers, and users might see as an indication of an attack related to the threat, as well as references to the best practices and mitigation techniques for the threat in Clause 7.

6.3.2.1 Threats to HCD Availability

Table 5—T.DOS.FAX.HOOK

Threat ID:	**T.DOS.FAX.HOOK**	
Threat description:	HCD Availability may be interrupted by unauthorized persons by inserting an off-hook telephone in the fax line to prevent incoming or outgoing faxes.	
Threat vector:	**Asset:**	HCD Availability
	Actor:	Present
	Skill:	Layman or higher
	Equipment:	Standard
	Access:	Telephone, physical
	Outcome:	Interruption
	Impact:	Direct
Threat scenario:	An attacker can effect denial of PSTN fax service by inserting an off-hook telephone or a device that simulates an off-hook telephone on the telephone circuit, either within the physical facility or on the outside of the facility.	
Manufacturers observe:	Nothing abnormal	
IT providers observe:	Nothing abnormal	
Users observe:	Inability to send or receive faxes, HCD indicates that its fax connection is busy	
Mitigation techniques:	See 7.1.1	

Table 6—T.DOS.FAX.LOOP

Threat ID:	**T.DOS.FAX.LOOP**	
Threat description:	HCD Availability may be interrupted by unauthorized persons by continuously sending grayscale fax pages at low speed to or from the HCD.	
Threat vector:	**Asset:**	HCD Availability
	Actor:	Anonymous, present
	Skill:	Layman or higher
	Equipment:	Standard
	Access:	Telephone, physical
	Outcome:	Interruption
	Impact:	Direct
Threat scenario:	An attacker can effect denial of PSTN fax service by continuously transmitting at low speed pages filled with a grayscale fax pattern that is may not be efficiently compressible. The HCD can be either the sender or receiver of the transmission.	
Manufacturers observe:	Nothing abnormal	
IT providers observe:	High usage metrics in the logs (or higher connection charges) for the fax connection or help desk complaints about the availability of the fax function	
Users observe:	Inability to use the fax function due to its unavailability	
Mitigation techniques:	See 7.1.2	

Table 7—T.DOS.FAX.TRAIN

Threat ID:	**T.DOS.FAX.TRAIN**	
Threat description:	HCD Availability may be interrupted by unauthorized persons by generating an incoming fax connection that forces the fax modem to continuously train (negotiate fax connection parameters).	
Threat vector:	**Asset:**	HCD Availability
	Actor:	Anonymous
	Skill:	Expert
	Equipment:	Standard (with specialized software)
	Access:	Telephone
	Outcome:	Interruption
	Impact:	Direct
Threat scenario:	An attacker can effect denial of the fax service by using a customized fax modem on a device on the external PSTN network that forces the HCD's fax modem to continuously negotiate and then renegotiate the fax connection parameters without ever completing the negotiation.	
Manufacturers observe:	Service calls relating to the HCD's fax connection not being able to complete negotiation	
IT providers observe:	High usage time in the logs that does not correlate with the number of faxes sent or received	
Users observe:	Inability to use the fax function due to its unavailability	
Mitigation techniques:	See 7.1.3	

Table 8—T.DOS.FAX.VOLUME

Threat ID:	**T.DOS.FAX.VOLUME**	
Threat description:	HCD Availability may be interrupted by unauthorized persons by continuously sending excessive scanned document volume to the HCD to prevent its normal use.	
Threat vector:	**Asset:**	HCD Availability
	Actor:	Anonymous
	Skill:	Layman or higher
	Equipment:	Standard
	Access:	Physical
	Outcome:	Interruption
	Impact:	Direct
Threat scenario:	An attacker can effect denial of fax service by continuously transmitting a large volume of scanned documents or a loop of paper taped or glued together. The documents can be transmitted either from the HCD or from an external fax modem.	
Manufacturers observe:	Nothing abnormal	
IT providers observe:	High usage metrics in the logs, excessive usage of consumables	
Users observe:	Inability to use the fax function due to its unavailability	
Mitigation techniques:	See 7.1.4	

Table 9—T.DOS.HCD.ALTER

Threat ID:	**T.DOS.HCD.ALTER**	
Threat description:	HCD Availability may be interrupted by unauthorized persons by mechanically or electrically altering or damaging the HCD or its components.	
Threat vector:	**Asset:**	HCD Availability, HCD Physical Resources
	Actor:	Present
	Skill:	Layman or higher
	Equipment:	Standard
	Access:	Physical
	Outcome:	Interruption
	Impact:	Direct
Threat scenario:	An attacker can damage or alter the various electronic or mechanical parts of the HCD making it unavailable for further use.	
Manufacturers observe:	Nothing abnormal	
IT providers observe:	Help desk calls relating to the non-functioning, broken HCD, resulting physical evidence of the damage	
Users observe:	Inability to use the HCD	
Mitigation techniques:	See 7.1.5	

Table 10—T.DOS.HCD.INTERFERE

Threat ID:	**T.DOS.HCD.INTERFERE**	
Threat description:	HCD Availability may be interrupted by unauthorized persons by mechanically or electrically interfering with the HCD or its components.	
Threat vector:	**Asset:**	HCD Availability
	Actor:	Present
	Skill:	Proficient or higher
	Equipment:	Standard
	Access:	Physical
	Outcome:	Interruption
	Impact:	Direct or indirect
Threat scenario:	An attacker can interfere with the various electronic or mechanical parts of the HCD, making it unavailable for further usage. The interference can be caused by introducing an external agent into the system, so that it affects the normal functioning of the electronic or the mechanical parts, or by external EM interference.	
Manufacturers observe:	Nothing abnormal	
IT providers observe:	Help desk calls relating to the non-functioning, broken HCD, resulting physical evidence of the alteration	
Users observe:	Inability to use the HCD	
Mitigation techniques:	See 7.1.6	

Table 11 —T.DOS.PRT.CHANNEL

Threat ID:	**T.DOS.PRT.CHANNEL**	
Threat description:	HCD Availability may be interrupted by unauthorized persons by submitting PDL or print protocol data to generate a back-channel message flood.	
Threat vector:	**Asset:**	HCD Availability, External Environment
	Actor:	Authorized
	Skill:	Proficient or higher
	Equipment:	Standard
	Access:	Network, local
	Outcome:	Interruption
	Impact:	Direct
Threat scenario:	An attacker can effect denial of print service by submitting PDL or print protocol data to induce a flood of back-channel notification messages back to the originating computer. This flood may induce a denial or degradation of service condition on the HCD, on the originating computer, on the network at large, or all three.	
Manufacturers observe:	Service calls relating to the HCD corrupting the network	
IT providers observe:	Help desk calls relating to the HCD being unavailable over the network or increases in network traffic on the HCD's subnet	
Users observe:	Sluggish or complete loss of access to the HCD via the network connection	
Mitigation techniques:	See 7.1.7	
NOTE—Print data may be submitted over a bidirectional network connection (Ethernet, Token Ring, IEEE 802.11, Bluetooth, etc.) or through a bidirectional local connection (enhanced parallel, serial, USB).		

Table 12 —T.DOS.PRT.CRASH

Threat ID:	**T.DOS.PRT.CRASH**	
Threat description:	HCD Availability may be interrupted by unauthorized persons by submitting PDL or print protocol data to cause print controller failure or code execution loop.	
Threat vector:	**Asset:**	HCD Availability
	Actor:	Authorized
	Skill:	Proficient or higher
	Equipment:	Standard
	Access:	Network, local
	Outcome:	Interruption
	Impact:	Direct
Threat scenario:	An attacker can effect denial of print service by submitting PDL or print protocol data to induce either an unrecoverable print controller failure or print controller looping, through either standard PDL constructs such as Postscript looping, or through crafted, malformed data that induces a controller failure.	
Manufacturers observe:	Service calls for the HCD repeatedly crashing or hanging	
IT providers observe:	Help desk calls relating to the HCD being unavailable	
Users observe:	Inability to use the HCD over the network or other data ports	
Mitigation techniques:	See 7.1.8	
NOTE—Print data may be submitted over a network connection (Ethernet, Token Ring, IEEE 802.11, Bluetooth, etc.) or through a local connection (parallel, serial, USB).		

Table 13—T.DOS.PRT.PRIORITY

Threat ID:	**T.DOS.PRT.PRIORITY**	
Threat description:	HCD Availability may be interrupted by unauthorized persons by intentionally, continuously sending print jobs that de-prioritize other types of jobs.	
Threat vector:	**Asset:**	HCD Availability
	Actor:	Authorized
	Skill:	Proficient or higher
	Equipment:	Standard
	Access:	Network, local
	Outcome:	Interruption
	Impact:	Direct
Threat scenario:	An attacker can effect denial of non-print services by submitting PDL or print protocol data that claims a higher priority than walk-up copy, scan, or print jobs. If combined with a looping threat (T.DOS.PRT.CRASH) this threat can induce persistent inability to access walk-up functions on the HCD.	
Manufacturers observe:	Nothing abnormal	
IT providers observe:	Help desk calls regarding the continual or overuse of the HCD making it unavailable or unexpected log entries	
Users observe:	Unable to use the walk-up features of the HCD due to availability issues	
Mitigation techniques:	See 7.1.9	
NOTE—Print data may be submitted over a bidirectional network connection (Ethernet, Token Ring, IEEE 802.11, Bluetooth, etc.) or through a bidirectional local connection (enhanced parallel, serial, USB).		

Table 14—T.DOS.SMI.CONNECT

Threat ID:	**T.DOS.SMI.CONNECT**	
Threat description:	HCD Availability may be interrupted by unauthorized persons by opening all available connections on a shared communication media and keeping them open to prevent legitimate connections.	
Threat vector:	**Asset:**	HCD Availability
	Actor:	Anonymous
	Skill:	Proficient or higher
	Equipment:	Standard
	Access:	Network
	Outcome:	Interruption
	Impact:	Direct
Threat scenario:	An attacker can effect DoS by opening a sufficiently large number of concurrent TCP connections, either to a specific port or to the device in general, to exhaust available network resources and prevent further connections. This threat includes opening many connections to conduct various protocol and application-level negotiations (e.g., RFC 2703 [B129]). This threat is generic to all networked devices.	
Manufacturers observe:	Service calls for the HCD relating to not functioning via the network connection	
IT providers observe:	Help desk calls relating to the HCD being unavailable over the network	
Users observe:	Inability to use the HCD over the network connection	
Mitigation techniques:	See 7.1.10	

Table 15—T.DOS.SMI.CRAFT

Threat ID:	**T.DOS.SMI.CRAFT**	
Threat description:	HCD Availability may be interrupted by unauthorized persons by sending crafted packets over the shared communication media to cause interface crash or failure.	
Threat vector:	**Asset:**	HCD Availability
	Actor:	Anonymous
	Skill:	Expert
	Equipment:	Standard
	Access:	Network
	Outcome:	Interruption
	Impact:	Direct
Threat scenario:	An attacker can effect DoS by transmitting crafted TCP (or other) packets that cause the HCD's TCP/IP (or other transport-level) stack to fail, including the crafting of application-level protocol packets. This threat is generic to all networked devices.	
Manufacturers observe:	Service calls for the HCD relating to not functioning via the network connection	
IT providers observe:	Help desk calls relating to the HCD being unavailable over the network	
Users observe:	Inability to use the HCD over the network connection	
Mitigation techniques:	See 7.1.11	

Table 16—T.DOS.SMI.FLOOD

Threat ID:	**T.DOS.SMI.FLOOD**	
Threat description:	HCD Availability may be interrupted by unauthorized persons by flooding packets over the shared communication media to cause a sustained interface interruption or failure.	
Threat vector:	**Asset:**	HCD Availability
	Actor:	Anonymous
	Skill:	Proficient or higher
	Equipment:	Standard
	Access:	Network
	Outcome:	Interruption
	Impact:	Direct
Threat scenario:	An attacker can effect DoS by transmitting high volumes of network data packets—such as, but not limited to, ICMP or UDP packets—to the HCD in order to cause the device's TCP/IP (or other transport-level) stack to fail. This threat is generic to all networked devices.	
Manufacturers observe:	Service calls relating to poor network performance of the HCD	
IT providers observe:	Help desk calls relating to the HCD being unavailable over the network or increases in network traffic on the HCD's subnet	
Users observe:	Sluggish or complete loss of access to the HCD via the network connection	
Mitigation techniques:	See 7.1.12	

Table 17 —T.HCD.AVAIL.COPY

Threat ID:	**T.HCD.AVAIL.COPY**	
Threat description:	HCD Availability may be misappropriated by using rogue copy control devices. This will allow unauthorized persons to bypass copy control or accounting mechanisms.	
Threat vector:	**Asset:**	HCD Availability, HCD Physical Resources
	Actor:	Present
	Skill:	Proficient or higher
	Equipment:	Standard
	Access:	Physical, network
	Outcome:	Loss (theft) of service
	Impact:	Direct
Threat scenario:	An attacker can steal HCD services by installing a rogue copy control device (e.g., click counter plug-in) to bypass existing electromechanical or software copy control mechanism. Copy control devices can potentially control access to other HCD services.	
Manufacturers observe:	Nothing abnormal	
IT providers observe:	High usage metrics in the logs or excessive consumables use that does not correlate with the accounting logs	
Users observe:	Nothing abnormal	
Mitigation techniques:	See 7.1.13	

Table 18 —T.HCD.AVAIL.BYPASS

Threat ID:	**T.HCD.AVAIL.BYPASS**	
Threat description:	HCD Availability may be misappropriated by circumventing normal HCD security or accounting controls.	
Threat vector:	**Asset:**	HCD Availability, HCD Physical Resources
	Actor:	Anonymous, present
	Skill:	Layman or higher
	Equipment:	Standard
	Access:	Network, local, physical
	Outcome:	Loss (theft) of service, loss (theft) of resource
	Impact:	Direct
Threat scenario:	An attacker can steal HCD services by using a peer-to-peer connection to circumvent server security or accounting, such as by printing directly to the HCD's IP address or connecting to its local ports (e.g., parallel, serial, USB)	
Manufacturers observe:	Nothing abnormal	
IT providers observe:	High usage metrics in the logs or excessive consumables use that doesn't correlate with the accounting logs	
Users observe:	Nothing abnormal	
Mitigation techniques:	See 7.1.14	

6.3.2.2 Threats to HCD Physical Resources

Table 19 —T.CONSUMABLES.THEFT

Threat ID:	**T.CONSUMABLES.THEFT**	
Threat description:	An HCD’s consumable items may be intentionally removed by unauthorized persons.	
Threat vector:	**Asset:**	HCD Physical Resources, HCD Availability
	Actor:	Present
	Skill:	Layman or higher
	Equipment:	None
	Access:	Physical
	Outcome:	Interruption, loss (theft) of resource
	Impact:	Direct
Threat scenario:	An attacker can remove the required supplies like toner, paper, etc., making the HCD unavailable for further use.	
Manufacturers observe:	Nothing abnormal	
IT providers observe:	Help desk calls relating to the HCD not functioning or missing consumables	
Users observe:	Inability to use the HCD	
Mitigation techniques:	See 7.2.1	

Table 20 —T.CONSUMABLES.EXHAUST

Threat ID:	**T.CONSUMABLES.EXHAUST**	
Threat description:	An HCD’s consumable items may be intentionally exhausted as a result of jobs being submitted by unauthorized persons.	
Threat vector:	**Asset:**	HCD Physical Resources, HCD Availability
	Actor:	Authorized
	Skill:	Layman or higher
	Equipment:	None
	Access:	Network, local
	Outcome:	Interruption, loss (theft) of resource
	Impact:	Direct
Threat scenario:	An attacker can create print jobs that result in the increased use of expensive consumables and supplies like color toner or ink, photo paper, etc., increasing the cost of ownership as well as effecting the availability of the HCD.	
Manufacturers observe:	Nothing abnormal	
IT providers observe:	Higher than expected cost of ownership metrics or unexpected log entries	
Users observe:	Inability to use the HCD due to exhausted consumables	
Mitigation techniques:	See 7.2.2	

6.3.2.3 Threats to HCD User Document and User Function Data assets

Table 21 —T.DOC.ANALYZE.DIS

Threat ID:	**T.DOC.ANALYZE.DIS**	
Threat description:	User Document Data may be disclosed to unauthorized persons by using an electron microscope or other equipment to read residual image on copier belt or drum.	
Threat vector:	**Asset:**	User Document Data
	Actor:	Present
	Skill:	Expert
	Equipment:	Specialized
	Access:	Physical
	Outcome:	Disclosure
	Impact:	Direct
Threat scenario:	Attacker can remove the HCD's drum or belt and use an electron microscope or other equipment to determine the contents of recently printed or copied documents.	
Manufacturers observe:	Nothing abnormal	
IT providers observe:	The absence of the belt or drum component if the attacker did not return or replace	
Users observe:	Possible inability to use the HCD	
Mitigation techniques:	See 7.3.1	

Table 22 —T.DOC.CAMERA.DIS

Threat ID:	**T.DOC.CAMERA.DIS**	
Threat description:	User Document Data may be disclosed to unauthorized persons by capturing this data with a hidden camera as it is processed by the HCD.	
Threat vector:	**Asset:**	User Document Data, HCD Confidential Data
	Actor:	Remote
	Skill:	Proficient or higher
	Equipment:	Specialized
	Access:	Physical proximity
	Outcome:	Disclosure
	Impact:	Direct
Threat scenario:	An attacker can use a digital or film camera, hidden either inside or outside the HCD, to record (1) copied or scanned document pages as they are scanned on the glass, (2) copied or scanned documents as they are fed in from the document input feeder, or (3) copied or printed documents as they are dropped in the output tray.	
Manufacturers observe:	Nothing abnormal	
IT providers observe:	Nothing abnormal	
Users observe:	Nothing abnormal	
Mitigation techniques:	See 7.3.2	

Table 23—T.DOC.DELETED.SAL

Threat ID:	**T.DOC.DELETED.SAL**	
Threat description:	Deleted User Document Data in a nonvolatile storage medium that has been removed from the HCD may be salvaged by unauthorized persons.	
Threat vector:	**Asset:**	User Document Data
	Actor:	Present
	Skill:	Proficient or higher
	Equipment:	Standard to bespoke
	Access:	Physical
	Outcome:	Disclosure
	Impact:	Direct
Threat scenario:	Attacker can remove an HCD's hard disk or other persistent storage device and attach it to either another similar device or to a computer system to read the contents of documents stored on the disk. If the data has been erased by simple methods, the attacker can use an unerase utility, otherwise use specialized equipment to determine the pattern of data written and overwritten on the hard disk material and recover the erased or stored data.	
Manufacturers observe:	Nothing abnormal	
IT providers observe:	May notice the removal or loss of the drive	
Users observe:	May notice the removal or loss of the drive or a loss of performance if the HCD uses the drive for document spooling	
Mitigation techniques:	See 7.3.3	

Table 24—T.DOC.EM.DIS

Threat ID:	**T.DOC.EM.DIS**	
Threat description:	User Document Data may be disclosed to unauthorized persons by capturing EM radiation from HCD.	
Threat vector:	**Asset:**	User Document Data
	Actor:	Remote
	Skill:	Expert
	Equipment:	Bespoke
	Access:	Physical (close proximity but not direct access)
	Outcome:	Disclosure
	Impact:	Direct
Threat scenario:	An attacker can monitor (sniff) EM emissions from the HCD's electronic components such as the laser or print head and recreate documents being printed.	
Manufacturers observe:	Nothing abnormal	
IT providers observe:	Nothing abnormal	
Users observe:	Nothing abnormal	
Mitigation techniques:	See 7.3.4	
NOTE—Requires proximity to the HCD but not direct physical access.		

Table 25—T.DOC.FAX.ALT

Threat ID:	**T.DOC.FAX.ALT**	
Threat description:	User Document Data may be altered by unauthorized persons via a man-in-the-middle attack on the PSTN interface.	
Threat vector:	**Asset:**	User Document Data
	Actor:	Anonymous
	Skill:	Proficient or higher
	Equipment:	Standard
	Access:	Phone line
	Outcome:	Corruption, disclosure
	Impact:	Direct, indirect
Threat scenario:	Attacker can intercept the faxed content being transmitted between the sender and the receiver, modify the content of the fax, and then send it to the original destination fax machine. This threat encompasses disclosure, alteration, and deletion of user documents by way of a man-in-the-middle attack.	
Manufacturers observe:	Nothing abnormal	
IT providers observe:	Nothing abnormal	
Users observe:	User may notice that the faxes were not received if the attack resulted in the deletion of the User Document Data	
Mitigation techniques:	See 7.3.5	

Table 26—T.DOC.FAX.DIS

Threat ID:	**T.DOC.FAX.DIS**	
Threat description:	User Document Data may be disclosed to unauthorized persons by tapping into a phone line to sniff fax traffic on the PSTN interface.	
Threat vector:	**Asset:**	User Document Data
	Actor:	Remote
	Skill:	Expert
	Equipment:	Specialized
	Access:	Telephone
	Outcome:	Disclosure
	Impact:	Direct
Threat scenario:	An attacker can use a phone tap to monitor (sniff) fax traffic to discover the contents of fax transmitted or received faxes.	
Manufacturers observe:	Nothing abnormal	
IT providers observe:	Nothing abnormal	
Users observe:	Nothing abnormal	
Mitigation techniques:	See 7.3.6	

Table 27—T.DOC.INPUT.DIS

Threat ID:	**T.DOC.INPUT.DIS**	
Threat description:	User Document Data may be disclosed to unauthorized persons by examining the document while in the original document handler or removing the document from the original document handler.	
Threat vector:	**Asset:**	User Document Data
	Actor:	Present
	Skill:	Layman or higher
	Equipment:	None
	Access:	Physical
	Outcome:	Disclosure
	Impact:	Direct
Threat scenario:	An attacker can pick up other users' scanned or copied document originals or examine their contents from the HCD's original document handler.	
Manufacturers observe:	Nothing abnormal	
IT providers observe:	Nothing abnormal	
Users observe:	User may detect the loss of the original input document	
Mitigation techniques:	See 7.3.7	

Table 28—T.DOC.OUTPUT.DIS

Threat ID:	**T.DOC.OUTPUT.DIS**	
Threat description:	User Document Data may be sent to the output handler and disclosed to unauthorized persons.	
Threat vector:	**Asset:**	User Document Data
	Actor:	Present
	Skill:	Layman or higher
	Equipment:	None
	Access:	Physical
	Outcome:	Disclosure
	Impact:	Direct
Threat scenario:	An attacker can pick up other user's printed or copied documents or examine their contents from the HCD output tray.	
Manufacturers observe:	Service calls relating to the HCD not performing some print or copy functions	
IT providers observe:	Help desk calls related to the HCD not performing the intended print or copy function for certain users	
Users observe:	The HCD doesn't appear to have performed its print or copy job with no status indicating an error	
Mitigation techniques:	See 7.3.8	

Table 29 —T.DOC.RETRIEVE.ALT

Threat ID:	**T.DOC.RETRIEVE.ALT**	
Threat description:	User Document Data that are retrievable from the HCD may be altered by unauthorized persons.	
Threat vector:	**Asset:**	User Document Data
	Actor:	Anonymous, remote
	Skill:	Proficient or higher
	Equipment:	None
	Access:	Physical, local, network
	Outcome:	Disclosure
	Impact:	Direct
Threat scenario:	An attacker can modify or delete another user’s document data from the internal document or raster image processor (RIP) server, print queue, or proof print queue by device’s using the HCD’s stored document management interface.	
Manufacturers observe:	Nothing abnormal	
IT providers observe:	Possible unexpected log entries	
Users observe:	Nothing abnormal	
Mitigation techniques:	See 7.3.9	

Table 30 —T.DOC.RETRIEVE.DIS

Threat ID:	**T.DOC.RETRIEVE.DIS**	
Threat description:	User Document Data that are retrievable from the HCD may be disclosed to unauthorized persons.	
Threat vector:	**Asset:**	User Document Data
	Actor:	Authorized, present
	Skill:	Layman or higher
	Equipment:	None
	Access:	Physical, network
	Outcome:	Disclosure
	Impact:	Direct
Threat scenario:	An attacker can access another user’s document data from the internal document or RIP server, print queue, or proof print queue. For example using a reprint function to reprint another user’s job.	
Manufacturers observe:	Nothing abnormal	
IT providers observe:	Possible unexpected log entries	
Users observe:	Nothing abnormal	
Mitigation techniques:	See 7.3.10	

Table 31—T.DOC.REST.SAL

Threat ID:	**T.DOC.REST.SAL**	
Threat description:	User Document Data in a nonvolatile storage medium that has been removed from the HCD may be salvaged by unauthorized persons.	
Threat vector:	**Asset:**	User Document Data
	Actor:	Anonymous, present
	Skill:	Proficient or higher
	Equipment:	Standard
	Access:	Physical
	Outcome:	Disclosure
	Impact:	Direct
Threat scenario:	An attacker can access another user's document data from the internal document or RIP server, print queue, or proof print queue by temporarily removing the HCD's HDD and reading the contents of the disk on another machine.	
Manufacturers observe:	Nothing abnormal	
IT providers observe:	Possible help desk calls relating to the HCD document store function not working.	
Users observe:	Nothing abnormal	
Mitigation techniques:	See 7.3.11	

Table 32—T.DOC.TRANSIT.ALT

Threat ID:	**T.DOC.TRANSIT.ALT**	
Threat description:	User Document Data in transit over a shared communications medium may be altered by unauthorized persons.	
Threat vector:	**Asset:**	User Document Data
	Actor:	Anonymous
	Skill:	Proficient or higher
	Equipment:	Standard
	Access:	Network
	Outcome:	Corruption, disclosure
	Impact:	Direct, indirect
Threat scenario:	An attacker can intercept a print or scan job being transmitted over the network, change the content of the job, and then forward to the recipient. This threat encompasses disclosure, alteration, and deletion of user documents by way of a man-in-the-middle attack.	
Manufacturers observe:	Nothing abnormal	
IT providers observe:	Nothing abnormal	
Users observe:	User may notice that the documents were not printed or scanned correctly if the attack resulted in the deletion of the User Document Data or that the resulting information has been altered	
Mitigation techniques:	See 7.3.12	

Table 33—T.DOC.TRANSIT.EM.DIS

Threat ID:	**T.DOC.TRANSIT.EM.DIS**	
Threat description:	User Document Data in transit over a shared communications medium may be disclosed to unauthorized persons by capturing EM radiation from the communication medium.	
Threat vector:	**Asset:**	User Document Data
	Actor:	Remote
	Skill:	Expert
	Equipment:	Bespoke
	Access:	Physical (close proximity but not direct access)
	Outcome:	Disclosure
	Impact:	Direct
Threat scenario:	An attacker can monitor (sniff) EM emissions from the network wiring with specialized sniffing tools to discover contents of documents being printed, scanned, or network faxed.	
Manufacturers observe:	Nothing abnormal	
IT providers observe:	Nothing abnormal	
Users observe:	Nothing abnormal	
Mitigation techniques:	See 7.3.13	
NOTE—Requires proximity to the device or to the network wiring but not a physical connection to the network.		

Table 34—T.DOC.TRANSIT.DIS

Threat ID:	**T.DOC.TRANSIT.DIS**	
Threat description:	User Document Data in transit over a shared communications medium may be disclosed to unauthorized persons.	
Threat vector:	**Asset:**	User Document Data
	Actor:	Anonymous
	Skill:	Proficient or higher
	Equipment:	Standard (with specialized software)
	Access:	Network
	Outcome:	Disclosure
	Impact:	Direct
Threat scenario:	An attacker can monitor (sniff) network traffic with standard network sniffing tools to discover contents of documents being printed, scanned, or network faxed.	
Manufacturers observe:	Nothing abnormal	
IT providers observe:	Nothing abnormal	
Users observe:	Nothing abnormal	
Mitigation techniques:	See 7.3.14	
NOTE—Requires access to the network traffic, whether through a wired (e.g., Ethernet) or wireless connection.		

Table 35—T.FUNC.REST.ALT

Threat ID:	**T.FUNC.REST.ALT**	
Threat description:	User Function Data in the HCD may be altered by unauthorized persons.	
Threat vector:	**Asset:**	User Function Data
	Actor:	Anonymous, remote
	Skill:	Proficient or higher
	Equipment:	None
	Access:	Physical, local, network
	Outcome:	Corruption
	Impact:	Direct
Threat scenario:	An attacker can modify information about or instructions for processing another user's documents that is stored on the HCD from the HCD's document or job management user interfaces.	
Manufacturers observe:	Nothing abnormal	
IT providers observe:	Possible unexpected log entries	
Users observe:	Nothing abnormal	
Mitigation techniques:	See 7.3.15	

Table 36—T.FUNC.TRANSIT.ALT

Threat ID:	**T.FUNC.TRANSIT.ALT**	
Threat description:	User Function Data in transit over a shared communications medium may be altered by unauthorized persons.	
Threat vector:	**Asset:**	User Function Data
	Actor:	Anonymous, remote
	Skill:	Proficient or higher
	Equipment:	None
	Access:	Physical, local, network
	Outcome:	Corruption
	Impact:	Direct
Threat scenario:	An attacker can intercept a print or scan document or job settings that are transmitted over the network, change the content of the settings, and then forward to the recipient.	
Manufacturers observe:	Nothing abnormal	
IT providers observe:	Possible unexpected log entries	
Users observe:	Nothing abnormal	
Mitigation techniques:	See 7.3.16	

Table 37 —T.FUNC.TRANSIT.DIS

Threat ID:	**T.FUNC.TRANSIT.DIS**	
Threat description:	User Function Data in transit over a shared communications medium may be disclosed to unauthorized persons.	
Threat vector:	**Asset:**	User Function Data
	Actor:	Anonymous, remote
	Skill:	Proficient or higher
	Equipment:	None
	Access:	Physical, local, network
	Outcome:	Corruption
	Impact:	Direct
Threat scenario:	An attacker can monitor (sniff) network traffic with standard network sniffing tools to discover information about another user's documents or another user's job history.	
Manufacturers observe:	Nothing abnormal	
IT providers observe:	Nothing abnormal	
Users observe:	Nothing abnormal	
Mitigation techniques:	See 7.3.17	

6.3.2.4 Threats to HCD Protected and Confidential Data

Table 38 —T.CONF.CAMERA.DIS

Threat ID:	**T.CONF.CAMERA.DIS**	
Threat description:	HCD Confidential Data may be disclosed to unauthorized persons by capturing this data with an external camera as it is entered into the HCD.	
Threat vector:	**Asset:**	HCD Confidential Data
	Actor:	Remote
	Skill:	Proficient or higher
	Equipment:	Specialized
	Access:	Physical proximity
	Outcome:	Disclosure
	Impact:	Direct
Threat scenario:	An attacker can use a digital or film camera, hidden either inside or outside the HCD, to record user entry of authentication data at the operator panel.	
Manufacturers observe:	Nothing abnormal	
IT providers observe:	Nothing abnormal	
Users observe:	Nothing abnormal	
Mitigation techniques:	See 7.4.1	

Table 39 —T.CONF.GUESS.DIS

Threat ID:	**T.CONF.GUESS.DIS**	
Threat description:	HCD Confidential Data may be disclosed to unauthorized persons by guessing or by observing the data as it is entered into the HCD.	
Threat vector:	**Asset:**	HCD Confidential Data
	Actor:	Anonymous, present
	Skill:	Layman or higher
	Equipment:	Standard
	Access:	Physical, network
	Outcome:	Disclosure
	Impact:	Indirect
Threat scenario:	Attacker can guess weak authentication data, observe authentication data being entered on the HCD, or obtain the data through local or network dictionary attacks.	
Manufacturers observe:	Nothing abnormal	
IT providers observe:	May see authorization failures on other systems in the environment as a result of attempts to use the disclosed authentication data or unexpected log entries	
Users observe:	Nothing abnormal	
Mitigation techniques:	See 7.4.2	

Table 40 —T.CONF.REST.ALT

Threat ID:	**T.CONF.REST.ALT**	
Threat description:	HCD Confidential Data in the HCD may be altered by unauthorized persons.	
Threat vector:	**Asset:**	HCD Confidential Data, HCD Availability, External Environment
	Actor:	Anonymous, present
	Skill:	Proficient or higher
	Equipment:	Standard
	Access:	Network, physical
	Outcome:	Corruption, interruption, loss (theft) of service
	Impact:	Direct, indirect
Threat scenario:	Attacker can modify user, HCD, or network authentication data by using the administrator functions on the HCD.	
Manufacturers observe:	Service calls relating the security settings not being maintained in the HCD	
IT providers observe:	Help desk calls relating to the HCD not functioning consistently; configuration of the HCD changes unexpectedly	
Users observe:	Inability to use the HCD or unexplained changes in the way the HCD functions	
Mitigation techniques:	See 7.4.3	

Table 41 —T.CONF.REST.DIS

Threat ID:	**T.CONF.REST.DIS**	
Threat description:	HCD Confidential Data in the HCD may be disclosed to unauthorized persons.	
Threat vector:	**Asset:**	HCD Confidential Data
	Actor:	Present
	Skill:	Proficient or higher
	Equipment:	Standard
	Access:	Physical
	Outcome:	Disclosure
	Impact:	Indirect
Threat scenario:	Attacker can recover user, HCD, or network authentication data by using the administrator functions on the HCD. This authentication data can then be used to enable other subsequent attacks.	
Manufacturers observe:	Nothing abnormal	
IT providers observe:	May see authorization failures on other systems in the environment as a result of attempts to use the disclosed authentication data or unexpected log entries or may notice the removal or loss of the drive	
Users observe:	Nothing abnormal	
Mitigation techniques:	See 7.4.4	

Table 42 —T.CONF.TRANSIT.ALT

Threat ID:	**T.CONF.TRANSIT.ALT**	
Threat description:	HCD Confidential Data in transit over a shared communications medium may be altered by unauthorized persons.	
Threat vector:	**Asset:**	HCD Confidential Data
	Actor:	Anonymous
	Skill:	Proficient or higher
	Equipment:	Standard
	Access:	Network
	Outcome:	Disclosure, corruption
	Impact:	Indirect
Threat scenario:	An attacker can intercept a user’s authentication data being transmitted over the network, change the information, and then forward to the recipient.	
Manufacturers observe:	Nothing abnormal	
IT providers observe:	May see authorization failures on other systems in the environment as a result of attempts to use the corrupted authentication data or unexpected log entries	
Users observe:	Nothing abnormal	
Mitigation techniques:	See 7.4.5	

Table 43—T.CONF.TRANSIT.DIS

Threat ID:	**T.CONF.TRANSIT.DIS**	
Threat description:	HCD Confidential Data in transit over a shared communications medium may be disclosed to unauthorized persons.	
Threat vector:	**Asset:**	HCD Confidential Data
	Actor:	Anonymous
	Skill:	Proficient or higher
	Equipment:	Standard
	Access:	Network
	Outcome:	Disclosure
	Impact:	Indirect
Threat scenario:	Attacker can sniff network traffic when user's authentication data is transmitted to or from the HCD over the network.	
Manufacturers observe:	Nothing abnormal	
IT providers observe:	May see authorization failures on other systems in the environment as a result of attempts to use the disclosed authentication data or unexpected log entries	
Users observe:	Nothing abnormal	
Mitigation techniques:	See 7.4.6	

Table 44—T.CONF.TRANSIT.EM.DIS

Threat ID:	**T.CONF.TRANSIT.EM.DIS**	
Threat description:	HCD Confidential Data in transit over a shared communications medium may be disclosed to unauthorized persons by capturing the EM radiation from the communication medium.	
Threat vector:	**Asset:**	HCD Confidential Data
	Actor:	Remote
	Skill:	Expert
	Equipment:	Bespoke
	Access:	Network
	Outcome:	Disclosure
	Impact:	Indirect
Threat scenario:	Attacker can use EM energy that is radiated from the network connection or cabling to sniff data generated from the HCD and recover authentication data.	
Manufacturers observe:	Nothing abnormal	
IT providers observe:	May see authorization failures on other systems in the environment as a result of attempts to use the disclosed authentication data or unexpected log entries	
Users observe:	Nothing abnormal	
Mitigation techniques:	See 7.4.7	

Table 45—T.PROT.REST.ALT

Threat ID:	**T.PROT.REST.ALT**	
Threat description:	HCD Protected Data in the HCD may be altered by unauthorized persons.	
Threat vector:	**Asset:**	HCD Protected Data, HCD Availability
	Actor:	Anonymous, present
	Skill:	Proficient or higher
	Equipment:	Standard
	Access:	Network, physical
	Outcome:	Corruption, interruption
	Impact:	Direct, indirect
Threat scenario:	Attacker can alter an HCD's e-mail or fax address book or an HCD's job log that is stored on the device.	
Manufacturers observe:	Service calls relating the configuration not being maintained in the HCD	
IT providers observe:	Help desk calls relating to the HCD not functioning consistently; configuration of the HCD changes unexpectedly	
Users observe:	Inability to use the HCD, or unexplained changes in the way the HCD functions or prints documents	
Mitigation techniques:	See 7.4.8	

Table 46—T.PROT.TRANSIT.ALT

Threat ID:	**T.PROT.TRANSIT.ALT**	
Threat description:	HCD Protected Data in transit over a shared communications medium may be altered by unauthorized persons.	
Threat vector:	**Asset:**	HCD Protected Data, HCD Availability
	Actor:	Anonymous
	Skill:	Proficient or higher
	Equipment:	Standard
	Access:	Network
	Outcome:	Corruption
	Impact:	Indirect
Threat scenario:	Attacker can intercept and alter the HCD's usage log data as they are being transferred over a network to the fleet management server.	
Manufacturers observe:	Nothing abnormal	
IT providers observe:	Possible unexpected log entries	
Users observe:	Nothing abnormal	
Mitigation techniques:	See 7.4.9	

6.3.2.5 Threats to HCD software

Table 47—T.SW.APPLET.ALT

Threat ID:	**T.SW.APPLET.ALT**	
Threat description:	HCD software applets in the HCD may be altered by unauthorized persons.	
Threat vector:	**Asset:**	Software, User Document Data, User Function Data, HCD Confidential Data, HCD Protected Data, HCD Availability, External Environment, HCD Physical Resources
	Actor:	Anonymous, present
	Skill:	Proficient or higher
	Equipment:	Standard
	Access:	Network, local, physical
	Outcome:	Interruption, corruption, disclosure
	Impact:	Indirect
Threat scenario:	An attacker can launch almost any type of attack by installing a rogue, embedded software applet on the HCD. Once the HCD is compromised with this type of attack the threats relative to the defined assets are endless.	
Manufacturers observe:	Possibly service calls relating the HCD bringing down the network	
IT providers observe:	Help desk calls relating to the HCD not functioning correctly, other systems on the same network not functioning as normal, attacks on other networked devices, or general network environment instability	
Users observe:	Inability to use the HCD and possibly other devices on the network	
Mitigation techniques:	See 7.5.1	

Table 48—T.SW.FIRMWARE.ALT

Threat ID:	**T.SW.FIRMWARE.ALT**	
Threat description:	HCD Firmware in the HCD may be altered by unauthorized persons.	
Threat vector:	**Asset:**	Software, User Document Data, User Function Data, HCD Confidential Data, HCD Protected Data, HCD Availability, External Environment, HCD Physical Resources
	Actor:	Anonymous, present
	Skill:	Proficient or higher
	Equipment:	Standard
	Access:	Network, local, physical
	Outcome:	Interruption, corruption, disclosure
	Impact:	Indirect
Threat scenario:	An attacker can launch almost any type of attack by installing rogue firmware or rogue embedded software updates on the HCD. Once the HCD is compromised with this type of attack the threats relative to the defined assets are endless.	
Manufacturers observe:	Possibly service calls relating the HCD *bringing down* the network	
IT providers observe:	Help desk calls relating to the HCD not functioning correctly, other systems on the same network not functioning as normal, attacks on other networked devices, or general network environment instability	
Users observe:	Inability to use the HCD and possibly other devices on the network	
Mitigation techniques:	See 7.5.2	

6.3.2.6 Threats to the HCD External Environment

Table 49—T.ENV.DOS

Threat ID:	**T.ENV.DOS**	
Threat description:	The External Environment may be interrupted by unauthorized persons by creating a DoS attack on the local network using the HCD's interface.	
Threat vector:	**Asset:**	External Environment
	Actor:	Anonymous
	Skill:	Proficient or higher
	Equipment:	Standard
	Access:	Network
	Outcome:	Interruption
	Impact:	Indirect
Threat scenario:	An attacker can effect a DoS attack on the network environment by triggering the HCD to generate excessive notifications, messages, SNMP traps, or other types of network traffic on the local network.	
Manufacturers observe:	Possibly service calls relating the HCD bringing down the network	
IT providers observe:	Help desk calls relating other systems on the same network not functioning as normal, attacks indicated on other networked devices, or general network environment instability	
Users observe:	Availability issues with the HCD or other networked device	
Mitigation techniques:	See 7.6.1	

Table 50—T.ENV.FAXBRIDGE

Threat ID:	**T.ENV.FAXBRIDGE**	
Threat description:	The External Environment or the HCD's internal components and software may be accessed by unauthorized persons via the fax connection.	
Threat vector:	**Asset:**	User Document and Function Data, HCD Confidential Data, HCD Protected Data, Software, External Environment, HCD Availability
	Actor:	Anonymous
	Skill:	Proficient or higher
	Equipment:	Standard
	Access:	Telephone
	Outcome:	Disclosure, corruption, loss of resource
	Impact:	Direct
Threat scenario:	An attacker can access any asset within the HCD or effect a DoS attack on the network environment by using the fax connection as an unsecured path into the HCD or as a bridge to the local network.	
Manufacturers observe:	Nothing abnormal	
IT providers observe:	Help desk calls relating to the HCD not functioning correctly, other systems on the same network not functioning as normal, attacks on other networked devices, or general network environment instability or abnormal usage statistics on the fax connection	
Users observe:	Availability issues with the HCD or other networked device	
Mitigation techniques:	See 7.6.2	

Table 51 — T.ENV.PROXY.DOS

<table>
<tr><td><b>Threat ID:</b></td><td colspan="2"><b>T.ENV.PROXY.DOS</b></td></tr>
<tr><td><b>Threat description:</b></td><td colspan="2">The External Environment may be interrupted by unauthorized persons by propagating an attack to the local network through a network service on the HCD.</td></tr>
<tr><td rowspan="7"><b>Threat vector:</b></td><td><b>Asset:</b></td><td>External Environment, HCD Availability</td></tr>
<tr><td><b>Actor:</b></td><td>Anonymous</td></tr>
<tr><td><b>Skill:</b></td><td>Proficient or higher</td></tr>
<tr><td><b>Equipment:</b></td><td>Standard</td></tr>
<tr><td><b>Access:</b></td><td>Network</td></tr>
<tr><td><b>Outcome:</b></td><td>Interruption</td></tr>
<tr><td><b>Impact:</b></td><td>Indirect</td></tr>
<tr><td><b>Threat scenario:</b></td><td colspan="2">An attacker can launch various other attacks on the network by using one of the network services on the HCD as a relay or proxy.</td></tr>
<tr><td><b>Manufacturers observe:</b></td><td colspan="2">Possibly service calls relating the HCD bringing down the network</td></tr>
<tr><td><b>IT providers observe:</b></td><td colspan="2">Help desk calls relating other systems on the same network not functioning as normal, attacks indicated on other networked devices, or general network environment instability</td></tr>
<tr><td><b>Users observe:</b></td><td colspan="2">Availability issues with the HCD or other networked device</td></tr>
<tr><td><b>Mitigation techniques:</b></td><td colspan="2">See 7.6.3</td></tr>
</table>

6.4 Threat risk levels

6.4.1 Overview

Using the threat vector definitions, the risk rating of each threat was determined by considering both the importance of the asset being compromised and severity of the threat's impact in each environment. Each threat was given a rating of *high, moderate,* or *low* for each of the functional environments. These threat ratings are listed in tables in the following subclauses.

6.4.2 Risk ratings for the various operational environments

Risk ratings for each of the defined threats in each of the defined operational environments are listed in Table 52.

Table 52—Risk ratings for threats in each operational environment

	Risk rating for operational environments				
Threat ID	**A**	**B**	**C**	**D**	**Vector**
T.CONSUMABLES.EXHAUST	Moderate	Moderate	Moderate	Moderate	Table 20
T.CONSUMABLES.THEFT	Moderate	Moderate	High	Moderate	Table 19
T.CONF.CAMERA.DIS	High	Moderate	Moderate	Moderate	Table 38
T.CONF.GUESS.DIS	High	High	High	Moderate	Table 39
T.CONF.REST.ALT	High	High	Moderate	Low	Table 40
T.CONF.REST.DIS	High	High	Moderate	Moderate	Table 41
T.CONF.TRANSIT.ALT	High	High	Moderate	Low	Table 42
T.CONF.TRANSIT.DIS	High	High	Moderate	Low	Table 43
T.CONF.TRANSIT.EM.DIS	Moderate	Low	Low	Low	Table 44
T.DOC.ANALYZE.DIS	Moderate	Moderate	Low	Moderate	Table 21
T.DOC.CAMERA.DIS	High	Moderate	Moderate	Moderate	Table 22
T.DOC.DELETED.SAL	High	Moderate	Low	Moderate	Table 23
T.DOC.EM.DIS	Moderate	Moderate	Low	Moderate	Table 24
T.DOC.FAX.ALT	Moderate	Moderate	Moderate	Moderate	Table 25
T.DOC.FAX.DIS	High	Moderate	Moderate	Moderate	Table 26
T.DOC.INPUT.DIS	Moderate	Moderate	Low	Moderate	Table 27
T.DOC.OUTPUT.DIS	Moderate	Moderate	Moderate	Moderate	Table 28
T.DOC.RETRIEVE.ALT	Moderate	Moderate	Low	Moderate	Table 29
T.DOC.RETRIEVE.DIS	High	Moderate	Low	Moderate	Table 30
T.DOC.REST.SAL	High	Moderate	Low	Low	Table 31
T.DOC.TRANSIT.ALT	High	Moderate	Moderate	Moderate	Table 32
T.DOC.TRANSIT.EM.DIS	Moderate	Low	Low	Low	Table 33
T.DOC.TRANSIT.DIS	High	Moderate	Moderate	Moderate	Table 34
T.DOS.FAX.HOOK	Moderate	Moderate	Moderate	Moderate	Table 5
T.DOS.FAX.LOOP	Moderate	Moderate	Moderate	Moderate	Table 6
T.DOS.FAX.TRAIN	Moderate	Moderate	Moderate	Moderate	Table 7
T.DOS.FAX.VOLUME	Moderate	Moderate	Moderate	Moderate	Table 8
T.DOS.HCD.ALTER	Moderate	Moderate	Moderate	Moderate	Table 9
T.DOS.HCD.INTERFERE	Moderate	Moderate	Moderate	Moderate	Table 10
T.DOS.PRT.CHANNEL	Moderate	Moderate	High	Moderate	Table 11
T.DOS.PRT.CRASH	Moderate	Moderate	High	Moderate	Table 12
T.DOS.PRT.PRIORTY	Moderate	Moderate	Moderate	Moderate	Table 13
T.DOS.SMI.CONNECT	Moderate	Moderate	Moderate	Moderate	Table 14
T.DOS.SMI.CRAFT	Moderate	Moderate	Moderate	Moderate	Table 15
T.DOS.SMI.FLOOD	Moderate	Moderate	High	Moderate	Table 16
T.ENV.DOS	Moderate	Moderate	High	Moderate	Table 49
T.ENV.FAXBRIDGE.	Moderate	Moderate	Low	Low	Table 50
T.ENV.PROXY.DOS	Moderate	Moderate	Moderate	Moderate	Table 51
T.FUNC.REST.ALT	Moderate	Moderate	Low	Low	Table 35
T.FUNC.TRANSIT.ALT	Moderate	Moderate	Low	Low	Table 36
T.FUNC.TRANSIT.DIS	Moderate	Moderate	Low	Low	Table 37
T.HCD.AVAIL.COPY	Moderate	Moderate	High	Moderate	Table 17
T.HCD.AVAIL.BYPASS	Moderate	Moderate	High	Moderate	Table 18
T.PROT.TRANSIT.ALT	High	High	Moderate	Low	Table 46
T.PROT.REST.ALT	Moderate	Moderate	Moderate	Moderate	Table 45
T.SW.APPLET.ALT	High	High	High	Moderate	Table 47
T.SW.FIRMWARE.ALT	Moderate	Moderate	Moderate	Moderate	Table 48

7. Threat mitigation techniques

This clause provides guidance for manufacturers and IT professionals with regard to mechanisms that may be effective in mitigating the various threats to an HCD. It also describes some of the mitigation techniques available to address the threats described in the previous clause. Each threat ID from Clause 6 is listed and contains a list of techniques for manufacturers relating to capabilities or features of an HCD that, if used, may help mitigate each individual threat. Each threat ID also has a section with recommendations for those IT professionals responsible for the operation of the HCD as well.

NOTE—For some threats, only one mitigation technique is described. In neither this case nor when multiple techniques are described should the lists be considered exhaustive.

7.1 Mitigating threats to HCD Availability

This subclause describes mitigation techniques available to address threats to the availability of an HCD. These threats can, in theory, be applicable in all of the defined operational environments if there are no other security mechanisms used in the environment. However, there are differences in the applicability of the DoS threats when basic standard security practices are followed.

For example, a network in a typical SOHO environment (Operational Environment D) that is connected directly to the Internet with no firewall protection or no virus scanning protection on its networked computers is just as susceptible to DoS attacks as a typical enterprise (Operational Environment B) environment. However, the addition of these basic security mechanisms can be a sufficient mitigation of the network interface DoS attacks in a typical SOHO environment because these threats are most likely only from outside the environment. This is not the case with the Operational Environment B since these types of threats are assumed to be from both outside and inside the environment.

7.1.1 T.DOS.FAX.HOOK

7.1.1.1 Definition

HCD Availability may be interrupted by unauthorized persons by inserting an off-hook telephone in the fax line to prevent incoming or outgoing faxes (see Table 5).

7.1.1.2 Background

This type of attack, like simply unplugging the power cord, is completely physical and can be performed by an attacker with little or no expertise.

7.1.1.3 Mitigation techniques for HCD manufacturers

The following techniques may be utilized by HCD manufacturers to mitigate this threat:

a) Providing the capability for the HCD to log attempts to send a fax into a busy or dead (no ring tone) fax line and optional administrative notification of repeated attempts

b) Providing the capability to periodically detect the dial tone at idle, and logging any failures to get the dial tone

7.1.1.4 Mitigation techniques for IT professionals

The following techniques may be utilized by IT professionals to mitigate this threat:

a) Ensuring that there are no additional, unconnected, and accessible fax or telephone port connections in the same wiring loop as the HCD's fax loop

b) Carefully examining the physical protection and isolation of the fax connection between the HCD and the telephone network infrastructure and ensure there are access control mechanisms for these physical locations

7.1.2 T.DOS.FAX.LOOP

7.1.2.1 Definition

HCD Availability may be interrupted by unauthorized persons by continuously sending grayscale fax pages at low speed to or from the HCD (see Table 6).

7.1.2.2 Background

The T.DOS.FAX.LOOP attack, like the T.DOS.FAX.VOLUME attack, is a relatively basic attack that can be performed by an attacker with little or no expertise. In the T.DOS.FAX.LOOP case, however, some basic knowledge of how different types of data affect the speed and volume of the transmitted fax data is required to create the most "efficient" attack. This type of attack can occur in any operational environment that has an HCD with fax capabilities.

7.1.2.3 Mitigation techniques for HCD manufacturers

The following techniques may be utilized by HCD manufacturers to mitigate this threat:

a) Providing administratively controlled fax job timers or fax data volume limits that restrict the amount of real time a fax job may consume or the amount of data that can be sent or received

b) Providing administratively controlled white lists or black lists for incoming fax identities

c) Providing logging capability of fax sender ID, data volume, etc. of incoming and outgoing fax jobs

d) Providing administratively configurable fax speed negotiation minimums (e.g., configure fax function to negotiate no speed slower than 14.4 kb/s)

7.1.2.4 Mitigation techniques for IT professionals

The following techniques may be utilized by IT professionals to mitigate this threat:

a) Carefully examining the physical protection and isolation of the fax connection between the HCD and the telephone network infrastructure and ensure there are access control mechanisms for these physical locations

b) Setting the minimum fax negotiation speed to the slowest expected speed for the environment (e.g.,14.4 kb/s)

7.1.3 T.DOS.FAX.TRAIN

7.1.3.1 Definition

HCD Availability may be interrupted by unauthorized persons by generating an incoming fax connection that forces the fax modem to continuously train (negotiate fax connection parameters) (see Table 7).

7.1.3.2 Background

This threat is applicable in all environments that use HCDs with fax function. There is a fairly high level of sophistication assumed by the attacker since this type of attack requires the modification of the normal fax protocol in the attacking device to perform the continuous training sequence.

7.1.3.3 Mitigation techniques for HCD manufacturers

The following techniques may be utilized by HCD manufacturers to mitigate this threat:

a) Providing administratively controlled fax job timers that restrict the amount of real time before abandoning the training sequence

b) Providing administratively controlled white lists or black lists for incoming fax identities

c) Providing automatic blacklisting of fax identities that repeatedly attempt to train outside the accepted fax parameters

d) Providing logging capability of fax caller ID of fax jobs that fail the training process

7.1.3.4 Mitigation techniques IT professionals

The following technique may be utilized by IT professionals to mitigate this threat:

a) Periodically reviewing the HCD logs for jobs that failed the training process

7.1.4 T.DOS.FAX.VOLUME

7.1.4.1 Definition

HCD Availability may be interrupted by unauthorized persons by continuously sending excessive scanned document volume to the HCD to prevent its normal use (see Table 8).

7.1.4.2 Background

This type of attack can occur in any operational environment that has an HCD with fax capabilities and its execution requires little expertise, other than knowing how to send a fax, to execute.

7.1.4.3 Mitigation techniques for HCD manufacturers

The following techniques may be utilized by HCD manufacturers to mitigate this threat:

a) Providing administratively controlled fax job timers or fax data volume limits that restrict the amount of real time a fax job may consume or the amount of data that can be sent or received

b) Providing administratively controlled white lists or black lists for incoming fax identities

c) Providing logging capability of fax caller ID, data volume, etc., of incoming and outgoing fax jobs

d) Providing administratively configurable fax speed negotiation minimums (e.g., configure fax function to negotiate no speed slower that 14.4 kb/s)

7.1.4.4 Mitigation techniques for IT professionals

The following techniques may be utilized by IT professionals to mitigate this threat:

a) Periodically reviewing the HCD logs for repeated large-volume jobs

b) Setting the minimum fax negotiation speed to the slowest expected speed for the environment (e.g., 14.4 kb/s)

7.1.5 T.DOS.HCD.ALTER

7.1.5.1 Definition

HCD Availability may be interrupted by unauthorized persons by mechanically or electrically altering or damaging the HCD or its components (see Table 9).

7.1.5.2 Background

This type of attack requires physical access to the HCD's location.

7.1.5.3 Mitigation techniques for HCD manufacturers

The following techniques may be utilized by HCD manufacturers to mitigate this threat:

a) Providing secure (e.g., lockable) doors and panels that reduce the likelihood of an unauthorized user gaining access to the internals of the HCD

b) Providing visual or electronic indication of the history of access to internal mechanisms or electronics

c) Ensuring that the HCD enclosure construction is of sound material and is internally secured

d) Utilizing locking connectors for power and signal cables, with securing provisions to prevent inadvertent disconnect and to sense intentional disconnect

e) Utilizing nonstandard fasteners that require nonstandard or specialized tools for any externally accessible fasteners, and any internal fasteners for components to be access only by authorized technicians

f) Providing alarms for attempted unauthorized access, damage, or disablement, using either audible or remote (e.g., network, radio, pager, or mobile phone) intrusion alarms if panels are forced, or power or signal connectors are disconnected

g) Providing unambiguous indication of post-manufacturing alteration of internal components

7.1.5.4 Mitigation techniques for IT professionals

The following techniques may be utilized by IT professionals to mitigate this threat:

a) Increasing the physical security of the HCD through either placement in a controlled-access location or monitoring of a public-access location

b) Using security cameras or other mechanisms to monitor the HCD

7.1.6 T.DOS.HCD.INTERFERE

7.1.6.1 Definition

HCD Availability may be interrupted by unauthorized persons by mechanically or electrically interfering with the HCD or its components (see Table 10).

7.1.6.2 Background

Because some of the more advanced T.DOS.HCD.INTERFERE attacks (e.g., EMI-based attacks) may not require direct physical access to the HCD, simple physical access controls cannot completely eliminate this threat.

7.1.6.3 Mitigation techniques for HCD manufacturers

The following techniques may be utilized by HCD manufacturers to mitigate this threat:

a) Providing secure (e.g., lockable) doors and panels that reduce the likelihood of an unauthorized user gaining access to the internals of the HCD

b) Providing visual or electronic indication of the history of access to internal mechanisms or electronics

c) Ensuring that the HCD enclosure construction is of sound material and is internally secured

d) Utilizing EM-shielded materials for the HCD enclosure

e) Utilizing locking connectors for power and signal cables, with securing provisions to prevent inadvertent disconnect and to sense intentional disconnect

f) Utilizing nonstandard fasteners that require nonstandard or specialized tools for any externally accessible fasteners, and any internal fasteners for components to be access only by authorized technicians

g) Providing alarms for attempted unauthorized access, damage, or disablement, using either audible or remote (e.g., network, radio, pager, or mobile phone) intrusion alarms if panels are forced, or power or signal connectors are disconnected

7.1.6.4 Mitigation techniques for IT professionals

The following techniques may be utilized by IT professionals to mitigate this threat:

a) Providing physical security for the HCD, whether through location in a controlled-access area or by positioning it in a high-traffic area where an attacker will be less likely to perform the attack unobserved

b) Using security cameras or other mechanisms to monitor the HCD

c) Locating the HCD in an EM-shielded area

7.1.7 T.DOS.PRT.CHANNEL

7.1.7.1 Definition

HCD Availability may be interrupted by unauthorized persons by submitting PDL or print protocol data to generate a back-channel message flood (see Table 11).

7.1.7.2 Background

This threat is applicable to all operational environments in which the HCD is shared. Because this threat is specifically related to the crafting of particular print jobs that result in a flood of back-channel messages, a certain amount of expertise is assumed on the part of the attacker; however once a print job with the ability to cause a flood of back-channel messages is found and distributed, anybody with the ability to print to the device can become an attacker.

7.1.7.3 Mitigation techniques for HCD manufacturers

The following techniques may be utilized by HCD manufacturers to mitigate this threat:

a) Providing an option for the administrator to disable all back-channel messages

b) Implementing a shutdown trigger whereby a print job generating excessive back-channel traffic can be automatically terminated by the print engine

7.1.7.4 Mitigation techniques for IT professionals

The following technique may be utilized by IT professionals to mitigate this threat:

a) If possible, restrict printing protocols to those protocols that provide for user authentication capability

7.1.8 T.DOS.PRT.CRASH

7.1.8.1 Definition

HCD Availability may be interrupted by unauthorized persons by submitting PDL or print protocol data to cause print controller failure or code execution loop (see Table 12).

7.1.8.2 Background

This threat is applicable to all operational environments in which the HCD is shared. Because this threat is specifically related to the crafting of particular print jobs that result in the failure of devices' hardware or firmware, a certain amount of expertise is assumed on the part of the attacker; however once a print job with the ability to induce HCD failure is found and distributed, anybody with the ability to print to the device can become an attacker.

7.1.8.3 Mitigation techniques for HCD manufacturers

The following techniques may be utilized by HCD manufacturers to mitigate this threat:

a) Ensuring that even where an attack of this type causes a failure of the print subsystem, it does not interfere with the operation of other HCD subsystems

b) Ensuring that the HCD's core functionality runs at a higher priority so that a looping print job cannot starve the core device functionality for central processing unit (CPU) time

c) Implementing a timer mechanism to cancel any print job that has exceeded a preset threshold of CPU or real time since last producing a printed page

d) Logging all jobs that are terminated based on the criteria for identifying crashed or looping print jobs, including the originating IP address and user authentication data, where available

e) Ensuring that the HCD can recover automatically and in a timely fashion after the end of the attack

7.1.8.4 Mitigation techniques for IT professionals

The following technique may be utilized by IT professionals to mitigate this threat:

a) If possible, restricting print protocols to those protocols that provide for user authentication capability

7.1.9 T.DOS.PRT.PRIORITY

7.1.9.1 Definition

HCD Availability may be interrupted by unauthorized persons by intentionally, continuously sending print jobs that de-prioritize other types of jobs. (see Table 13).

7.1.9.2 Background

The T.DOS.PRT.PRIORITY is one of the easiest of the DoS type attacks to execute since on many types of devices it requires nothing more than using the HCD via its normal access methods. The only difference between the normal use, or overuse, of the HCD and the DoS attack is the intent of the initiator of the jobs.

7.1.9.3 Mitigation techniques for HCD manufacturers

The following techniques may be utilized by HCD manufacturers to mitigate this threat:

a) Providing the capability to enable only protocols that require user authentication before jobs can be sent to the HCD

b) Providing audit capability for all users of the HCD (for tracking the source of an attack)

c) Providing the capability to restrict the number of jobs that a given authenticated user can have queued to the HCD at a given time (administrative controllability of the threshold level)

d) Providing an administratively controllable job timer that restricts the amount of time that can be spent processing a given job

e) Providing an administratively controllable priority scheme for ports and services in the HCD, possibly including port rotation priorities, etc.

f) Providing users or administrators with the ability to pause or interrupt an active job (e.g., print job) to initiate another (e.g., copy or scan job)

7.1.9.4 Mitigation techniques for IT professionals

The following technique may be utilized by IT professionals to mitigate this threat:

a) If possible, restricting print protocols to those protocols that provide for user authentication capability

7.1.10 T.DOS.SMI.CONNECT

7.1.10.1 Definition

HCD Availability may be interrupted by unauthorized persons by opening all available connections on a shared communication media and keeping them open to prevent legitimate connections (see Table 14).

7.1.10.2 Background

In a networked environment of any type, the mostly likely target of a coordinated DoS attack is not going to be an HCD. Instead, the most likely targets of these types of attacks are Web servers or other types of servers in the enterprise. The most effective strategy for the mitigation of this threat is to not allow it to take place in the first place by properly protecting all devices on the network from executing unauthorized code, such as Trojan horses, viruses, etc.

7.1.10.3 Mitigation techniques for HCD manufacturers

The following techniques may be utilized by HCD manufacturers to mitigate this threat:

a) Implementing MAC address filtering to discard all network packets from non-white-listed network devices without requiring any processing outside the network interface itself

b) Implementing a shutdown trigger whereby a MAC address attempting to establish an excessive number of connections can be automatically filtered by the network interface

c) Ensuring that even where an attack of this type causes a failure of the network interface on the HCD, it does not interfere with the operation of those HCD subsystems that do not require network access

d) Ensuring that the HCD implements a best effort mechanism to recover automatically when the network interface is nonresponsive

7.1.10.4 Mitigation techniques for IT professionals

The following techniques may be utilized by IT professionals to mitigate this threat:

a) Ensuring that all networked devices have the latest security updates applied, and effective antivirus software installed and operational

b) Limiting network access to the HCDs to specific network nodes, such as print and mail servers, through the use of virtual local area networks (VLANs) or similar technologies

c) Networked devices without up-to-date security patches are isolated on the network by firewalls or other mechanisms

d) Ensuring that access controls to networked devices that are appropriate for the operational environment are present

7.1.11 T.DOS.SMI.CRAFT

7.1.11.1 Definition

HCD Availability may be interrupted by unauthorized persons by sending crafted packets over the shared communication media to cause interface crash or failure (see Table 15).

7.1.11.2 Background

Because this threat is specifically related to the crafting of packets that result in the failure of the network interface, a certain amount of expertise is assumed on the part of the attacker. Just as with the T.DOS.SMI.CONNECT threat, the most likely target of a coordinated attack of this type is likely not going to be an HCD but a Web or other critical high-profile networked device.

7.1.11.3 Mitigation techniques for HCD manufacturers

With regard to the range of possible illegal packets on the network, it is impractical to expect the network hardware and software to be completely bulletproof. Basic checking of the contents of the packet's structure (e.g., making sure the packet is of legal size) before parsing and passing data to the application layer stack can create an interface that is more resilient to these types of events.

The following techniques may be utilized by HCD manufacturers to mitigate this threat:

a) Implementing MAC address filtering to discard all network packets from non-white-listed network devices without doing any processing beyond the identification of the MAC address on those packets

b) Ensuring that even where an attack of this type causes a failure of the network interface on the HCD, it does not interfere with the operation of those HCD subsystems that do not require network access

c) Ensuring that the HCD implements a best effort mechanism to recover automatically when the network interface is nonresponsive

d) Ensuring that all incidents of malformed packets including date, time, IP, and MAC address of the source are logged

7.1.11.4 Mitigation techniques for IT professionals

The following techniques may be utilized by IT professionals to mitigate this threat:

a) Ensuring that all networked devices have the latest security updates applied, and effective antivirus software installed and operational

b) Limiting network access to the HCDs to specific network nodes, such as print and mail servers, through the use of VLANs or similar technologies

c) Ensure that HCDs are placed behind firewalls or other network security devices

7.1.12 T.DOS.SMI.FLOOD

7.1.12.1 Definition

HCD Availability may be interrupted by unauthorized persons by flooding packets over the shared communication media to cause a sustained interface interruption or failure (see Table 16).

7.1.12.2 Background

This type of attack is likely the most prevalent type of DoS attack on networked devices, partially because there are many programs or scripts that have been written and made available on the Internet that can initiate such an attack and partially because most network protocols contain the concept of a broadcast message that, by definition, is processed by all network devices. Some of these attacks are merely random or global with respect to their target while others have been created that allow for a very specific target of the attack.

7.1.12.3 Mitigation techniques for HCD manufacturers

The following techniques may be utilized by HCD manufacturers to mitigate this threat:

a) Implementing MAC address filtering to discard all network packets from non-white-listed network devices without requiring any processing outside the network interface itself

b) Implementing a shutdown trigger whereby a MAC address generating excessive network traffic can be automatically filtered by the network interface

c) Ensuring that even where an attack of this type causes a failure of the network interface on the HCD, it does not interfere with the operation of those HCD subsystems that do not require network access

d) Ensuring that the HCD implements a best effort mechanism to recover automatically when the network interface is nonresponsive

7.1.12.4 Mitigation techniques for IT professionals

The following techniques may be utilized by IT professionals to mitigate this threat:

a) Ensuring that all networked devices have the latest security updates applied, and effective antivirus software installed and operational

b) Limiting network access to the HCDs to specific network nodes, such as print and mail servers, through the use of VLANs or similar technologies

c) Ensure that HCDs are placed behind firewalls or other network security devices

7.1.13 T.HCD.AVAIL.COPY

7.1.13.1 Definition

HCD Availability may be misappropriated by using rogue copy control devices. This will allow unauthorized persons to bypass copy control or accounting mechanisms (see Table 17).

7.1.13.2 Background

The T.HCD.AVAIL.COPY threat, while possible in any operational environment that uses a hardware-based copy control device, is most relevant to Operational Environment C (e.g., kiosks, libraries, schools, or copy centers) that may have limited physical monitoring or control. However, in higher security operational environments, this threat still presents a risk to the integrity of the audit trail.

By its nature, the simple, four-wire electrical copy control interface is the most at risk to this threat; other types of copy control interfaces (e.g., digital interfaces controlled through a network, serial or USB connection, or internal embedded copy control functionality) should be used in preference to the four-wire interface, if possible.

7.1.13.3 Mitigation techniques for HCD manufacturers

The following techniques may be utilized by HCD manufacturers to mitigate this threat:

a) Supporting the use of secure digital interfaces for external copy control devices through an authentication mechanism and encrypting the copy control communications

b) Ensuring that if a four-wire copy control interface is included with the HCD, the interface is capable of being disabled

c) Ensuring that if a four-wire copy control interface is included with the HCD, the interface connector is internal to the device and secured behind lockable panels

d) Utilizing proprietary connectors for copy control to reduce the opportunity for an attacker to either manufacture a rogue copy control cable or to mimic its operation directly without the use of an actual connector

e) Supporting the use of sufficiently secure identifiers and passwords (e.g., not limited to four digit numeric PIN codes)

7.1.13.4 Mitigation techniques for IT professionals

The following techniques may be utilized by IT professionals to mitigate this threat:

a) Securely fastening both ends of the cable for any external copy control devices to prevent an attacker from accessing the copy control connectors directly

b) Regularly auditing the copy and print data collected by the copy control system against the device’s internal meters to ensure that systemic attacks to bypass the copy control mechanism are not taking place

7.1.14 T.HCD.AVAIL.BYPASS

7.1.14.1 Definition

HCD Availability may be misappropriated by circumventing normal HCD security or accounting controls (see Table 18).

7.1.14.2 Background

This threat, while possible in all of the defined operational environments, is most likely to be of concern in environments that require very close tracking of the utilization of the HCD. Examples of these types of environments include a public, for pay, print or copy shop or a law office where very rigorous tracking of work performed versus user or client charged is practiced.

7.1.14.3 Mitigation techniques for HCD manufacturers

The following techniques may be utilized by HCD manufacturers to mitigate this threat:

a) Providing the ability to completely and individually disable or turn off all HCD ports, including both physical and network ports, and protocols that allow the submission of jobs to the HCD

b) Ensuring that the configuration mechanisms for enabling and disabling these ports and protocols are authenticated

c) Providing the ability to create specific connection restrictions (e.g., white lists, IP, or MAC address filtering) at the communications protocol level

d) Providing robust protocol level authentication, such as IPSec or virtual private network (VPN) support

7.1.14.4 Mitigation techniques for IT professionals

The following techniques may be utilized by IT professionals to mitigate this threat:

a) Disabling or turning off all HCD ports [e.g., IEEE 1284, USB, EIA RS-232-C (serial), and IEEE 1394], network interfaces (e.g., Wi-Fi or Bluetooth), and protocols that allow the submission of jobs to the HCD, except the fully secured protocols

b) Where direct IP printing is required, enabling authentication at either the protocol level (e.g., CIFS or IPP) or at the application level (e.g., workstation-based authentication)

c) Turning on the maximum set of connection restrictions (e.g., white lists, IP or MAC address filtering) that still allow the required secured printing protocols to function

d) Implementing protocol-level authentication, such as IPSec, if it is available

e) Regular auditing of the print data collected by the print-tracking or auditing system should be performed against the device’s internal meters, to ensure that systemic attacks to bypass the print auditing mechanism are not taking place

f) Providing a dedicated connection (both physical and logical) from the server (whether print, accounting, or authorization) to the HCD to prevent users from establishing unauthorized connections

g) Disabling unauthenticated reprint capabilities in the HCD configuration

7.2 Mitigating threats to HCD Physical Resources

7.2.1 T.CONSUMABLES.THEFT

7.2.1.1 Definition

An HCD’s consumable items may be intentionally removed by unauthorized persons (see Table 19).

7.2.1.2 Background

The unauthorized removal of supplies (e.g., ink or toner cartridge, or input media) can be of concern in any of the defined operational environments, however, by the nature of the open access might be more likely in Operational Environment C (public) environments. The impact of the removal (theft) of the consumable resources of an HCD in any environment is determined much the same way as any other asset, the cost of the asset itself and the resulting impact (loss of use) of the asset removal.

While manufacturers may provide a basic level of mechanical protection to the consumables in an HCD via locking access panels or input media trays, an attacker with uncontrolled direct access can still defeat these protections. Users in environments where the impact of unauthorized removal of supplies and consumables is a concern should consider physical access controls or device monitoring rather than relying solely on the mechanical protections on the HCD.

7.2.1.3 Mitigation techniques for HCD manufacturers

The following techniques may be utilized by HCD manufacturers to mitigate this threat:

a) Providing lockable device access panels (for access to toner, ink, and other consumables) that can be unlocked only by an authorized device administrator

b) Providing lockable device input trays that can be unlocked only by an authorized device administrator

c) Providing a notification mechanism (e.g., network status alerts) to indicate that access doors or input media trays have been accessed

7.2.1.4 Mitigation techniques for IT professionals

The following technique may be utilized by IT professionals to mitigate this threat:

a) Providing physical security for the HCD, whether through location in a controlled-access area or by positioning it in a high-traffic area where an attacker will be less likely to be able remove supplies unobserved

7.2.2 T.CONSUMABLES.EXHAUST

7.2.2.1 Definition

An HCD’s consumable items may be intentionally exhausted as a result of jobs being submitted by unauthorized persons (see Table 20).

7.2.2.2 Background

The intentional misuse of the HCD with the intent of exhausting the consumables can be a problem in any operational environment where there is open access, whether via the data connections or through physical access, to the use of the HCD. In most environments, the occasional attack on the HCD to exhaust consumables or supplies may be tolerated. In other instances, the impact of an attack, whether on the cost of operation of the HCD or on the availability of the same, can be intolerable.

7.2.2.3 Mitigation techniques for HCD manufacturers

The following techniques may be utilized by HCD manufacturers to mitigate this threat:

a) Providing the ability to completely and individually disable or turn off all HCD ports and protocols that allow the submission of jobs to the HCD

b) Ensuring that the configuration mechanisms for enabling and disabling these ports and protocols are authenticated

c) For network protocols such as TCP/IP, providing the ability to create specific connection restrictions (e.g., white lists, IP, or MAC address filtering) at the communications protocol level

d) Providing robust protocol level authentication, such as IPSec or VPN support

e) Providing the ability for the administrator to define and set rules governing permissions given to users or groups of users, such as for access to print, scan, fax, or copy functions, access to color printing, or limits on the number of pages that can be processed

f) Providing a comprehensive audit trail of all copy and print transactions, including information about the authenticated user and the quantity of toner (e.g., toner coverage) utilized for those transactions

7.2.2.4 Mitigation techniques for IT professionals

The following techniques may be utilized by IT professionals to mitigate this threat:

a) Disabling or turning off all HCD ports and protocols that allow the submission of jobs to the HCD, except the fully secured protocols

b) Where direct IP printing is required, enabling authentication at either the protocol level (e.g., CIFS or IPP) or at the application level (e.g., workstation-based authentication)

c) Turning on the maximum set of connection restrictions (e.g., white lists, IP or MAC address filtering) that still allow the required secured printing protocols to function

d) Implementing protocol-level authentication, such as IPSec, if it is available

e) Regular auditing of the print data collected by the print-tracking or auditing system should be performed against the device's internal meters, to ensure that systemic attacks to bypass the print auditing mechanism are not taking place

f) Providing a dedicated connection (both physical and logical) from the server (whether print, accounting, or authorization) to the HCD to prevent users from establishing unauthorized connections

g) Disabling unauthenticated reprint capabilities in the HCD configuration

h) Implementing a periodic administrator review process for all HCD audit logs and account for any unusual events

7.3 Mitigating threats to HCD User Document and User Function Data

7.3.1 T.DOC.ANALYZE.DIS

7.3.1.1 Definition

User Document Data may be disclosed to unauthorized persons by using an electron microscope or other equipment to read residual image on copier belt or drum (see Table 21).

7.3.1.2 Background

The equipment needed to do this is expensive and the technology is difficult, so this threat is applicable only to Operational Environment A where there is very high value to the information.

There are three circumstances where this threat might be exercised:

1) Scrapping of the equipment (analogous to scrapping of workstations with hard disks)

2) Equipment maintenance that involves replacement of the intermediate imaging medium

3) Intentional removal of the intermediate imaging medium for analysis

The primary protection against this threat is vigilance on the part of personnel maintaining the device and the site.

Unlike an HDD, where erased data may not be immediately overwritten with new data to be saved, the intermediate imaging medium on an HCD is overwritten, perhaps several times, with each subsequent printed page. Any residual image that may be present on the photoconductor or transfer roll is masked by the image of the new page to be printed and eventually will degenerate such that the original image is unrecoverable.

7.3.1.3 Mitigation techniques for HCD manufacturers

The following techniques may be utilized by HCD manufacturers to mitigate this threat:

a) Providing secure (e.g., lockable) doors that reduce the likelihood of an unauthorized user gaining access to the internals of the HCD

b) Providing visual or electronic indication of the history of access to internal mechanisms or electronics

c) Ensuring that the HCD enclosure is of sound material and is internally secured

d) Utilizing nonstandard fasteners that require nonstandard or specialized tools for any externally accessible fasteners, and any internal fasteners for components to be access only by authorized technicians

e) Providing alarms for attempted unauthorized access, damage, or disablement, using either audible or remote (e.g., network, radio, pager, or mobile phone) intrusion alarms if panels are forced, or power or signal connectors are disconnected

f) Providing a service whereby any imaging medium removed while servicing an HCD is verifiably destroyed to prevent analysis of that medium

g) Providing an administrator initiated mechanism to print pages that clear residual data from the imaging media

7.3.1.4 Mitigation techniques for IT professionals

The following techniques may be utilized by IT professionals to mitigate this threat:

a) Increasing the physical security of the HCD through either placement in a controlled-access location or monitoring of a public-access location

b) Using security cameras or other mechanisms to monitor the HCD

c) Printing a large number of pages with random nonsecure content on the HCD prior to replacing the imaging media or disposing of the HCD (an example procedure may be found in ACSI 33 [B4])

d) Monitoring the HCD equipment for unauthorized entry

e) Ensuring that any service on the HCD equipment is be done by a trusted technician or monitored by security personnel

7.3.2 T.DOC.CAMERA.DIS

7.3.2.1 Definition

User Document Data may be disclosed to unauthorized persons by capturing this data with a hidden camera as it is processed by the HCD (see Table 22).

7.3.2.2 Background

The complexity of this attack and potential cost of equipment suggests that it is primarily applicable to Operational Environment A, although with the advent of inexpensive networked cameras, other types of organizations should also be aware of this. As an example of this type of attack, there have been cases of hidden cameras recording users entering ATM PINs, with obvious repercussions.

Although some design features can assist in mitigating this threat, protection primarily requires vigilance on the part of personnel maintaining the device and the site. Any signs of equipment entry, new objects in the vicinity, or changes in the positions of existing objects should be investigated. Any service on the equipment should be done by a trusted technician or properly monitored.

7.3.2.3 Mitigation techniques for HCD manufacturers

The following techniques may be utilized by HCD manufacturers to mitigate this threat:

a) Providing secure (e.g., lockable) doors that reduce the likelihood of an unauthorized user gaining access to the internals of the HCD

b) Providing visual or electronic indication of the history of access to internal mechanisms or electronics

c) Ensuring that the HCD enclosure is of sound material and is internally secured

d) Utilizing nonstandard fasteners that require nonstandard or specialized tools for any externally accessible fasteners, and any internal fasteners for components to be access only by authorized technicians

e) Providing alarms for attempted unauthorized access, damage, or disablement, using either audible or remote (e.g., network, radio, pager, or mobile phone) intrusion alarms if panels are forced, or power or signal connectors are disconnected

f) Offering visual shielding for the original document handler, output trays, and the operator panel of the HCD

7.3.2.4 Mitigation techniques for IT professionals

The following techniques may be utilized by IT professionals to mitigate this threat:

a) Increasing the physical security of the HCD through either placement in a controlled-access location or monitoring of a public-access location

b) Providing additional visual shielding of the HCD from possible external hidden cameras

c) Using security cameras or other mechanisms to monitor the HCD

d) Monitoring the HCD equipment for unauthorized entry, for new objects in the vicinity of the HCD, or changes in the positions of existing objects

e) Ensuring that any service on the HCD equipment is be done by a trusted technician or monitored by security personnel

7.3.3 T.DOC.DELETED.SAL

7.3.3.1 Definition

Deleted User Document Data in a nonvolatile storage medium that has been removed from the HCD may be salvaged by unauthorized persons (see Table 23).

7.3.3.2 Background

When data, whether User Document Data or not, is no longer needed by the HCD, the memory that is used to store this data is made available for use by the HCD’s OS when needed for subsequent tasks or processing. Like most commercial OSs for PCs, the freed data is not actually removed from the HCD’s memory space, merely the reference to that data is deleted, and the memory is marked for use in the OS’s memory management code. This leaves residual data on the HCD’s hard drive or other memory that may contain User Document Data assets that may be compromised by an attacker. Even volatile memory that eventually clears after power down may hold information for some time after the HCD is powered off.

There are various degrees of difficulty involved in exploiting this vulnerability. Except in cases where the hardcopy equipment is designed for hard disk removal and secure storage, removing the disk would involve some disassembly of the equipment. Some of the techniques that may be used to mitigate the threat can be expensive and may affect the performance of the HCD.

The equipment needed to recover data from a properly overwritten hard disk is expensive and the technology is difficult. Therefore, the advanced form of this threat (i.e., post-overwrite data salvage) is applicable primarily to environments such as Operational Environment A or B.

There are three circumstances where this threat might be exercised:

1) Scrapping of the equipment

2) Equipment maintenance that involves replacement of the storage medium

3) Intentional removal of the intermediate storage medium for analysis

The primary protection against this threat is vigilance on the part of personnel maintaining the device and the site.

7.3.3.3 Mitigation techniques for HCD manufacturers

The following techniques may be utilized by HCD manufacturers to mitigate this threat:

a) Providing secure (e.g., lockable) doors that reduce the likelihood of an unauthorized user gaining access to the internals of the HCD

b) Providing visual or electronic indication of the history of access to internal mechanisms or electronics

c) Ensuring that the HCD enclosure is of sound material and is internally secured

d) Utilizing nonstandard fasteners that require nonstandard or specialized tools for any externally accessible fasteners, and any internal fasteners for components to be access only by authorized technicians

e) Providing alarms for attempted unauthorized access, damage, or disablement, using either audible or remote (e.g., network, radio, pager, or mobile phone) intrusion alarms if panels are forced, or power or signal connectors are disconnected

f) Providing the option for the HCD to automatically overwrite deleted data on the HCD’s hard disk using an effective wiping technique, whether immediately upon deletion of that data or as an automatically scheduled task

g) Providing the option for the administrator to initiate an overwrite of the deleted data on the HCD’s hard disk using an effective wiping technique

h) Encrypting all data stored on the hard disk

i) Providing a removable hard disk option, whereby an authenticated administrator is able to quickly and securely remove a hard disk for storage in a secure location

j) Providing a service whereby any hard disk removed while servicing an HCD is verifiably destroyed to prevent analysis of that medium

k) Offering a version of the HCD that does not include persistent storage, or utilizing nonpersistent storage media, such as RAM memory, in place of a conventional hard disk, to ensure that the storage media is automatically erased upon loss of power

7.3.3.4 Mitigation techniques for IT professionals

The following techniques may be utilized by IT professionals to mitigate this threat:

a) Increasing the physical security of the HCD through either placement in a controlled-access location or monitoring of a public-access location

b) Using security cameras or other mechanisms to monitor the HCD

c) Using a magnetic wiping technique to comprehensively erase the contents of the HCD's hard disk prior to replacing the hard disk or disposing of the HCD

d) Removing the hard disk into secure storage at the end of each day to prevent an attacker from removing the disk while the location is unmonitored

e) Monitoring the HCD equipment for unauthorized entry

f) Ensuring that any service on the HCD equipment is be done by a trusted technician or monitored by security personnel

7.3.4 T.DOC.EM.DIS

7.3.4.1 Definition

User Document Data may be disclosed to unauthorized persons by capturing EM radiation from HCD (see Table 24).

7.3.4.2 Background

EM sniffing generally requires relatively advanced equipment, which suggests that the primary applicability of this threat is to high value information that is otherwise well-protected. This corresponds to Operational Environment A.

Encryption of network traffic only provides protection against interception of job input data, whether by network or local port. However, input/output (I/O) encryption will typically not protect information contained in internal signals. The most obvious examples are marking actuation signals (laser, inkjet, or impact mechanism) that if intercepted and characterized, can provide a raster image of the material printed. This vulnerability can be mitigated (but depending upon the complexity of sniffing equipment, not totally eliminated) by increased shielding, filtering, masking, and proper grounding, etc. Note that the emission suppression done for regulator compliance would probably not be sufficient for security purposes since it is concerned with radiated energy peaks over the frequency spectrum. See information on emanations phenomenology, measurement, and control technologies and techniques (TEMPEST INC. [B147], NSSTISSAM TEMPEST/1-92 [B104], Air Force Instruction 33-203 [B1]).

7.3.4.3 Mitigation techniques for HCD manufacturers

The following techniques may be utilized by HCD manufacturers to mitigate this threat:

a) Utilizing a well-shielded and filtered device enclosure to prevent leakage of EM radiation from the HCD's internal components

b) Minimizing the number of active external connectors to reduce the amount of EM leakage through such connectors

c) Utilizing an internal print controller rather than an external one, thus eliminating the EM radiation from the exposed controller-to-HCD connection cable

7.3.4.4 Mitigation techniques for IT professionals

The following techniques may be utilized by IT professionals to mitigate this threat:

a) Locating the HCD in an EM-shielded room or away from the perimeter of the facility

7.3.5 T.DOC.FAX.ALT

7.3.5.1 Definition

User Document Data may be altered by unauthorized persons via a man-in-the-middle attack on the PSTN interface (see Table 25).

7.3.5.2 Background

Because this threat assumes that the attacker has the ability to impersonate either the sender or the recipient, it can be assumed that a significant amount of effort has been put into the attack. It is therefore likely that this threat applies primarily to higher value data, typical to Operational Environment A or B.

7.3.5.3 Mitigation techniques for HCD manufacturers

The following techniques may be utilized by HCD manufacturers to mitigate this threat:

a) Providing the capability for encrypting fax traffic to and from the HCD

b) Providing the capability to disable the fax function on the HCD

7.3.5.4 Mitigation techniques for IT professionals

The following techniques may be utilized by IT professionals to mitigate this threat:

a) Connecting the HCD's fax port to a secure private telephone network rather than to the public telephone network

b) Ensuring that the authentication mechanisms in the HCD used to control the configuration of the HCD's fax settings are not set to the default values

c) Ensuring that a strong password is selected for all administrator user IDs

d) Ensuring that only authorized administrators have access to the administrator user IDs and passwords

7.3.6 T.DOC.FAX.DIS

7.3.6.1 Definition

User Document Data may be disclosed to unauthorized persons by tapping into a phone line to sniff fax traffic on the PSTN interface (see Table 26).

7.3.6.2 Background

Depending upon proximity to the phone line, equipment for phone line and therefore fax interception is inexpensive and easily obtained. Furthermore, despite common perceptions to the contrary, the public switched telephone network (PSTN) is totally nonsecure and unencrypted fax should never be used for critical information in any case. However, because the process of recovering the faxed image from the intercepted transmission is not trivial, this threat is considered primarily applicable where the information is worth the effort (e.g., Operational Environments A and B).

The only protections against fax interception are the use of encrypted, secure telephone lines or the actual encryption of the fax data. Note that most standard encrypted fax solutions currently offered are Internet fax-based or fax-to-e-mail approaches using Internet protocol-based encryption techniques.

7.3.6.3 Mitigation techniques for HCD manufacturers

The following techniques may be utilized by HCD manufacturers to mitigate this threat:

a) Providing the capability for encrypting fax traffic to and from the HCD

b) Providing the capability to disable the fax function on the HCD

7.3.6.4 Mitigation techniques for IT professionals

The following techniques may be utilized by IT professionals to mitigate this threat:

a) Connecting the HCD’s fax port to a secure private telephone network rather than to the public telephone network

b) Ensuring that the authentication mechanisms in the HCD used to control the configuration of the HCD’s fax settings are not set to the default values

c) Ensuring that a strong password is selected for all administrator user IDs

d) Ensuring that only authorized administrators have access to the administrator user IDs and passwords

7.3.7 T.DOC.INPUT.DIS

7.3.7.1 Definition

User Document Data may be disclosed to unauthorized persons by examining the document while in the original document handler or removing the document from the original document handler (see Table 27).

7.3.7.2 Background

This confidentiality threat is applicable to all scanning devices, whether for making duplicate hard copies, for fax, or for image digitization and storage. Although applicable to all operational environments, the criticality is a function of the cost of compromising the information, which is likely to be higher in Operational Environments A and B.

This threat is similar to T.DOC.OUTPUT.DIS, except that because the hardcopy already exists, only the locked-box technique applies. The corollary to private printing is a policy that requires that the originator stay present during the scanning and takes the copy.

There can be one or multiple locked boxes for the originals; or in a copier or multifunction unit, a common mailbox mechanism could be used for output and input documents. Access to the documents would use identification and authentication mechanisms appropriate to the site.

7.3.7.3 Mitigation techniques for HCD manufacturers

The following techniques may be utilized by HCD manufacturers to mitigate this threat:

a) Providing physically secure original document handler on the HCD

b) Providing an audible alarm when detecting that documents have been left either on the glass or in the document feeder’s output or input trays, whereby an end user is required to explicitly dismiss that alarm after removing the documents

7.3.7.4 Mitigation techniques for IT professionals

The following technique may be utilized by IT professionals to mitigate this threat:

a) Educating users, through training or posted instructions, to remove original documents after scanning or copying them

7.3.8 T.DOC.OUTPUT.DIS

7.3.8.1 Definition

User Document Data may be sent to the output handler and disclosed to unauthorized persons (see Table 28).

7.3.8.2 Background

This is perhaps one of the most obvious confidentiality threats. Although applicable to all operational environments, the criticality is a function of the cost of compromising the information, which is likely to be higher in Operational Environments A and B.

7.3.8.3 Mitigation techniques for HCD manufacturers

The following techniques may be utilized by HCD manufacturers to mitigate this threat:

a) Providing physically locked mailboxes on the HCD, selectable by the end user at the time of print job submission

b) Providing local *secure printing*, whereby the document is held on the HCD’s local hard disk and not printed until the end user releases the document for printing by entering a valid job ID, password, or PIN code

c) Providing server-based secure printing, whereby the document is held in a secure spool area on the print server’s hard disk and not transmitted to the HCD for printing until the end user releases the document by authenticating at the HCD, whether by using an identity card, PIN codes, network security authentication data, or biometric authentication

d) Providing a secure audit trail of the document release events

7.3.8.4 Mitigation techniques for IT professionals

The following techniques may be utilized by IT professionals to mitigate this threat:

a) Implementing network security policies to ensure that all sensitive documents are printed using either HCD- or server-based secure printing

b) Turning on the maximum set of connection restrictions (e.g., white lists, IP or MAC address filtering) that still allow the required secured printing protocols to function

c) Providing appropriate training for users regarding the secure operation of the HCD in the particular operational environment

7.3.9 T.DOC.RETRIEVE.ALT

7.3.9.1 Definition

User Document Data that are retrievable from the HCD may be altered by unauthorized persons (see Table 29).

7.3.9.2 Background

An attacker may be able to access HCD User Document Data electronically from the internal document server, proof print queue, or other internal HCD mechanism used to store User Document Data assets within the HCD via unauthenticated or poorly authenticated access methods that are normally present in the HCD. If access controls are ineffective or bypassed and the HCD allows an attacker to access the User

Document Data assets on the HCD, use of hard disk encryption may not be effective in preventing access to the data.

7.3.9.3 Mitigation techniques for HCD manufacturers

The following techniques may be utilized by HCD manufacturers to mitigate this threat:

a) Providing the ability for the HCD to create a secure message integrity code (MIC), cyclic redundancy check (CRC), or other data integrity check for the data that is stored on the HCD

b) Providing the capability for completely disabling document storage, retrieval, and proof-printing capability in the HCD

c) Providing the capability for disabling unauthenticated document storage, retrieval, and proof-printing capability in the HCD

d) Providing the capability to enforce policies for minimum password or PIN code strength for document storage, retrieval, and proof-printing jobs

e) Providing a comprehensive, secure audit trail for all document storage, retrieval, and proof-printing submissions and access

7.3.9.4 Mitigation techniques for IT professionals

The following techniques may be utilized by IT professionals to mitigate this threat:

a) Disabling all unauthenticated document storage, retrieval, and proof-printing capability in the HCD

b) Where document storage, retrieval, or proof-printing capability is required, enforcing policies for minimum password or PIN code strength for document storage, retrieval, and proof-printing jobs

7.3.10 T.DOC.RETRIEVE.DIS

7.3.10.1 Definition

User Document Data that are retrievable from the HCD may be disclosed to unauthorized persons (see Table 30).

7.3.10.2 Background

An attacker may be able to access HCD User Document Data electronically from the internal document server, proof print queue, or other internal HCD mechanism used to store User Document Data assets within the HCD via unauthenticated or poorly authenticated access methods that are normally present in the HCD. If access controls are ineffective or bypassed and the HCD allows an attacker to access the User Document Data assets on the HCD, use of hard disk encryption may not be effective in preventing access to the data.

7.3.10.3 Mitigation techniques for HCD manufacturers

The following techniques may be utilized by HCD manufacturers to mitigate this threat:

a) Providing the capability for completely disabling document storage, retrieval, and proof-printing capability in the HCD

b) Providing the capability for disabling unauthenticated document storage, retrieval, and proof-printing capability in the HCD

c) Providing the capability to enforce policies for minimum password or PIN code strength for document storage, retrieval, and proof-printing jobs

d) Providing a comprehensive, secure audit trail for all document storage, retrieval, and proof-printing submissions and access

e) Providing configurable access control mechanisms for user access and administrator access to data stored on the HCD

7.3.10.4 Mitigation techniques for IT professionals

The following techniques may be utilized by IT professionals to mitigate this threat:

a) Disabling all document storage, retrieval, and proof-printing capability in the HCD

b) Where document storage, retrieval, or proof-printing capability is required, mandating the use of passwords or PIN codes through either policies or device configuration

c) Providing appropriate training for users regarding the secure operation of the HCD in the particular operational environment

d) Ensuring that only authorized users have access to only those HCD functions for which access has been granted by a security administrator

7.3.11 T.DOC.REST.SAL

7.3.11.1 Definition

User Document Data in a nonvolatile storage medium that has been removed from the HCD may be salvaged by unauthorized persons (see Table 31).

7.3.11.2 Background

Many HCDs provide the capability of sending a User Document to the HCD for future processing or provide the capability to process the document, but hold a copy of the document for later reprinting or processing. When User Document Data is stored in an HCD’s nonvolatile storage, the data is exposed to the threat that the nonvolatile storage media could be removed by an attacker and its contents read on another machine or computer thus bypassing any built in access control mechanism that may be present in the HCD.

7.3.11.3 Mitigation techniques for HCD manufacturers

The following techniques may be utilized by HCD manufacturers to mitigate this threat:

a) Providing the capability for completely disabling document storage, retrieval, and proof-printing capability in the HCD

b) Providing a comprehensive, secure audit trail for all document storage, retrieval, and proof-printing submissions and access

c) Providing secure (e.g., lockable) doors that reduce the likelihood of an unauthorized user gaining access to the internals of the HCD

d) Providing visual or electronic indication of the history of access to internal mechanisms or electronics

e) Ensuring that the HCD enclosure is of sound material and is internally secured

f) Utilizing nonstandard fasteners that require nonstandard or specialized tools for any externally accessible fasteners, and any internal fasteners for components to be access only by authorized technicians

g) Providing alarms for attempted unauthorized access, damage, or disablement, using either audible or remote (e.g., network, radio, pager, or mobile phone) intrusion alarms if panels are forced, or power or signal connectors are disconnected

h) Encrypting all data stored on the hard disk

i) Providing a removable hard disk option, whereby an authenticated administrator is able to quickly and securely remove a hard disk for storage in a secure location

j) Providing a service whereby any hard disk removed while servicing an HCD is verifiably destroyed to prevent analysis of that medium

k) Offering a version of the HCD that does not include persistent storage, or utilizing nonpersistent storage media, such as RAM memory, in place of a conventional hard disk, to ensure that the storage media is automatically erased upon loss of power

7.3.11.4 Mitigation techniques for IT professionals

The following techniques may be utilized by IT professionals to mitigate this threat:

a) Disabling all document storage, retrieval, and proof-printing capability in the HCD

b) Increasing the physical security of the HCD through either placement in a controlled-access location or monitoring of a public-access location

c) Using security cameras or other mechanisms to monitor the HCD

d) Removing the hard disk into secure storage at the end of each day to prevent an attacker from removing the disk while the location is unmonitored

e) Monitoring the HCD equipment for unauthorized entry

f) Ensuring that any service on the HCD equipment is be done by a trusted technician or monitored by security personnel

7.3.12 T.DOC.TRANSIT.ALT

7.3.12.1 Definition

User Document Data in transit over a shared communications medium may be altered by unauthorized persons (see Table 32).

7.3.12.2 Background

Because this threat assumes that the attacker has the ability to impersonate either the sender or the recipient, it can be assumed that a significant amount of effort has been put into the attack.

This threat does not identify the specific method by which the print or scan job transmission is intercepted or the access method that is used to intercept stored data. This threat is essentially a combination of the threats relating to the intercepting of User Document Data or HCD Confidential Data over the network and the threats relating to authentication of users.

7.3.12.3 Mitigation techniques for HCD manufacturers

The following techniques may be utilized by HCD manufacturers to mitigate this threat:

a) Providing support for encryption algorithms that include data integrity checks such as CRCs or MICs for all traffic to and from the HCD

b) Providing the capability to authenticate all print connections to the HCD and all connections to external scan servers from the HCD

c) Implementing IP and MAC address filtering capability

d) Providing a mechanism to secure or lock the HCD’s network connection

7.3.12.4 Mitigation techniques for IT professionals

The following techniques may be utilized by IT professionals to mitigate this threat:

a) Connecting the HCD to the network through a switched, rather than a hub, connection

b) Ensuring that in the case of a switched connection, the network switches’ management and monitoring ports are secured and prevent attackers from enabling monitoring promiscuous mode on those switches

c) Providing a secure, locking connection for the network wall jack connection

7.3.13 T.DOC.TRANSIT.EM.DIS

7.3.13.1 Definition

User Document Data in transit over a shared communications medium may be disclosed to unauthorized persons by capturing EM radiation from the communication medium (see Table 33).

7.3.13.2 Background

EM sniffing generally requires relatively advanced equipment, which suggests that the primary applicability of this threat is to high value information that is otherwise well-protected.

7.3.13.3 Mitigation techniques for HCD manufacturers

The following techniques may be utilized by HCD manufacturers to mitigate this threat:

a) Providing the capability for encrypting network traffic to and from the HCD

b) Where wireless networking is offered, supporting the strongest available encryption mechanism for that networking standard

c) Offering an optical networking capability, such as 100base-FX (see IEEE Std 802.3-2005 [B39], Clause 26) Ethernet, as an option

7.3.13.4 Mitigation techniques for IT professionals

The following techniques may be utilized by IT professionals to mitigate this threat:

a) Implementing an encryption infrastructure to enable HCD traffic to be encrypted

b) Utilizing optical networking to eliminate EM-based network sniffing

c) Where the HCD does not support optical networking, minimizing the length of non-optical Ethernet connections between the HCD and the fiber media converter, and shielding that connecting cable

7.3.14 T.DOC.TRANSIT.DIS

7.3.14.1 Definition

User Document Data in transit over a shared communications medium may be disclosed to unauthorized persons (see Table 34).

7.3.14.2 Background

Although possible in all operational environments, the threat of an attacker sniffing network traffic to intercept User Document Data while in transit to or from an HCD is more of a concern in Operational

Environment A. This is because of both the value of the User Document Data assets present and the types of networks on which the HCD is deployed.

Wireless networks are of particular concern since access to the network cannot be physically controlled. While the attacker requires somewhat specialized software to intercept wireless traffic and break the weaker wireless data-protection protocols, these software tools are readily available on the Internet.

Wired networks can also be subject to attack if the network is deployed using hubs such that all network attached devices share all network traffic. With the use of properly configured network switches in place of hubs, Ethernet traffic to a node is limited to broadcasts and packets specifically addressed to that node. Therefore, communications directed to or from an HCD will not be accessible to a different ordinary node on the network, unless the attacker is able to insert a network device between the switch and the HCD by, for example, unplugging the Ethernet cable from the wall jack and inserting a device between the jack and the HCD.

7.3.14.3 Mitigation techniques for HCD manufacturers

The following techniques may be utilized by HCD manufacturers to mitigate this threat:

a) Providing the capability for encrypting network traffic to and from the HCD

b) Where wireless networking is offered, supporting the strongest available encryption mechanism for that networking standard

c) Providing support for wire-level authentication mechanisms like IEEE 802.1X™ to control port access on the wired network

d) Providing a mechanism to secure or lock the HCD’s network connection

7.3.14.4 Mitigation techniques for IT professionals

The following techniques may be utilized by IT professionals to mitigate this threat:

a) Implementing an encryption infrastructure to enable HCD traffic to be encrypted

b) Connecting the HCD to the network through a switched, rather than a hub, connection

c) Ensuring that in the case of a switched connection, the network switches’ management and monitoring ports are secured and prevent attackers from enabling monitoring promiscuous mode on those switches

d) Providing a secure, locking connection for the network wall jack connection

7.3.15 T.FUNC.REST.ALT

7.3.15.1 Definition

User Function Data in the HCD may be altered by unauthorized persons (see Table 35).

7.3.15.2 Background

Many HCDs provide the capability of sending a *user document* to an HCD for either processing later or provide the capability to process the document, but hold a copy of the document for later reprinting or reprocessing. Along with the User Document Data, there may also be data associated with the processing of the job stored along with the User Document Data for use by the reprint function. If unauthenticated or poorly authenticated access methods are present in the HCD, an attacker can access and modify the User Function Data that may be associated with the user's stored job. If access controls are ineffective or bypassed and the HCD allows an attacker to access the User Function Data assets on the HCD, use of hard disk encryption may not be effective in preventing access to the data.

7.3.15.3 Mitigation techniques for HCD manufacturers

The following techniques may be utilized by HCD manufacturers to mitigate this threat:

a) Providing the ability for the HCD to create a secure MIC, CRC, or other data integrity check for the data that is stored on the HCD

b) Providing the capability for completely disabling document storage, retrieval, and proof-printing capability in the HCD

c) Providing the capability for disabling unauthenticated document storage, retrieval, and proof-printing capability in the HCD

d) Providing the capability to enforce policies for minimum password or PIN code strength for document storage, retrieval, and proof-printing jobs

e) Providing a comprehensive, secure audit trail for all document storage, retrieval, and proof-printing submissions and access

f) Providing configurable access control mechanisms for user access and administrator access to data stored on the HCD

7.3.15.4 Mitigation techniques for IT professionals

The following techniques may be utilized by IT professionals to mitigate this threat:

a) Disabling all unauthenticated document storage, retrieval, and proof-printing capability in the HCD

b) Where document storage, retrieval, or proof-printing capability is required, enforcing policies for minimum password or PIN code strength for document storage, retrieval, and proof-printing jobs

7.3.16 T.FUNC.TRANSIT.ALT

7.3.16.1 Definition

User Function Data in transit over a shared communications medium may be altered by unauthorized persons (see Table 36).

7.3.16.2 Background

Because this threat assumes that the attacker has the ability to impersonate either the sender or the recipient, it can be assumed that a significant amount of effort has been put into the attack.

This threat does not identify the specific method by which the User Function Data transmission is intercepted or the access method that is used.

7.3.16.3 Mitigation techniques for HCD manufacturers

The following techniques may be utilized by HCD manufacturers to mitigate this threat:

a) Providing support for encryption algorithms that include data integrity checks such as CRCs or MICs for all print traffic to the HCD

b) Providing the capability to authenticate all print or scan connections to the HCD

c) Implementing IP and MAC address filtering capability

d) Providing a mechanism to secure or lock the HCD’s network connection

7.3.16.4 Mitigation techniques for IT professionals

The following techniques may be utilized by IT professionals to mitigate this threat:

a) Connecting the HCD to the network through a switched, rather than a hub, connection

b) Ensuring that in the case of a switched connection, the network switches’ management and monitoring ports are secured and prevent attackers from enabling monitoring promiscuous mode on those switches

c) Ensuring that IP and MAC address filtering is enabled and configured to reduce the potential for unauthorized network access to the HCD

d) Providing a secure, locking connection for the network wall jack connection

7.3.17 T.FUNC.TRANSIT.DIS

7.3.17.1 Definition

User Function Data in transit over a shared communications medium may be disclosed to unauthorized persons (see Table 37).

7.3.17.2 Background

Although possible in all operational environments, the threat of an attacker sniffing network traffic to intercept User Function Data while in transit to or from an HCD is more of a concern in Operational Environment A.

Wireless networks are of particular concern since access to the network cannot be physically controlled. While the attacker requires somewhat specialized software to intercept wireless traffic and break the weaker wireless data-protection protocols, these software tools are readily available on the Internet.

Wired networks can also be subject to attack if the network is deployed using hubs such that all network attached devices share all network traffic. With the use of properly configured network switches in place of hubs, Ethernet traffic to a node is limited to broadcasts and packets specifically addressed to that node. Therefore, communications directed to or from an HCD will not be accessible to a different ordinary node on the network, unless the attacker is able to insert a network device between the switch and the HCD by, for example, unplugging the Ethernet cable from the wall jack and inserting a device between the jack and the HCD.

7.3.17.3 Mitigation techniques for HCD manufacturers

The following techniques may be utilized by HCD manufacturers to mitigate this threat:

a) Providing the capability for encrypting network traffic to and from the HCD

b) Where wireless networking is offered, supporting the strongest available encryption mechanism for that networking standard

c) Providing support for wire-level authentication mechanisms like IEEE 802.1X to control port access on the wired network

d) Providing a mechanism to secure or lock the HCD’s network connection

7.3.17.4 Mitigation techniques for IT professionals

The following techniques may be utilized by IT professionals to mitigate this threat:

a) Implementing an encryption infrastructure to enable HCD traffic to be encrypted

b) Connecting the HCD to the network through a switched, rather than a hub, connection

c) Ensuring that in the case of a switched connection, the network switches’ management and monitoring ports are secured and prevent attackers from enabling monitoring promiscuous mode on those switches

d) Providing a secure, locking connection for the network wall jack connection

7.4 Mitigating threats to HCD Confidential and Protected Data

7.4.1 T.CONF.CAMERA.DIS

7.4.1.1 Definition

HCD Confidential Data may be disclosed to unauthorized persons by capturing this data with an external camera as it is entered into the HCD (see Table 38).

7.4.1.2 Background

The complexity of this attack and potential cost of equipment suggests that it is primarily applicable to Operational Environment A, although with the advent of inexpensive networked cameras, other types of organizations should also be aware of this. As an example of this type of attack, there have been cases of hidden cameras recording users entering ATM PINs, with obvious repercussions.

Although some design features can assist in mitigating this threat, protection primarily requires vigilance on the part of personnel maintaining the device and the site. Any signs of equipment entry, new objects in the vicinity, or changes in the positions of existing objects should be investigated. Any service on the equipment should be done by a trusted technician or while properly monitored.

7.4.1.3 Mitigation techniques for HCD manufacturers

The following technique may be utilized by HCD manufacturers to mitigate this threat:

a) Offering visual shielding for the original document handler, output trays, and the operator panel of the HCD

7.4.1.4 Mitigation techniques for IT professionals

The following techniques may be utilized by IT professionals to mitigate this threat:

a) Increasing the physical security of the HCD through either placement in a controlled-access location or monitoring of a public-access location

b) Providing additional visual shielding of the HCD from possible external hidden cameras

c) Using security cameras or other mechanisms to monitor the HCD

d) Monitoring the HCD equipment for unauthorized entry, for new objects in the vicinity of the HCD, or changes in the positions of existing objects

e) Ensuring that any service on the HCD equipment be done by a trusted technician or monitored by security personnel

7.4.2 T.CONF.GUESS.DIS

7.4.2.1 Definition

HCD Confidential Data may be disclosed to unauthorized persons by guessing or by observing the data as it is entered into the HCD (see Table 39).

7.4.2.2 Background

Devices with weak passwords can easily be compromised. Users who are not aware of observers may inadvertently disclose their password. Other techniques for obtaining user passwords, such as using social engineering, are not included in this threat. Those threats are addressed by increasing the security awareness of users.

7.4.2.3 Mitigation techniques for HCD manufacturers

The following techniques may be utilized by HCD manufacturers to mitigate this threat:

a) Providing user credential policies for minimum password length and complexity

b) Providing password expiry capability

c) Providing temporary or permanent lockout capabilities in case of excessive authentication failures

d) Requiring the administrator password to be changed on first power on of the HCD

e) Providing visual shielding for entry of user authentication data on the operator panel of the HCD

7.4.2.4 Mitigation techniques for IT professionals

The following techniques may be utilized by IT professionals to mitigate this threat:

a) Enforcing password policies mandating such characteristics as minimum length, complexity, and expiry

b) Educating users to exercise care in selecting passwords and in entering user authentication data at the operator panel of the HCD

c) Providing appropriate training for users regarding the secure operation of the HCD in the particular operational environment

7.4.3 T.CONF.REST.ALT

7.4.3.1 Definition

HCD Confidential Data in the HCD may be altered by unauthorized persons (see Table 41).

7.4.3.2 Background

The considerations and mitigation techniques for this threat are the same as for T.PROT.REST.ALT, except that changing security settings requires the highest levels of authority and the strongest authentication applicable to the environment.

7.4.3.3 Mitigation techniques for HCD manufacturers

The following techniques may be utilized by HCD manufacturers to mitigate this threat:

a) Requiring security administrator authorization for any change to any security settings

b) Providing the capability for the HCD to create and securely maintain a log of security-related and usage-related events

c) Providing configurable access control mechanisms for user access and administrator access to data stored on the HCD

7.4.3.4 Mitigation techniques for IT professionals

The following techniques may be utilized by IT professionals to mitigate this threat:

a) Ensuring that a strong password is selected for all security administrator user IDs

b) Ensuring that only authorized security administrators have access to a given security administrator user ID and password

c) Providing appropriate training for administrators regarding the security requirements of the HCD's environment and provide the training and time for the administrator to follow the manufacturer's guidance and documentation to correctly configure and operate the HCD in accordance with those requirements

d) Ensure that appropriate human resource controls have been applied to security administrators, such as background screening, separation of duties, and rotation of duties (see Department of Homeland Security [B16] and ISO/IEC 27001:2005 [B71])

e) Perform periodic external audits of security administrator activities

7.4.4 T.CONF.REST.DIS

7.4.4.1 Definition

HCD Confidential Data in the HCD may be disclosed to unauthorized persons (see Table 41).

7.4.4.2 Background

Unauthorized access to very sensitive data such as audit logs or stored authentication data, while not providing an attacker with direct access to User Document Data, may provide an attacker with information that can be used in either a T.CONF.GUESS.DIS type of attack, a social engineering attack (e.g., using the name of the document to solicit details about its content), or an attack on other systems in the HCD's IT environment.

7.4.4.3 Mitigation techniques for HCD manufacturers

The following techniques may be utilized by HCD manufacturers to mitigate this threat:

a) Providing support for strong authentication mechanisms for administrator access

b) Requiring auditor-level authorization for any access to the audit logs

c) Requiring appropriate authorization for any connection to the HCD's audit logs from a server-based auditing application

d) Ensuring that any authentication data stored on the HCD are encrypted

e) Ensuring that any audit logs stored on the HCD are encrypted

f) Ensuring that all network access to the audit logs is encrypted

7.4.4.4 Mitigation techniques for IT professionals

The following techniques may be utilized by IT professionals to mitigate this threat:

a) Ensuring that a strong password is selected for all administrator user IDs

b) Ensuring that only authorized security administrators have access to a given security administrator user ID and password

c) Ensuring that any audit logs stored on a remote server are stored in an encrypted form or protected by an access control mechanism

d) Ensuring that appropriate human resource controls have been applied to security administrators, such as background screening, separation of duties, and rotation of duties

e) Perform periodic external audits of security administrator activities

7.4.5 T.CONF.TRANSIT.ALT

7.4.5.1 Definition

HCD Confidential Data in transit over a shared communications medium may be altered by unauthorized persons (see Table 42).

7.4.5.2 Background

The HCD should ensure that authentication data such as PINs and passwords are reasonably strong and that they are stored and transmitted in encrypted form. In more critical situations, more detailed authentication such as smart cards or biometric devices should be used.

7.4.5.3 Mitigation techniques for HCD manufacturers

The following techniques may be utilized by HCD manufacturers to mitigate this threat:

a) Providing the capability for encrypting all network management traffic to and from the HCD

b) Where wireless networking is offered, supporting the strongest available encryption mechanism for that networking standard

c) Providing a mechanism to secure or lock the HCD's network connection

d) Accepting management connections only from networked HCD management tools whose authenticity can be verified

e) Ensuring that the networked HCD management tools only connect to HCDs whose authenticity can be verified

f) Providing the ability to create specific connection restrictions, such as IP address or MAC address white lists, for the management tools

7.4.5.4 Mitigation techniques for IT professionals

The following techniques may be utilized by IT professionals to mitigate this threat:

a) Implementing an encryption infrastructure to enable HCD traffic to be encrypted

b) Connecting the HCD to the network through a switched, rather than a hub, connection

c) Ensuring that in the case of a switched connection, the network switches' management and monitoring ports are secured and prevent attackers from enabling monitoring promiscuous mode on those switches

d) Providing a secure, locking connection for the network wall jack connection

7.4.6 T.CONF.TRANSIT.DIS

7.4.6.1 Definition

HCD Confidential Data in transit over a shared communications medium may be disclosed to unauthorized persons (see Table 43).

7.4.6.2 Background

Although possible in all operational environments, the threat of an attacker sniffing network traffic to intercept authentication data while in transit to or from an HCD is more of a concern in Operational Environments A and B due to both the value of the data itself as well as the value of other assets that may be compromised by using the disclosed information.

Wireless networks are of particular concern since access to the network cannot be physically controlled. While the attacker requires somewhat specialized software to intercept wireless traffic and break the weaker wireless data-protection protocols, these software tools are readily available on the Internet.

Wired networks can also be subject to attack if the network is deployed using hubs such that all network attached devices share all network traffic. With the use of properly configured network switches in place of hubs, Ethernet traffic to a node is limited to broadcasts and packets specifically addressed to that node. Therefore, communications directed to or from an HCD will not be accessible to a different ordinary node on the network, unless the attacker is able to insert a network device between the switch and the HCD by, for example, unplugging the Ethernet cable from the wall jack and inserting a device between the jack and the HCD.

7.4.6.3 Mitigation techniques for HCD manufacturers

The following techniques may be utilized by HCD manufacturers to mitigate this threat:

a) Providing the capability for encrypting all user authentication data transmitted over the network to or from the HCD

b) Where wireless networking is offered, supporting the strongest available encryption mechanism for that networking standard

c) Providing a mechanism to secure or lock the HCD's network connection

7.4.6.4 Mitigation techniques for IT professionals

The following techniques may be utilized by IT professionals to mitigate this threat:

a) Implementing an encryption infrastructure to enable HCD traffic to be encrypted

b) Connecting the HCD to the network through a switched, rather than a hub, connection

c) Ensuring that in the case of a switched connection, the network switches' management and monitoring ports are secured and prevent attackers from enabling monitoring promiscuous mode on those switches

d) Providing a secure, locking connection for the network wall jack connection

7.4.7 T.CONF.TRANSIT.EM.DIS

7.4.7.1 Definition

HCD Confidential Data in transit over a shared communications medium may be disclosed to unauthorized persons by capturing the EM radiation from the communication medium (see Table 44).

7.4.7.2 Background

EM sniffing generally requires fairly complicated equipment, which suggests that the primary applicability of this threat is to high value information that is otherwise well-protected.

The considerations here are similar to those for T.DOC.TRANSIT.EM.DIS. The distinction is that encrypting and shielding HCD Confidential Data requires less processing overhead than encrypting and shielding all job content.

7.4.7.3 Mitigation techniques for HCD manufacturers

The following techniques may be utilized by HCD manufacturers to mitigate this threat:

a) Providing the capability for encrypting all user authentication data transmitted over the network to or from the HCD

b) Where wireless networking is offered, supporting the strongest available encryption mechanism for that networking standard

c) Offering an optical networking capability, such as 100base-FX Ethernet as an option

7.4.7.4 Mitigation techniques for IT professionals

The following techniques may be utilized by IT professionals to mitigate this threat:

a) Implementing an encryption infrastructure to enable HCD traffic to be encrypted

b) Utilizing optical networking to eliminate EM-based network sniffing

c) Where the HCD does not support optical networking, minimizing the length of non-optical Ethernet connections between the HCD and the fiber-optic cable media converter, and shielding that connecting cable

7.4.8 T.PROT.REST.ALT

7.4.8.1 Definition

HCD Protected Data in the HCD may be altered by unauthorized persons (see Table 45).

7.4.8.2 Background

Some information stored on an HCD may be accessed by any user, but should not be modified or deleted without a higher level of authorization. One example of this is a list of shortcuts for phone number or e-mail distribution lists. Any user might be able to use the shortcut to send his User Document Data to a distribution list, but the specific phone numbers or e-mail addresses on that list may be under administrative control.

7.4.8.3 Mitigation techniques for HCD manufacturers

The following techniques may be utilized by HCD manufacturers to mitigate this threat:

a) Requiring administrator authorization for any change to any device settings that would affect a user other than the user making the change

b) Requiring administrator authorization for any change to any networking settings

c) Providing configurable access control mechanisms for user access and administrator access to data stored on the HCD

7.4.8.4 Mitigation techniques for IT professionals

The following techniques may be utilized by IT professionals to mitigate this threat:

a) Ensuring that a strong password is selected for all administrator user IDs

b) Ensuring that only authorized administrators have access to the administrator user IDs and passwords

c) Ensuring that appropriate human resource controls have been applied to security administrators, such as background screening, separation of duties, and rotation of duties

d) Perform periodic external audits of security administrator activities

7.4.9 T.PROT.TRANSIT.ALT

7.4.9.1 Definition

HCD Protected Data in transit over a shared communications medium may be altered by unauthorized persons (see Table 46).

7.4.9.2 Background

Some information that is either used by or generated by and HCD requires protection against modification, but not necessarily protection against disclosure or access while being sent to or received from an HCD. Examples of this type of data include accounting logs that may be used by a fleet management package, or a particular set of fonts or forms that may be downloaded as part of a print job.

7.4.9.3 Mitigation techniques for HCD manufacturers

The following techniques may be utilized by HCD manufacturers to mitigate this threat:

a) Providing support for network transports that include secure data integrity checks such as CRCs or MICs for all traffic to or from the HCD

b) Providing the capability for encrypting all network management traffic to and from the HCD

c) Where wireless networking is offered, supporting the strongest available encryption mechanism for that networking standard

d) Providing a mechanism to secure or lock the HCD's network connection

e) Accepting management connections only from networked HCD management tools whose authenticity can be verified

f) Ensuring that the networked HCD management tools only connect to HCDs whose authenticity can be verified

g) Providing the ability to create specific connection restrictions, such as IP address or MAC address white lists, for the management tools

7.4.9.4 Mitigation techniques for IT professionals

The following techniques may be utilized by IT professionals to mitigate this threat:

a) Implementing an encryption infrastructure to enable HCD traffic to be encrypted

b) Connecting the HCD to the network through a switched, rather than a hub, connection

c) Ensuring that in the case of a switched connection, the network switches' management and monitoring ports are secured and prevent attackers from enabling monitoring promiscuous mode on those switches

d) Providing a secure, locking connection for the network wall jack connection

7.5 Mitigating threats to HCD software

7.5.1 T.SW.APPLET.ALT

7.5.1.1 Definition

HCD software applets in the HCD may be altered by unauthorized persons (see Table 47).

7.5.1.2 Background

The convenience of being able to customize an HCD with an applet is very attractive. The potential threat, however, is applicable to all operational environments.

7.5.1.3 Mitigation techniques for HCD manufacturers

The following techniques may be utilized by HCD manufacturers to mitigate this threat:

a) Ensuring that only administrators have the ability to install or uninstall applets

b) Providing the option for the security administrator to disable the operation of all applets

c) Providing the option for the security administrator to disable the installation of additional applets

d) Validating the authenticity of any applets at the time of installation, by means of digital signature or otherwise

e) Validating the compatibility of any applets at the time of installation with the specific model of HCD

f) Controlling access to the applet development tools to trusted internal and third-party developers

g) Performing validation or certification testing on third-party-developed applets prior to providing those developers with the capability to sign the applets

h) Recording all applet install or uninstall events in the HCD's security log

i) Ensuring that applet installations can be performed only through either physical connections (e.g., using a local connection or a memory card) or encrypted network connections

j) Ensuring that the applet environment prevents applets from changing the device security settings

k) Minimizing the opportunities for an applet to disrupt the operation of the standard HCD functionality, including, but not limited to, copying, printing, scanning, PSTN faxing, and remote device management

l) Providing the capability for an authorized management tool to remotely retrieve details of all installed applets

m) Performing a check of the integrity and validity of the installed applets each time the HCD boots

7.5.1.4 Mitigation techniques for IT professionals

The following techniques may be utilized by IT professionals to mitigate this threat:

a) Selecting in advance what applets are required, if any, and testing those applets for additional vulnerabilities prior to full deployment

b) Once required applets are installed, disabling the installation of further applets

c) Regularly auditing the list of installed applets on each HCD and validating that against the list of authorized applets

d) Regularly auditing the security log on each HCD for applet install and uninstall events

7.5.2 T.SW.FIRMWARE.ALT

7.5.2.1 Definition

HCD firmware in the HCD may be altered by unauthorized persons (see Table 48).

7.5.2.2 Background

This threat has been defined as applicable to all environments. The ability to update or modify the firmware on an HCD allows fielded units to be kept up-to-date with bug fixes and updated features.

7.5.2.3 Mitigation techniques for HCD manufacturers

The following techniques may be utilized by HCD manufacturers to mitigate this threat:

a) Ensuring that only administrators have the ability to install firmware updates

b) Providing the option for the security administrator to disable the installation of firmware updates

c) Validating the authenticity of any firmware updates at the time of installation, by means of digital signature or other means

d) Validating the compatibility of any firmware updates at the time of installation with the specific model of HCD

e) Recording all firmware update events in the HCD's security log

f) Ensuring that firmware updates can be performed only through either physical connections (e.g., using a local connection or a memory card) or encrypted network connections

g) Providing the capability for an authorized management tool to remotely retrieve details of all installed firmware updates

h) Performing a check of the integrity and validity (e.g., checksum, CRC, digital signature) of the installed firmware each time the HCD boots

7.5.2.4 Mitigation techniques for IT professionals

The following techniques may be utilized by IT professionals to mitigate this threat:

a) Selecting in advance what firmware updates are required, if any, and testing that firmware for additional vulnerabilities prior to full deployment

b) Once required firmware updates are installed, disabling the installation of further firmware updates

c) Regularly auditing the list of installed firmware on each HCD and validating that against the list of authorized firmware updates

d) Regularly auditing the security log on each HCD for firmware update events

7.6 Mitigating threats to the HCD External Environment

7.6.1 T.ENV.DOS

7.6.1.1 Definition

The External Environment may be interrupted by unauthorized persons by creating a DoS attack on the local network using the HCD’s interface (see Table 49).

7.6.1.2 Background

Improperly designed HCD networking components may improperly propagate DoS attacks to other devices on the network.

7.6.1.3 Mitigation techniques for HCD manufacturers

The following techniques may be utilized by the HCD manufacturers to mitigate this threat:

a) Providing the ability to disable individual protocols and ports on the device

b) Providing address or destination filters to block or permit connections from known or unknown hosts (e.g., white list, black list of IP, MAC, phone)

c) If downloadable applets are supported, implementing Mitigation Techniques for the T.SW.APPLET.ALT threat

d) If a standard off-the-shelf (OTS) OS is used, disable or, preferably, remove all unused services (e.g., unused telnet server)

7.6.1.4 Mitigation techniques for IT professionals

The following techniques may be utilized by IT professionals to mitigate this threat:

a) Disabling all unnecessary ports and protocols

b) Ensuring all configuration PINs and passwords are robustly set

c) Implementing network access authentication (e.g., IEEE 802.1X) to tightly control access to the network

7.6.2 T.ENV.FAXBRIDGE

7.6.2.1 Definition

The External Environment or the HCD's internal components and software may be accessed by unauthorized persons via the fax connection (see Table 50).

7.6.2.2 Background

In some operational environments, especially Operational Environment A, users may be concerned about the threat of the fax connection on an HCD providing access to their internal network using the HCD as a data bridge. This is because a fax is from an outside network and is a connection that is usually not part of the environment's firewall protection. Many HCD fax interfaces also have the capability to support a data modem function in addition to a fax modem function. This is because it is either an inherent part of the modem chip set or because it is used for remote debug or management.

7.6.2.3 Mitigation techniques for HCD manufacturers

The following techniques may be utilized by the HCD manufacturers to mitigate this threat:

a) Ensuring that no mechanism exists that allows non-fax data between any other data interface and the HCD's fax connection subsystem

b) Ensuring that the HCD's fax connection subsystem does not allow negotiation to a data modem connection

c) Ensuring that the software and firmware used to operate the fax connection is logically isolated from the other software, firmware, and non-fax related memory spaces on the HCD

d) Ensuring that data modem capability for debug purposes can be disabled in the HCD

e) Providing the capability to disable the fax function on the HCD

f) Ensuring that configuration of the HCD's fax connection (including both enabling and disabling) requires administrator authorization

7.6.2.4 Mitigation techniques for IT professionals

The following techniques may be utilized by IT professionals to mitigate this threat:

a) Connecting the HCD's fax port to a secure private telephone network rather than to the public telephone network

b) Ensuring that the authentication mechanisms in the HCD used to control the configuration of the fax connection are not set to the default values

7.6.3 T.ENV.PROXY.DOS

7.6.3.1 Definition

The External Environment may be interrupted by unauthorized persons by propagating an attack to the local network through a network service on the HCD (see Table 51).

7.6.3.2 Background

Attacks using the HCD as an intermediary may hide the true source of an attack.

7.6.3.3 Mitigation techniques for HCD manufacturers

The following techniques may be utilized by the HCD manufacturers to mitigate this threat:

a) Providing the ability to disable individual protocols and ports on the device

b) Providing address or destination filters to block or permit connections from known or unknown hosts (e.g., white list, black list of IP, MAC, phone)

c) If downloadable applets are supported, implementing the Mitigation techniques for the T.SW.APPLET.ALT threat

d) If a standard OTS OS is used, disabling or, preferably, removing all unused services (e.g., unused telnet server)

e) Ensuring that the protocol stacks for external unprotected interfaces like fax are completely isolated from the other interface protocol stacks

f) Ensuring that the internal communication paths between subsystems (e.g., a wireless link between the operator panel and the main HCD processor subsystem) of the HCD cannot introduce security exposures

7.6.3.4 Mitigation techniques for IT professionals

The following techniques may be utilized by IT professionals to mitigate this threat:

a) Disabling all unnecessary ports and protocols

b) Ensuring all configuration PINs and passwords are robustly set

c) Implementing network access authentication (e.g., IEEE 802.1X) to tightly control access to the network

8. Compliance

8.1 Compliance security objectives for HCD manufacturers

This subclause describes the security objectives that a manufacturer's product is required to meet in order to claim compliance to this standard. To claim compliance to this standard, a manufacturer's product shall meet all requirements for a given operational environment.

Techniques provided in this clause and Clause 7 are meant as examples; HCD manufacturers may use any suitable technique(s) to meet the objectives.

8.1.1 Security objectives for the HCD in Environment A

8.1.1.1 Protecting HCD software from unauthorized modification

The HCD shall provide procedures to verify that the currently installed software in the HCD is consistent with the authorized, installed HCD software.

For example, one possible technique may be found in 7.5.2.3:

— Performing a check of the integrity and validity (e.g., checksum, CRC, digital signature) of the installed firmware each time the HCD boots

8.1.1.2 User identification and authentication

The HCD shall identify and authenticate each user who tries to access HCD assets or execute HCD applications.

For example, one possible technique may be found in 7.1.9.3:

— Providing the capability to enable only protocols that require user authentication before jobs can be sent to the HCD

8.1.1.3 User authorization

The HCD shall ensure that users are authorized prior to permitting access to HCD assets and performance of HCD functions.

The HCD shall also ensure that *unauthorized users* are not permitted to access HCD assets or execute HCD applications including installation or update of firmware, software, and *applet.*

For example, one possible technique may be found in 7.2.2.3:

— Providing the ability for the administrator to define and set rules governing permissions given to users or groups of users, such as for access to print, scan, fax, or copy functions, access to color printing, or limits on the number of pages that can be processed

8.1.1.4 Offline salvage of deleted or stored User Document Data

The HCD shall ensure that user documents that have been logically deleted or released after use cannot be recovered from nonvolatile storage devices that have been removed from the HCD.

The HCD shall also ensure that user documents that have been stored in the HCD cannot be recovered from nonvolatile storage devices that have been removed from the HCD.

For example, possible techniques may be found in 7.3.3.3 and 7.3.11.3:

- Providing the option for the HCD to automatically overwrite deleted data on the HCD's hard disk using an effective wiping technique, whether immediately upon deletion of that data or as an automatically scheduled task
- Encrypting all data stored on the hard disk

8.1.1.5 Protecting User Document Data, User Function Data, HCD Confidential Data, HCD Protected Data, and software in the HCD

8.1.1.5.1 From disclosure

The HCD shall protect User Document Data and HCD Confidential Data from unauthorized disclosure when such data is in the HCD.

For example, possible techniques may be found in 7.3.8.3, 7.4.4.3, and 7.3.10.3:

- Providing local *secure printing,* whereby the document is held on the HCD's local hard disk and not printed until the end user releases the document for printing by entering a valid job ID, password, or PIN code
- Providing server-based secure printing, whereby the document is held in a secure spool area on the print server's hard disk and not transmitted to the HCD for printing until the end user releases the document by authenticating at the HCD, whether by using an identity card, PIN codes, network security authentication data, or biometric authentication
- Providing support for strong authentication mechanisms for administrator access
- Ensuring that any authentication data stored on the HCD are encrypted
- Providing configurable access control mechanisms for user access and administrator access to data stored on the HCD

8.1.1.5.2 From modification

The HCD shall protect User Document Data, User Function Data, HCD Confidential Data, HCD Protected Data, and software from unauthorized modification when such data is in the HCD.

For example, one possible technique may be found in 7.3.10.3:

- Providing configurable access control mechanisms for user access and administrator access to data stored on the HCD

8.1.1.6 Protecting User Document Data, User Function Data, HCD Confidential Data, HCD Protected Data, and software in transit

8.1.1.6.1 From disclosure

The HCD shall protect User Document Data and HCD Confidential Data from unauthorized disclosure when such data is in transit to or from the HCD over a shared communications medium.

For example, one possible technique may be found in 7.3.14.3:

- Providing the capability for encrypting network traffic to and from the HCD

8.1.1.6.2 From modification

The HCD shall protect User Document Data, User Function Data, HCD Confidential Data, HCD Protected Data, and software from unauthorized modification when such data is in transit to or from the HCD over a shared communications medium.

For example, one possible technique may be found in 7.1.12.3:

- Providing support for encryption algorithms that include data integrity checks such as CRCs or MICs for all traffic to and from the HCD

8.1.1.7 Administrator identification, authentication, and authorization

The HCD shall identify and authenticate each HCD administrator and shall ensure that administrators are authorized prior to permitting access to HCD data assets and performance of administration functions on the HCD.

For example, one possible technique may be found in 7.4.4.3:

- Providing support for strong authentication mechanisms for administrator access

8.1.1.8 Monitoring of HCD events

The HCD shall create and maintain a log of HCD use and security-relevant events.

For example, one possible technique may be found in 7.4.3.3:

- Providing the capability for the HCD to create and securely maintain a log of security-related and usage-related events

8.1.1.9 HCD cannot be used as a proxy for malicious attacks

The HCD shall ensure that its shared communication media interfaces cannot be used as a proxy for or a source of malicious attacks on the external IT environment.

For example, possible techniques may be found in 7.6.3.3:

- Providing the ability to disable individual protocols and ports on the device

- Providing address or destination filters to block or permit connections from known or unknown hosts (e.g., white list, black list of IP, MAC, phone)

8.1.1.10 HCD cannot be used as an unauthorized bridge from one interface to a shared communications media interface

If a shared communication interface (e.g., network connection) is present on the HCD, the HCD shall not permit users to establish a malicious connection to the external IT environment from any other interface. In addition, the HCD should not permit an unauthorized non-fax data connection to the HCD via the fax interface.

For example, possible techniques may be found in 7.6.2.3 and 7.6.3.3:

- Providing the capability to disable the fax function on the HCD
- Ensuring that the protocol stacks for external unprotected interfaces like fax are completely isolated from the other interface protocol stacks

8.1.1.11 Mitigation of denial of service attack

The HCD should protect assets during DoS attacks against the external HCD interfaces and should restore normal operation without requiring human intervention upon termination of such attacks.

For example, techniques that may be used to address this requirement may be found in 7.1.11.3 and 7.1.9.3:

- Ensuring that even where an attack of this type causes failure of the network interface on the HCD, it does not interfere with the operation of those HCD subsystems that do not require network access
- Ensuring that the HCD implements a best effort mechanism to recover automatically when the network interface is nonresponsive
- Providing the capability to enable only protocols that require user authentication before jobs can be sent to the HCD

8.1.2 Security objectives for the HCD in Environment B

8.1.2.1 Protecting HCD software from unauthorized modification

The HCD shall provide procedures to verify that the currently installed software in the HCD is consistent with the authorized, installed HCD software.

For example, one possible technique may be found in 7.5.2.3:

- Performing a check of the integrity and validity (e.g., checksum, CRC, digital signature) of the installed firmware each time the HCD boots

8.1.2.2 User identification and authentication

The HCD shall identify and authenticate each user who tries to access HCD assets or execute HCD applications.

For example, one possible technique may be found in 7.1.9.3:

- Providing the capability to enable only protocols that require user authentication before jobs can be sent to the HCD

8.1.2.3 User authorization

The HCD shall ensure that users are authorized prior to permitting access to HCD assets and performance of HCD functions.

The HCD shall also ensure that Unauthorized Users are not permitted to access HCD assets or execute HCD applications including installation or update of firmware, software, and applet.

For example, one possible technique may be found in 7.2.2.3:

- Providing the ability for the administrator to define and set rules governing permissions given to users or groups of users, such as for access to print, scan, fax, or copy functions, access to color printing, or limits on the number of pages that can be processed

8.1.2.4 Offline salvage of deleted or stored User Document Data

The HCD shall ensure that user documents that have been logically deleted or released after use cannot be recovered from nonvolatile storage devices that have been removed from the HCD.

The HCD shall also ensure that user documents that have been stored in the HCD cannot be recovered from nonvolatile storage devices that have been removed from the HCD.

For example, possible techniques may be found in 7.3.3.3 and 7.3.11.3:

- Providing the option for the HCD to automatically overwrite deleted data on the HCD's hard disk using an effective wiping technique, whether immediately upon deletion of that data or as an automatically scheduled task
- Encrypting all data stored on the hard drive

8.1.2.5 Protecting User Document Data, User Function Data, HCD Confidential Data, HCD Protected Data, and software in the HCD

8.1.2.5.1 From disclosure

The HCD shall protect User Document Data and HCD Confidential Data from unauthorized disclosure when such data is in the HCD.

For example, possible techniques may be found in 7.3.8.3, 7.4.4.3, and 7.3.10.3:

- Providing local secure printing, whereby the document is held on the HCD's local hard disk and not printed until the end user releases the document for printing by entering a valid job ID, password, or PIN code
- Providing server-based secure printing, whereby the document is held in a secure spool area on the print server's hard disk and not transmitted to the HCD for printing until the end user releases the document by authenticating at the HCD, whether by using an identity card, PIN codes, network security authentication data, or biometric authentication
- Providing support for strong authentication mechanisms for administrator access

- Ensuring that any authentication data stored on the HCD are encrypted
- Providing configurable access control mechanisms for user access and administrator access to data stored on the HCD

8.1.2.5.2 From modification

The HCD shall protect User Document Data, User Function Data, HCD Confidential Data, HCD Protected Data, and software from unauthorized modification when such data is in the HCD.

For example, one possible technique may be found in 7.3.10.3:

- Providing configurable access control mechanisms for user access and administrator access to data stored on the HCD

8.1.2.6 Protecting HCD Confidential Data, HCD Protected Data, and software in transit

8.1.2.6.1 From disclosure

The HCD shall protect HCD Confidential Data from unauthorized disclosure when such data is in transit to or from the HCD over a shared communications medium.

For example, one possible technique may be found in 7.3.14.3:

- Providing the capability for encrypting network traffic to and from the HCD

8.1.2.6.2 From modification

The HCD shall protect HCD Confidential Data, HCD Protected Data, and software from unauthorized modification when such data is in transit to or from the HCD over a shared communications medium.

For example, one possible technique may be found in 7.1.12.3:

- Providing support for encryption algorithms that include data integrity checks such as CRCs or MICs for all traffic to and from the HCD

8.1.2.7 Administrator identification, authentication, and authorization

The HCD shall identify and authenticate each HCD administrator and shall ensure that administrators are authorized prior to permitting access to HCD data assets and performance of administration functions on the HCD.

For example, one possible technique may be found in 7.4.4.3:

- Providing support for strong authentication mechanisms for administrator access

8.1.2.8 Monitoring of HCD events

The HCD shall create and maintain a log of HCD use and security-relevant events.

For example, one possible technique may be found in 7.4.3.3:

- Providing the capability for the HCD to create and securely maintain a log of security-related and usage-related events

8.1.2.9 HCD cannot be used as a proxy for malicious attacks

The HCD shall ensure that its shared communication media interfaces cannot be used as a proxy for or a source of malicious attacks on the external IT environment.

For example, possible techniques may be found in 7.6.3.3:

- Providing the ability to disable individual protocols and ports on the device
- Providing address or destination filters to block or permit connections from known or unknown hosts (e.g., white list, black list of IP, MAC, phone)

8.1.2.10 HCD cannot be used as an unauthorized bridge from one interface to a shared communications media interface

If a shared communication interface (e.g., network connection) is present on the HCD, the HCD shall not permit users to establish a malicious connection to the external IT environment from any other interface. In addition, the HCD should not permit an unauthorized non-fax data connection to the HCD via the fax interface.

For example, possible techniques may be found in 7.6.2.3 and 7.6.3.3:

- Providing the capability to disable the fax function on the HCD
- Ensuring that the protocol stacks for external unprotected interfaces like fax are completely isolated from the other interface protocol stacks

8.1.2.11 Mitigation of denial of service attack

The HCD should protect assets during DoS attacks against the external HCD interfaces, and should restore normal operation without requiring human intervention upon termination of such attacks.

For example, techniques that may be used to address this requirement may be found in 7.1.11.3 and 7.1.9.3:

- Ensuring that even where an attack of this type causes failure of the network interface on the HCD, it does not interfere with the operation of those HCD subsystems that do not require network access.
- Ensuring that the HCD implements a best effort mechanism to recover automatically when the network interface is nonresponsive
- Providing the capability to enable only protocols that require user authentication before jobs can be sent to the HCD

8.1.3 Security objectives for the HCD in Environment C

8.1.3.1 Protecting HCD software from unauthorized modification

The HCD shall provide procedures to verify that the currently installed software in the HCD is consistent with the authorized, installed HCD software.

For example, one possible technique may be found in 7.5.2.3:

- Performing a check of the integrity and validity (e.g., checksum, CRC, digital signature) of the installed firmware each time the HCD boots

8.1.3.2 Deletion of residual User Document Data

The HCD shall ensure that User Documents that have been logically deleted or released after use cannot be recovered from nonvolatile storage devices that have been removed from the HCD.

For example, one possible technique may be found in 7.3.3.3:

- Providing the option for the HCD to automatically overwrite deleted data on the HCD's hard disk using an effective wiping technique, whether immediately upon deletion of that data or as an automatically scheduled task

8.1.3.3 Protecting HCD Confidential Data, HCD Protected Data, and software in the HCD

8.1.3.3.1 From disclosure

The HCD shall protect HCD Confidential Data from unauthorized disclosure when such data is in the HCD.

For example, possible techniques may be found in 7.4.4.3:

- Providing support for strong authentication mechanisms for administrator access
- Ensuring that any authentication data stored on the HCD are encrypted

8.1.3.3.2 From modification

The HCD shall protect HCD Confidential Data, HCD Protected Data, and software from unauthorized modification when such data is in the HCD.

For example, one possible technique may be found in 7.3.9.3:

- Providing the ability for the HCD to create a secure MIC, CRC, or other data integrity check for the data that is stored on the HCD

8.1.3.4 Protecting HCD Confidential Data, HCD Protected Data, and software in transit

8.1.3.4.1 From disclosure

The HCD shall protect HCD Confidential Data from unauthorized disclosure when such data is in transit to or from the HCD over a shared communications medium.

For example, one possible technique may be found in 7.3.14.3:

- Providing the capability for encrypting network traffic to and from the HCD

8.1.3.4.2 From modification

The HCD shall protect HCD Confidential Data, HCD Protected Data, and software from unauthorized modification when such data is in transit to or from the HCD over a shared communications medium.

For example, one possible technique may be found in 7.3.12.3:

- Providing support for encryption algorithms that include data integrity checks such as CRCs or MICs for all traffic to and from the HCD

8.1.3.5 Administrator identification, authentication, and authorization

The HCD shall identify and authenticate each HCD administrator and shall ensure that administrators are authorized prior to permitting access to HCD data assets and performance of administration functions on the HCD.

For example, one possible technique may be found in 7.4.4.3:

- Providing support for strong authentication mechanisms for administrator access

8.1.3.6 Monitoring of HCD events

The HCD shall create and maintain a log of HCD use and security-relevant events.

For example, one possible technique may be found in 7.4.3.3:

- Providing the capability for the HCD to create and securely maintain a log of security-related and usage-related events

8.1.3.7 HCD cannot be used as a proxy for malicious attacks

The HCD shall ensure that its shared communication media interfaces cannot be used as a proxy for or a source of malicious attacks on the external IT environment.

For example, possible techniques may be found in 7.6.3.3:

- Providing the ability to disable individual protocols and ports on the device
- Providing address or destination filters to block or permit connections from known or unknown hosts (e.g., white list, black list of IP, MAC, phone)

8.1.3.8 HCD cannot be used as an unauthorized bridge from one interface to a shared communications media interface

If a shared communication interface (e.g., network connection) is present on the HCD, the HCD shall not permit users to establish a malicious connection to the external IT environment from any other interface. In addition, the HCD should not permit an unauthorized non-fax data connection to the HCD via the fax interface.

For example, possible techniques may be found in 7.6.2.3 and 7.6.3.3:

- Providing the capability to disable the fax function on the HCD

- Ensuring that the protocol stacks for external unprotected interfaces like fax are completely isolated from the other interface protocol stacks

8.1.3.9 Mitigation of denial of service attack

The HCD should protect assets during DoS attacks against the external HCD interfaces, and should restore normal operation without requiring human intervention upon termination of such attacks.

For example, techniques that may be used to address this requirement may be found in 7.1.11.3 and 7.1.9.3:

- Ensuring that even where an attack of this type causes failure of the network interface on the HCD, it does not interfere with the operation of those HCD subsystems that do not require network access.
- Ensuring that the HCD implements a best effort mechanism to recover automatically when the network interface is nonresponsive.
- Providing the capability to enable only protocols that require user authentication before jobs can be sent to the HCD.

8.1.4 Security objectives for the HCD in Environment D

8.1.4.1 Protecting HCD software from unauthorized modification

The HCD shall provide procedures to verify that the currently installed software in the HCD is consistent with the authorized, installed HCD software.

For example, one possible technique may be found in 7.5.2.3:

- Performing a check of the integrity and validity (e.g., checksum, CRC, digital signature) of the installed firmware each time the HCD boots

8.1.4.2 Protecting HCD Confidential Data, HCD Protected Data, and software in the HCD

8.1.4.2.1 From disclosure

The HCD shall protect HCD Confidential Data from unauthorized disclosure when such data is in the HCD.

For example, possible techniques may be found in 7.4.4.3:

- Providing support for strong authentication mechanisms for administrator access
- Ensuring that any authentication data stored on the HCD are encrypted

8.1.4.2.2 From modification

The HCD shall protect HCD Confidential Data and HCD Protected Data from unauthorized modification when such data is stored on the HCD. The HCD should provide protection for, or an indication of change in, HCD software that is in the HCD.

For example, one possible technique may be found in 7.3.9.3:

- Providing the ability for the HCD to create a secure MIC, CRC, or other data integrity check for the data that is stored on the HCD

8.1.4.3 Protecting HCD Confidential Data, HCD Protected Data, and software in transit

8.1.4.3.1 From disclosure

The HCD shall protect HCD Confidential Data from unauthorized disclosure when such data is in transit to or from the HCD over a shared communications medium.

For example, one possible technique may be found in 7.3.14.3:

- Providing the capability for encrypting network traffic to and from the HCD

8.1.4.3.2 From modification

The HCD shall protect HCD Confidential Data, HCD Protected Data, and software from unauthorized modification when such data is in transit to or from the HCD over a shared communications medium.

For example, one possible technique may be found in 7.3.12.3:

- Providing support for encryption algorithms that include data integrity checks such as CRCs or MICs for all traffic to and from the HCD

8.1.4.4 Administrator identification, authentication, and authorization

The HCD shall identify and authenticate each HCD administrator and shall ensure that administrators are authorized prior to permitting access to HCD data assets and performance of administration functions on the HCD.

For example, one possible technique may be found in 7.4.4.3:

- Providing support for strong authentication mechanisms for administrator access

8.1.4.5 HCD cannot be used as a proxy for malicious attacks

The HCD shall ensure that its shared communication media interfaces cannot be used as a proxy for or a source of malicious attacks on the external IT environment.

For example, techniques that may be used to address this requirement may be found in 7.6.3.3:

- Providing the ability to disable individual protocols and ports on the device
- Providing address or destination filters to block or permit connections from known or unknown hosts (e.g., white list, black list of IP, MAC, phone)

8.1.4.6 HCD cannot be used to bridge between fax interface and a shared communications media

If a shared communication interface (e.g., network connection) is present on the HCD, the HCD shall not permit users to establish a malicious connection to the external IT environment via the fax interface and should not permit an unauthorized non-fax data connection to the HCD via the fax interface.

For example, one possible technique may be found in 7.6.2.3:

- Providing the capability to disable the fax function on the HCD

8.1.4.7 Mitigation of denial of service attack

The HCD should protect assets during DoS attacks against the external HCD interfaces and should restore normal operation upon termination of such attacks.

For example, techniques that may be used to address this requirement may be found in 7.1.11.3 and 7.1.9.3:

- Ensuring that even where an attack of this type causes failure of the network interface on the HCD, it does not interfere with the operation of those HCD subsystems that do not require network access
- Ensuring that the HCD implements a best effort mechanism to recover automatically when the network interface is nonresponsive
- Providing the capability to enable only protocols that require user authentication before jobs can be sent to the HCD

8.2 Compliance security objectives for IT professionals

This subclause describes a set of minimum requirements for IT professionals that claim compliance to this standard. To claim compliance to this standard, an IT professional shall follow all requirements for a given operational environment.

Techniques provided in this subclause and Clause 7 are meant as examples; IT professionals may use any suitable technique(s) to meet the objectives.

8.2.1 Security objectives for IT professionals in Environment A

8.2.1.1 Training for administrators

Administrators shall be aware of and follow the security policies and procedures of their organization.

For example, one technique that may be used to address this requirement may be found in 7.4.3.4:

- Providing appropriate training for administrators regarding the security requirements of the HCD’s environment and provide the training and time for the administrator to follow the manufacturer’s guidance and documentation to correctly configure and operate the HCD in accordance with those requirements

8.2.1.2 Training for users

Users shall be aware of and follow the security policies and procedures of their organization.

For example, techniques that may be used to address this requirement may be found in 7.4.2.4:

- Providing appropriate training for users regarding the secure operation of the HCD in the particular operational environment

- Educating users to exercise care in selecting passwords and in entering user authentication data at the operator panel of the HCD

8.2.1.3 Limited physical access

The HCD shall be placed in an area that limits the opportunity for unauthorized physical access to the HCD.

For example, one possible technique may be found in 7.4.1.4:

- Increasing the physical security of the HCD through either placement in a controlled-access location or monitoring of a public-access location

8.2.1.4 Protecting data on shared communications medium

The operating environment shall provide support for protecting data from unauthorized disclosure and modification when data is exchanged with the HCD over a shared communications medium.

For example, one possible technique may be found in 7.3.14.4:

- Implementing an encryption infrastructure to enable HCD traffic to be encrypted

8.2.1.5 Protecting from unmanaged public access

The operating environment shall provide protection from unmanaged public access to the HCD over shared communications media.

For example, possible techniques may be found in 7.3.14.4 and 7.1.11.4:

- Connecting the HCD to the network through a switched, rather than a hub, connection
- Ensure that HCDs are placed behind firewalls or other network security devices

8.2.1.6 HCD management

Only those responsible for the management of the HCD (e.g., administrators) shall be authorized to perform that function.

For example, one possible technique may be found in 7.4.3.4:

- Ensuring that only authorized security administrators have access to a given security administrator user ID and password

8.2.1.7 User authorization

Only administratively sanctioned users shall be granted authorization to use the HCD

For example, one possible technique may be found in 7.3.10.4:

- Ensuring that only authorized users have access to only those HCD functions for which access has been granted by a security administrator

8.2.1.8 Administrators should not use their privileges for malicious purposes

The HCD owner shall establish trust that HCD administrators will not use their privileged access rights for malicious purposes.

For example, one technique that may be used to address this requirement may be found in 7.4.3.4:

— Ensure that appropriate human resource controls have been applied to security administrators, such as background screening, separation of duties, and rotation of duties

8.2.1.9 Audit trail protection

Remotely stored records and logs that provide an audit trail for an HCD shall be maintained and protected from unauthorized disclosure or alteration.

For example, one possible technique may be found in 7.4.4.4:

— Ensuring that any audit logs stored on a remote server are stored in an encrypted form or protected by an access control mechanism

8.2.1.10 Review audit trail for potential security violations

Operations staff shall ensure that audit logs are reviewed at appropriate intervals for security violations or unusual patterns of activity.

For example, one possible technique may be found in 7.2.2.4:

— Implementing a periodic administrator review process for all HCD audit logs and account for any unusual events

8.2.1.11 Mitigation of denial of service attack

Those responsible for the management of HCD’s IT environment (e.g., network administrators) shall employ reasonable mechanisms to protect the HCD from DoS attacks.

For example, possible techniques may be found in 7.1.12.4:

— Limiting network access to the HCDs to specific network notes, such as print and mail servers, through the use of VLANs or similar technologies

— Ensure that HCDs are placed behind firewalls or other network security devices

— Ensuring that all networked devices have the latest security updates applied, and effective antivirus software installed and operational

8.2.2 Security objectives for IT professionals in Environment B

8.2.2.1 Training for administrators

Administrators shall be aware of and follow the security policies and procedures of their organization.

For example, one technique that may be used to address this requirement may be found in 7.4.3.4:

- Providing appropriate training for administrators regarding the security requirements of the HCD's environment and provide the training and time for the administrator to follow the manufacturer's guidance and documentation to correctly configure and operate the HCD in accordance with those requirements

8.2.2.2 Training for users

Users shall be aware of and follow the security policies and procedures of their organization.

For example, techniques that may be used to address this requirement may be found in 7.4.2.4:

- Providing appropriate training for users regarding the secure operation of the HCD in the particular operational environment
- Educating users to exercise care in selecting passwords and in entering user authentication data at the operator panel of the HCD

8.2.2.3 Limited physical access

The HCD shall be placed in an area that limits the opportunity for unauthorized physical access to the HCD.

For example, one possible technique may be found in 7.4.1.4:

- Increasing the physical security of the HCD through either placement in a controlled-access location or monitoring of a public-access location

8.2.2.4 Protecting data on shared communications medium

The operating environment shall provide support for protecting HCD Confidential Data from unauthorized disclosure and modification and HCD Protected Data from modification when this type of data is exchanged with the HCD over a shared communications medium.

For example, one possible technique may be found in 7.3.14.4:

- Implementing an encryption infrastructure to enable HCD traffic to be encrypted

8.2.2.5 Protecting from unmanaged public access

The operating environment should provide protection from unmanaged public access to the HCD over shared communications media.

For example, one possible technique may be found in 7.3.14 and 7.1.11.4:

- Connecting the HCD to the network through a switched, rather than a hub, connection
- Ensure that HCDs are placed behind firewalls or other network security devices

8.2.2.6 HCD management

Only those responsible for the management of the HCD (e.g., administrators) shall be authorized to perform that function.

For example, one possible technique may be found in 7.4.3.4:

- Ensuring that only authorized security administrators have access to a given security administrator user ID and password

8.2.2.7 Administrators should not use their privileges for malicious purposes

The HCD owner should establish trust that HCD administrators will not use their privileged access rights for malicious purposes.

For example, one technique that may be used to address this requirement may be found in 7.4.3.4:

- Ensure that appropriate human resource controls have been applied to security administrators, such as background screening, separation of duties, and rotation of duties

8.2.2.8 Audit trail protection

Remotely stored records and logs that provide an audit trail for an HCD shall be maintained and protected from unauthorized disclosure or alteration.

For example, one possible technique may be found in 7.4.4.4:

- Ensuring that any audit logs stored on a remote server are stored in an encrypted form or protected by an access control mechanism

8.2.2.9 Review audit trail for potential security violations

Operations staff shall ensure that audit logs are reviewed at appropriate intervals for security violations or unusual patterns of activity.

For example, one possible technique may be found in 7.2.2.4:

- Implementing a periodic administrator review process for all HCD audit logs and account for any unusual events

8.2.2.10 User authorization

Only administratively sanctioned users shall be granted authorization to use the HCD.

For example, one possible technique may be found in 7.3.10.4:

- Ensuring that only authorized users have access to only those HCD functions for which access has been granted by a security administrator

8.2.2.11 Mitigation of denial of service attack

Those responsible for the management of HCD’s IT environment (e.g., network administrators) shall employ reasonable mechanisms to protect the HCD from DoS attacks.

For example, possible techniques may be found in 7.1.12.4:

- Limiting network access to the HCDs to specific network notes, such as print and mail servers, through the use of VLANs or similar technologies
- Ensure that HCDs are placed behind firewalls or other network security devices
- Ensuring that all networked devices have the latest security updates applied, and effective antivirus software installed and operational

8.2.3 Security objectives for IT professionals in Environment C

8.2.3.1 Training for administrators

Administrators shall be aware of and follow the security policies and procedures of their organization.

For example, one technique that may be used to address this requirement may be found in 7.4.3.4:

- Providing appropriate training for administrators regarding the security requirements of the HCD's environment and provide the training and time for the administrator to follow the manufacturer's guidance and documentation to correctly configure and operate the HCD in accordance with those requirements

8.2.3.2 Limited physical access

The HCD shall be placed in an area that limits the opportunity for unauthorized physical access to the HCD.

For example, one possible technique may be found in 7.4.1.4:

- Increasing the physical security of the HCD through either placement in a controlled-access location or monitoring of a public-access location

8.2.3.3 Protecting data on shared communications medium

The operating environment shall provide support for protecting HCD Confidential Data from unauthorized disclosure and modification and HCD Protected Data from modification when this type of data is exchanged with the HCD over a shared communications medium.

For example, one possible technique may be found in 7.3.14.4:

- Implementing an encryption infrastructure to enable HCD traffic to be encrypted

8.2.3.4 Protecting from unmanaged public access

The operating environment should provide protection from unmanaged public access to the HCD over shared communications media.

For example, one possible technique may be found in 7.3.14 and 7.1.11.4:

- Connecting the HCD to the network through a switched, rather than a hub, connection
- Ensure that HCDs are placed behind firewalls or other network security devices

8.2.3.5 HCD management

Only those responsible for the management of the HCD (e.g., administrators) shall be authorized to perform that function.

For example, one possible technique may be found in 7.4.3.4:

- Ensuring that only authorized security administrators have access to a given security administrator user ID and password

8.2.3.6 User authorization

Only administratively sanctioned users shall be granted authorization to use the HCD.

For example, one possible technique may be found in 7.3.10.4:

- Ensuring that only authorized users have access to only those HCD functions for which access has been granted by a security administrator

8.2.3.7 Administrators should not use their privileges for malicious purposes

The HCD owner should establish trust that HCD administrators will not use their privileged access rights for malicious purposes.

For example, one technique that may be used to address this requirement may be found in 7.4.3.4:

- Ensure that appropriate human resource controls have been applied to security administrators, such as background screening, separation of duties, and rotation of duties

8.2.3.8 Audit trail protection

Remotely stored records and logs that provide an audit trail for an HCD shall be maintained and protected from unauthorized disclosure or alteration.

For example, one possible technique may be found in 7.4.4.4:

- Ensuring that any audit logs stored on a remote server are stored in an encrypted form or protected by an access control mechanism

8.2.3.9 Review audit trail for potential security violations

Operations staff shall ensure that audit logs are reviewed at appropriate intervals for security violations or unusual patterns of activity.

For example, one possible technique may be found in 7.2.2.4:

- Implementing a periodic administrator review process for all HCD audit logs and account for any unusual events

8.2.3.10 Mitigation of denial of service attack

Those responsible for the management of HCD's IT environment (e.g., network administrators) shall employ reasonable mechanisms to protect the HCD from DoS attacks.

For example, possible techniques may be found in 7.1.12.4:

- Limiting network access to the HCDs to specific network notes, such as print and mail servers, through the use of VLANs or similar technologies
- Ensure that HCDs are placed behind firewalls or other network security devices

8.2.4 Security objectives for IT professionals in Environment D

8.2.4.1 Limited physical access

The HCD shall be placed in an area that limits the opportunity for unauthorized physical access to the HCD.

For example, one possible technique may be found in 7.4.1.4:

- Increasing the physical security of the HCD through either placement in a controlled-access location or monitoring of a public-access location

8.2.4.2 Protecting data on shared communications medium

The operating environment shall provide support for protecting HCD Confidential Data from unauthorized disclosure and modification and HCD Protected Data from modification when this type of data is exchanged with the HCD over a shared communications medium.

For example, one possible technique may be found in 7.3.14.4:

- Implementing an encryption infrastructure to enable HCD traffic to be encrypted

8.2.4.3 Administrators should not use their privileges for malicious purposes

The HCD owner should establish trust that HCD administrators will not use their privileged access rights for malicious purposes.

For example, one technique that may be used to address this requirement may be found in 7.4.3.4:

- Providing appropriate training for administrators regarding the security requirements of the HCD's environment and provide the training and time for the administrator to follow the manufacturer's guidance and documentation to correctly configure and operate the HCD in accordance with those requirements

Annex A

(informative)

Best practices

A.1 Overview

This clause provides a series of best practices for the following:

a) HCD developers and manufacturers

b) IT administrators of HCDs

c) Users of the HCDs

The security objectives and goals of hardcopy systems are basically the same as that of PC systems or any other kind of IT equipment that creates, stores, or processes information; namely, to restrict access to and use of assets to those who are authorized and to prevent malicious use or disruption of those assets. As discussed in Clause 5, the assets or asset classes relevant to an HCD include: the use or function of the device, the User Document Data being processed, the security relevant management information of the device, and the integrity of the network infrastructure in a networked environment.

In general, many of the same organizational, physical, and technical measures used to provide security in a PC environment can be applied to a hardcopy environment as well; however, hardcopy systems are different from PC systems in the following ways:

1) Hardcopy systems not only process and store User Document Data assets in electronic form like PC systems, but also process or generate assets in physical form when the pages are scanned or printed.

2) Hardcopy systems have additional physical assets, such as toner or ink cartridges and blank media that are required for the device to perform its intended function.

3) An HCD is, by its intended function, more physically accessible to a larger number of users than a PC or server in the same environment.

A.2 Best practices for HCD architecture, design, deployment, and usage

A.2.1 Internal operating system and its features

A.2.1.1 Overview

The vendor’s choice of base OS, network protocol stack, and the design of core OS functions can also have an impact on the security or ease of securing an HCD. Many HCDs implement all or part of standard OS kernels (e.g., *Linux*®, UNIX®[9]) that are also parts of PCs or workstations. This strategy aids vendors with

[9] *Linux*® is a registered trademark of Linus Torvalds in the U.S. and other countries; UNIX is a registered trademark of the The Open Group. This information is given for the convenience of users of this standard and does not constitute an endorsement by the IEEE of these products. Equivalent products may be useful if they can be shown to lead to the same results.

product time to market and with feature addition but can also result in the system being subject to the same security issues (e.g., buffer overruns) that effect the PC or workstation versions of the OSs.

Another OS feature that is common among HCDs is the capability of executing applets (i.e., Java-type downloadable code) that can be remotely downloaded an executed. This feature can create a security exposure if the applet download and execute functions are not properly authenticated.

A.2.1.2 Recommended practices for HCD manufacturers

The implementation of the following OS-level features can aid in increasing the security of an HCD:

a) Isolation of core OS functions from network code and applets and defining very rigorous software interfaces to prevent inadvertent paths into the heap or stack space

b) Ability to restrict or prevent access to firmware update modules, core memory spaces, and other services by downloaded applets

c) Authentication and integrity checking of downloaded applets before execution of the code

d) Support for remapping of the standard port numbers in the network protocol stack to nonstandard or random port numbers (e.g., nonstandard TCP port)

e) Support for the use of proxies by the network protocol stack

f) Support for the use of external or internal software-based firewalls by the OS and protocol stack

A.2.1.3 Recommended practices for IT professionals

The following IT practice can aid in increasing the security of an HCD:

a) Maintain the device firmware at a current level with all vendor-released security patches applied

A.2.2 Methodologies and processes for the development of secure HCDs

A.2.2.1 Overview

As stated in Clause 1 one of the goals of this standard is to “instruct manufacturers and software developers on appropriate security capabilities to include in their devices and systems and instructs users on appropriate ways to use these security capabilities.” To achieve this goal, guidance is provided to users and manufacturers on the best ways to improve the HCD’s functionality under the types of malicious attacks discussed in Clause 6.

One important component to providing this type of guidance is the understanding that the methodologies described in Clause 7 can only protect the software that comprises HCDs and the systems that the HCDs run on in a post facto way, i.e., after the development is complete. To provide the full measure of assurance against malicious threats, HCD manufacturers should embrace the concept of software security—engineering the software for HCDs in a way that builds security into the software from the beginning as well as educates software architects, developers, and users in the best ways to build secure software.

This subclause provides a brief discussion of the basic methodologies and processes for building security into software for HCDs with references to where readers of this standard can find more information on the subject of software security.

A.2.2.2 Software security principles

The concept of software security is really about defining a secure software development process, i.e., defining the specific methodologies and processes that a software developer should implement within their defined software development process, regardless on what type of software life cycle model (e.g., spiral, incremental development, waterfall) that a developer uses to describe its software development process, that will have a positive impact on reducing potential vulnerabilities that can be introduced into the software prior to its release to users.

The basis for a secure software development process is a set of guiding security principals that form the foundation for any secure software methodology. There are a number of different formulations of these security principals, but all encompass the same basic ideas. As an example of these security principles, *Building Secure Software* [B149] describes the following 10 software security principles:

1) *Secure the weakest link*—The security of an entire system is only as good as its weakest link because attackers will always attack the weakest parts (the parts most likely to be broken) of the system first.

2) *Practice defense in depth*—Incorporate multiple, diverse defensive strategies so that if one layer of defense is inadequate or broken, another layer of defense might prevent the attack.

3) *Fail securely*—Always design a system so that when the system fails in any way, the system will fail in a way that maintains the security of the system.

4) *Follow the path of least privilege*—When providing access of a user or process to a system, make sure only the minimum access is granted and only for the minimum amount of time necessary.

5) *Compartmentalize*—Break up the design and implementation of the system into components that isolate the security privileges so that the amount of damage that is done to a system via some type of attack is minimized.

6) *Keep it simple stupid (KISS)*—Avoid complexity in design and implementation of the system so that they are as straightforward as possible; complexity adds risks and increase the likelihood of vulnerabilities being introduced.

7) *Promote privacy*—Do not do anything in the design or implementation of a system that would compromise the privacy of a user.

8) *Hiding secrets is hard (avoid security by obscurity)*—Keeping secrets in a system design or implementation is extremely difficult and almost always poses a huge security risk.

9) *Be reluctant to trust*—Systems should be very reluctant to extend trust to processes or users in their design and implementation.

10) *Use your community resources*—Always use widely available and scrutinized security mechanisms (e.g., cryptographic libraries) in the system design and implementation instead of internally developed ones.

Other good statements of these security principles can be found in NIST Special Publication 800-30 [B82] and *Improving Security Across the Software Development Lifecycle, Task Force Report* [B45].

A.2.2.3 Security risk management

When one looks at the set of security principles described in A.2.2.2 one should note that software security, or more specifically the specification of methodologies and processes for implementing a secure software development life cycle, is really about defining and managing the security risks in a system.

NIST Special Publication 800-30 [B82] describes risk management as “the process that allows IT managers to balance the operational and economic costs of protective measures and achieve gains in mission capability by protecting the IT systems and data that support their organizations’ missions.” Although the concept of risk management is not solely confined to security, it is clear that the idea of security risk management is critical to helping to prevent or at least minimize potential vulnerabilities from occurring in the first place. If one can determine what the potential security risks are as early as the requirements phase of a software development cycle and design and implement the system to minimize or hopefully eliminate those security risks, it is likely that the resultant system will be more secure from a user’s perspective.

Building Secure Software [B149] defines the following steps in a software security risk management process:

1) Derive the set of software security requirements. Learn as much as possible about the system to be developed

2) Identify via risk analysis and then quantify the potential software security risks from these derived security requirements. Quantification is typically in terms of the likelihood (probability) of the security problem or vulnerability defined by the risk actually being exploited, the frequency with which that problem or vulnerability might be exploited, and the impact (in terms of financial loss, damage to reputation, violation of federal or state laws, etc.) should the problem or vulnerability actually be exploited

3) Identify the largest or most critical risks and define or evaluate strategies for mitigating these risks

4) Implement these defined mitigation strategies

5) Repeat steps 2–5

Threat Modeling [B146] defines another very good approach to software security risk analysis called DREAD. In DREAD, potential software security risks are quantified in terms of five different aspects:

Damage potential—How much damage can be done to the system or data)

Reproducibility—Will the attack work every time or does it depend on special conditions or circumstances

Exploitability—How much effort or expertise is required for an arbitrary attacker to mount the attack

Affected users—Who and how many would be affected if the attack occurred, and

Discoverability—How difficult is it for an arbitrary attacker to identify the vulnerability

The goal in a secure software development life cycle should be to start this software security risk management process as early as possible in the software life cycle, and then continually refine and update the software security risk assessment throughout the software development life cycle all the way through system test and up to system release to the user.

Building Secure Software [B149] and *Threat Modeling* [B146] provide more details on software security risk management and techniques for performing software security risk analysis.

A.2.2.4 Secure software development best practices

The Software Process Subgroup of the *Improving Security Across the Software Development Cycle, Task Force Report* [B45] listed the following "process-related requirements" for the processes and practices that will effectively produce secure software:

a) They should cover the full software life cycle from the earliest requirements through design, development, delivery, maintenance, and end-of-life

b) They should be precisely defined so they can be taught, supported, verified, maintained, etc.

c) They should establish and guard the integrity of the product throughout the life cycle

d) They should include measures to verify that the product developers are capable of consistently and correctly using the process and that the process consistently produces secure software products

e) They should be able to be tailored

f) They should be usable by properly trained and qualified persons

g) They should be owned, supported, widely available, and regularly updated

h) They should be fully supported with training programs

i) They should include the use of state-of-the-practice methods

A.2.2.5 Secure software methodologies

A secure software development life cycle based on the recommendations in *Improving Security Across The Software Development Cycle, Task Force Report* [B45] should have at its core the goal of including software methodologies and associated software tools that would facilitate the architecting, design, and development of more secure software. These secure software methodologies should start in the beginning of any software development life cycle and continue on throughout all life cycle phases until the developed system is finally released to its intended users.

There are many different formulations of a secure software development life cycles, but all have similar components by software life cycle phase regardless of the underlying life cycle model used as follows.

A.2.2.6 Software requirements

Software security considerations should begin in the requirements definition phase. Security requirements should be defined that specify not only the functional security requirements [e.g., use of secure protocols like secure socket layer (SSL)] but also the behavior characteristics of the system that enforce the security principles discussed in A.2.2.2. It should be noted that the description of these behavior security requirements should cover both the intended and unintended system behavior (i.e., what the system should do should it fail due to errors of omission and not just errors of commission).

Threat Modeling [B146] provides more details on security requirements, threat modeling, and abuse/misuse cases.

A.2.2.6.1 System analysis and system/software design

During system analysis and system/software design the focus of the secure software development life cycle should be on analysis of the security requirements to determine potential vulnerabilities and threats, and then create a system and software architecture and design that will minimize the identified vulnerabilities and threats.

The cornerstone of this activity is the security risk management activities described in A.2.2.3. To support the security risk assessment, there are many techniques that have been proposed to aid in defining and analyzing the potential vulnerabilities and threats. Among them are creation of *abuse/misuse* cases and some type of threat modeling.

Abuse or misuse cases are cases that describe system behavior in case of either intentional (abuse) or unintentional (misuse) attacks in terms of:

a) How the system should respond to the attack

b) What portions of the system should be protected and for how long, and

c) How the system should recover from the attack

Threat modeling attempts to define potential security threats using mathematical or formalized techniques to identify the potential threats. Among the many threat modeling techniques used are the following:

1) *Attack trees*—Graphs built to represent the decision-making process of a well-informed attacker, where the *roots* of the tree represent potential goal(s) of an attacker, the *leaves* represent ways of achieving a goal, the *nodes* under the root node represent high-level ways in which a goal might be achieved, *lower level nodes* represent increasingly more specific ways in which a goal might be achieved, and *pruning nodes* represent conditions that are required to be true for a child node to be relevant.

2) *Attack patterns*—Generalized attack patterns that should guide design, implementation, and testing. Samples include target programs that write to privileged resources, direct access to executable files, HTTP cookies, HTTP query strings, and buffer overflows.

3) *STRIDE*—A methodology for threat modeling described in *Threat Modeling* [B146] that categorizes potential threats in terms of the following:

Spoofing identity—Allows an attacker to pose as another user or allows a rogue server to pose as a valid server

Tampering with data—Malicious modification of data

Repudiation—Deny performing an action without other parties having a way to prove otherwise

Information disclosure—Exposure of information to individuals who are not supposed to have access to it

Denial of service—Deny service to valid users

Elevation of privilege—Unprivileged user gains privileged access to compromise or destroy a system

During system analysis and system/software design preliminary vulnerability analysis should be performed. The purpose of vulnerability analysis is to identify potential vulnerabilities in the product, principally by applying the network analyzers and by probing the product’s external data interfaces based on the available design information for potential vulnerabilities. The goal of vulnerability analysis is to analyze the system to determine if the product is potentially vulnerable to known vulnerabilities found in similar products. This vulnerability analysis should be updated during all of the remaining software development life cycle phases.

Building Secure Software [B149] and *Threat Modeling* [B146] provide more details on threat modeling, abuse/misuse cases, and vulnerability analysis.

A.2.2.6.2 Implementation

As developers implement the system and software design, two important secure software development methodologies should be employed, as follows.

A.2.2.6.3 Security code reviews/inspections

A well-accepted software life cycle process during implementation is the use of software code reviews or inspections (*Building Secure Software* [B149]). These software code reviews should include security code review, a review of code for key security related guidelines and secure coding best practices. For example, "A Static Analyzer for Finding Dynamic Programming Errors" [B12] includes the following general set of secure programming guidelines that were promoted by the Open Web Application Security Project [10] and should be checked for in any review or inspection of code:

a) Validate inputs and outputs

b) Ensure that the code fails securely

c) Use and reuse trusted components

d) Perform "Defense in Depth"

e) Avoid "Security by Obscurity"

f) Ensure "Least Privilege" is followed to provide only the privileges required

g) Emphasize compartmentalization (or separation of privileges)

h) Do not use homegrown encryption algorithms

i) Encrypt all communications whenever possible

j) Forbid transmission of passwords in plain text

k) Make the default configuration the secure configuration

l) Do not include any back doors into the software

It should be noted that not all code necessarily should be subject to a security code review or inspection depending on the system; the focus of security code reviews or inspections could be the software that implements security features, key external data interfaces, Web interfaces, etc.

Additional information on security code reviews and secure coding practices can be found in *Building Secure Software* [B149] and Threat Modeling [B146].

[10] See http://www.owasp.org/.

Static security code analysis

Security code reviews should be supplemented by use of automated static code analysis tools that analyze source code for not only standards violations and other programming guidelines, but for common vulnerabilities like buffer overflows. The creation of security-related static analysis tools has been driven in large part by the recognition that security code reviews or inspections, although a very necessary step in ensuring secure software is created, are not sufficient, if for no other reason than the fact that code reviews are a human process and humans are fallible.

There are numerous automated static analysis tools for security that have surfaced and are being used today. No specific tool is being recommended here; *Improving Security Across The Software Development Cycle, Task Force Report* [B45] provides references to some of the more common security static code analysis tools available today.

A.2.2.6.4 Testing

Testing encompasses a wide variety of activities, from unit testing of software code modules through integration testing where software components are assembled and tested, to testing of the fully integrated software, and finally to testing of the fully integrated system. From a security software development cycle perspective, the focus typically is on methodologies that help in the testing of the integrated software and system. Among the techniques that support security testing are the following.

Security test plans and procedures

The important first step in any testing phase should be the creation of security test plans and associated test procedures that address both security functionality testing and security vulnerability testing based on the attack scenarios defined in A.2.2.6.1. Security test plans and associated security test procedures should cover all the security testing and should be created as part of any standard test plan and procedure creation process.

Security test plans should be created as early as possible (e.g., during software preliminary design activities) while the various security test procedures should be created during code development and prior to the start of testing. Security test plans and procedures should be reviewed for completeness and adequacy and then approved before any security related testing begins.

Security functionality testing

Security testing should include testing of the functional and behavioral security requirements described in A.2.2.6. The focus of this testing should be the system’s security functionality.

An important benefit of security functional testing is that security can now be specified and measured so that the required level of security can be achieved, i.e., software developers can start treating software security as a software property just like reliability or interoperability. For this to occur, the development of consistent measures of software security and the analysis of how a system’s software security matures as the system is developed and tested are needed. Eventually, quantitative software security targets for a system can be specified and security functionality testing can then help determine if these targets are met.

Security functionality testing should be performed alongside the other functionality testing done for the system.

Vulnerability testing

Vulnerability testing (whether it is denoted as risk-based testing or penetration testing) involves the creation of test plans and procedures driven by the security risk analysis in A.2.2.3 and the threat modeling and abuse or misuse case development described in A.2.2.6.1. Vulnerability testing generally is black-box testing designed to exploit known or anticipated vulnerabilities of the system to see if the associated vulnerabilities are exploitable and, if so, in what ways. Vulnerability testing is also important to ascertain whether or not the system will default to the proper secure modes (i.e., will fail "gracefully" in expected ways) when an attack is executed. Vulnerability testing also pro-actively determines if previously found vulnerabilities remain. Often the focus of vulnerability testing is those risks derived from security risk analysis with the highest risk ratings or with the highest *threat* values indicating likelihood of occurrence.

Building Secure Software [B149] and *Improving Security Across The Software Development Cycle, Task Force Repo*rt [B45] provide more information on security testing and vulnerability testing.

A.2.2.7 Other considerations

A Static Analyzer for Finding Dynamic Programming Errors [B12] discusses other considerations that should be included in any secure software development life cycle as follows.

A.2.2.7.1 Authentication, authorization, session management, and encryption

As "A Static Analyzer for Finding Dynamic Programming Errors" [B12] indicates, *authentication, authorization, session management,* and *encryption* are common problems that designers of secure software face.

a) Authentication should be handled using standard protocols and components where available and will require special expertise to implement.

b) Authorization should be done using standard available applications where possible. Developers implementing authorization should be deeply concerned with privilege management and accumulation over time of excess privileges.

c) Application designers should implement a state mechanism that allows multiple requests from a single user to be associated in a session, since poor use of session variables to manage state can lead to serious vulnerabilities.

d) Cryptography should be left to experts. Application designers should consider what information needs to be encrypted and when, and applications involving cryptography should implement sound key management processes.

A.2.2.7.2 Accountability

Some guidelines proposed here are as follows:

a) Code signing can be an important technique to help maintain careful, rigorous control of and accountability for code

b) Every change to software should be identified, analyzed, reviewed, and tested

c) Access to critical components or subsystems should be controlled

d) Code access authorizations and code signing will help promote accountability but do not totally address issues of malicious code

A.2.2.7.3 Modifications and patch management

With the ever increasing number of security vulnerabilities being uncovered daily, the necessity for continuous modifications and patch management becomes critical for HCD manufacturers to ensure that both their product software and the software that comprises their IT infrastructures is as secure as possible. As the sub-report of the *Improving Security Across the Software Development Lifecycle, Task Force Repo*rt [B46] indicates, any process for software modification and patch management is required to be "considerate of requirements for safe and secure introduction into the environments of critical infrastructure providers. A complex process of impact and risk evaluation, patch preparation and testing, and deployment in a large, complex organization is not a simple endeavor…."

With that in mind, *Improving Security Across the Software Development Lifecycle, Task Force Repo*rt [B46] provides some fundamental guidelines that providers should be aware of in implementing any modification or patch management process are as follows:

a) Patches should be well tested before they are implemented

b) Patches should introduce minimal (only what is necessary) code changes

c) Patches should be as small as possible

d) Patches should be localized and made available for all applicable languages and environments simultaneously

e) Patches should be reversible so the system can return to its prior state

f) Patches should not disrupt system availability and strictly limit system downtime

g) Patches should use consistent methods to register themselves on the system

h) Patches should provide a consistent user experience, and the patch process should be automated and user-controlled to the maximum extent possible

i) Patches should support diverse deployment methods to accommodate all the applicable categories of users

j) Patches should make it easy to bring a system up-to-date (from a patch perspective) via methods like cumulative patching

A.2.2.7.4 Use of third-party software

Since the use of third-party software is becoming prevalent, the following should be considered when planning to use third-party software:

a) Carefully consider the proper use of the third-party software contemplated

b) Have some means of identifying and categorizing the trust level of any components that will use the third-party software and demand that third-party software be developed using a secure development process and be validated using security-related validated methods

c) Make the third-party software vendor include a disclosure of security assumptions and limitations and assess the quality and content of third-party software vendor documentation of security limits and security assumptions

A.2.2.7.5 Management practices

Since management has an important role in any software development life cycle, the following specific management practices are recommended to support a secure software development life cycle:

a) Establish organizational policies for secure software development

b) Set specific, measurable improvement goals for developing secure software

c) Establish leadership roles for security at the organization and at the project level

d) Provide resources and funding for needed training in software engineering practices and security practices

e) Provide an oversight function through quality and security reviews of projects and encourage reviews by external security experts

A.3 Best practices for physical security

A.3.1 General physical security

A.3.1.1 Overview

In general, the most appropriate countermeasures to physical access-based threats are dependent on the type organizational controls present in the particular environment and the degree that the area is physically secured. In environments with effective access control of the physical area, the need for device-specific physical security measures is reduced; however, an HCD in a tightly controlled area is likely to contain assets with a higher probability for attack and be subject to attackers of higher expertise, resources, and motivation.

A.3.1.2 Recommended practices for HCD manufacturers

Due to the fact that placement of the HCD is out of the control of the manufacturer, there are no specific recommendations with regard to physical security.

A.3.1.3 Recommended practices for IT professionals

There are two basic strategies for IT departments to provide device-specific physical security for HCDs. These are a means to

a) Prevent or deter access to the areas of the equipment that allow access to the assets being protected

b) Provide an indicator that access to area of the equipment has occurred for detection or auditing

It should be noted, however, that device-specific physical security measures alone cannot provide fail-safe security protection from a motivated attacker in an uncontrolled physical environment. In addition, some of the physical access threats can be further or completely mitigated using technical measures discussed in Clause 7 as opposed to using physical measures alone.

A.3.2 Protecting physical access to hardcopy output or input

A.3.2.1 Overview

HCDs will have bins, drawers, or trays to hold the input media for scanning as well as the output media that has been printed. Securing these components can prevent unauthorized users from retrieving documents of others.

A.3.2.2 Recommended practices for HCD manufacturers

There are several different strategies that can be employed by HCD manufacturers to increase the security of hardcopy input and output, as follows:

a) Provide multiple locked physical output bins that require the originator or designee to insert a key (or equivalent) to open the bin and access print or copy job or scan originals

b) Provide secure printing technology, whether server-based or device-based, to hold documents in secure storage until the originator or designee has authenticated at the device that consists of network credentials, PIN codes, an identity card, a key issued when the job is submitted, or a combination of these authentication techniques

c) Provide visually shielded scan input and output trays and printer output bins to prevent passers-by or a strategically positioned camera from reading scan originals or printed output

d) Provide visual or audible warnings to the end user for input hardcopy documents left either in the document feeder or on the glass

A.3.2.3 Recommended practices for IT professionals

The key objective for the IT department is to prevent unauthorized access to hardcopy output. One or more of the following strategies can be utilized to minimize the risk to the output hardcopy documents:

a) Select HCDs that support secure printing or physical locked mailboxes, or deploy a third-party solution to secure the printing at the server

b) If utilizing a secure printing solution, select an authentication method that provides a sufficient level of security at the HCD

c) If utilizing a secure printing solution, ensure that users cannot bypass the secure printing functionality by selecting an unsecured driver option, printing to an unsecured server print queue, or by printing directly to the device to bypass the server security

Protection of hardcopy input documents is considerably more difficult, as no technology is available to prevent such documents being accidentally left on the glass or in the document feeder. The following strategies can, however, be employed to mitigate the risks:

1) Educate the end-user community regarding the risks of leaving input documents at the HCD. (This education should be part of the standard security training in higher security operational environments.)

2) Provide visual shielding for the original document handler to prevent a remote-controlled or automated camera from photographing the input documents as they are fed through the document feeder.

A.3.3 Protecting physical access to supplies and consumables

A.3.3.1 Overview

HCDs require supplies such as paper and consumables such as ink or toner cartridges to operate. In some cases, these items have significant value and should be protected from theft.

A.3.3.2 Recommended practices for HCD manufacturers

The following strategies can be employed by HCD manufacturers to increase the security of supplies and consumables:

a) Provide locked media supply trays that automatically unlock only when empty or when accessed by an authorized device administrator

b) Provide locked device access panels that automatically unlock only in the case of a device malfunction or when accessed by an authorized device administrator

c) Minimize the use of standard PC add-on components in the design of an HCD, such as memory cards and hard disks. (The use of such components can lead to the risk of these add-on components becoming assets to be protected as well. For example, the use in an HCD of a memory expansion module that also works in a PC can become a source for an attacker to acquire memory modules for their own PC.)

A.3.3.3 Recommended practices for IT professionals

The following guideline for IT professionals with respect to the security of HCD supplies and consumables should be considered:

a) Use the manufacturer provided capabilities to secure supplies and consumables

A.3.4 Protecting physical access to subunits and components

A.3.4.1 Overview

Little can be done to protect against someone physically attacking the unit—with a sledgehammer or otherwise—aside from controlling physical access to the unit. However, there are protections that can be applied against incidental damage or attempted covert access.

A.3.4.2 Recommended practices for HCD manufacturers

The following strategies can be employed by HCD manufacturers to mitigate the risk to internal components and to increase the physical security of the device itself:

a) Provide locked device access panels that automatically unlock only in the case of a device malfunction, or when accessed by an authorized device administrator

b) Ensure that the HCD enclosure's construction is of sound material and is internally secured

c) Utilize locking connectors for power and signal cables, with securing provisions to prevent inadvertent disconnect and to sense intentional disconnect

d) Utilize nonstandard fasteners that require nonstandard or specialized tools for any externally accessible fasteners, and any internal fasteners for components to be access only by authorized technicians

e) Utilize selective quick-disconnect components to enable easy authorized removal of hard disk or other nonvolatile memory that may either have a high inherent value to an attacker or that may contain critical information, for overnight storage in secure facility

f) Provide alarms for attempted unauthorized access, damage, or disablement, using either audible or remote (e.g., radio, pager, or cell phone) intrusion alarms if panels are forced, or power or signal connectors are disconnected

A.3.4.3 Recommended practices for IT professionals

The following guideline for IT professionals with respect to the security HCD subunits and components should be considered:

a) Use the manufacturer provided capabilities to secure subunits and components

A.3.5 Theft of imaging components for analysis

A.3.5.1 Overview

If the User Document Data asset is of sufficient value, it can be assumed that physical access security provisions can be overcome. In this case, protection of the User Document Data asset is provided by minimizing accessibility of the information that may be obtained from the stolen imaging components, such as a photoconductor drum or belt.

A.3.5.2 Recommended practices for HCD manufacturers

The following strategy can be employed by HCD manufacturers to mitigate the risk of data recovery from imaging components:

a) Provide a mechanism to erase or clear residual information on intermediate imaging components such as photoconductors, drums, or belts

A.3.5.3 Recommended practices for IT professionals

The following strategy can be employed by IT professionals to mitigate the risk of theft of imaging components:

a) Run some number of all black copies (either copies of black pages, or all-black printed pages) after a highly confidential or valuable document has been printed or copied. (In the case of an HCD that supports color, pages that clear the imaging components for each color should also be printed or copied.)

A.3.6 Electromagnetic interception

A.3.6.1 Overview

Like other IT equipment, HCDs emit EM radiation. It may be possible to interpret the EM signatures of these devices and determine what the equipment is doing.

A.3.6.2 Recommended practices for HCD manufacturers

The following strategy can be employed by HCD manufacturers to mitigate the risk of EM interception:

a) Apply shielding to the HCD housing components to reduce signature emissions. (EMI emission regulations require limiting conducted and radiated emissions to reduce interference. However, there may be specific areas of the device that emit signals that can be correlated with the data, and although the energy in these emissions may be very low, it may still be sufficient to allow sophisticated equipment to recover information. Manufacturers should determine if such signals exist and if so, take special care to either additionally shield or mask such emissions.)

A.3.6.3 Recommended practices for IT professionals

The following strategy can be employed by IT professionals to mitigate the risk of EM interception:

a) HCDs used for very sensitive documents may be protected by locating them in a specially shielded room

A.4 Best practices for network data confidentiality, integrity, and non-repudiation

A.4.1 Overview

Protecting the assets of an HCD from unauthorized access or disruption, especially in a networked environment, not only requires the authentication of users and devices that directly access the assets, but also protecting assets (e.g., User Document Data, firmware update files and applet code) from unauthorized access or corruption while in transit. In some user environments, there may also be a need for the receiver of the User Document Data assets (this may be the HCD or another user) to verify or prove that the sender in fact is the source of the assets.

Some operational environments (e.g., Operational Environment D) may be able to simply use physical security measures to assure that User Document Data assets are protected while in transit to or from an HCD; however most environments will require some sort of technical measure to augment any sort of physical measure or environmental assumption about the security of the communication paths.

The common technical measures that can be used in network communication protocols to provide confidentiality, integrity, and non-repudiation of the transmitted data are following, although some of the protocols do not address all three requirements alone or require the use of optional features of the protocol to address all three requirements.

A.4.2 Recommended practices for HCD manufacturers

Mechanisms that can be used in an HCD environment to provide data confidentiality, integrity, or non-repudiation are as follows:

a) Use of protocols that support encryption at the Network Layer {e.g., VPNs using IPSec (RFCs 2401 [B116] to 2412 [B127] and 2451 [B128])}. IPSec provides data confidentiality and integrity and can provide mutual authentication (non-repudiation) if digital certificates are used

b) Use of protocols that support the transport layer using SSL or transport layer security (TLS) (RFC 2246 [B113]) record protocol, or protocols that support secure shell (SSH). (It should be noted that during the SSL/TLS handshake protocol, optional mutual authentication can be performed if the server requests a client certificate during the handshake.)

c) Use of applications that provide encryption, and integrity checking of the print data for use over unsecured, unknown, or legacy channel or network protocol (non-repudiation can also be addressed by the use of digital signatures).

d) Use of a Kerberos system to provide integrity and non-repudiation.

e) Use of the PSTN fax system, for transmission of the data over the telephone wires. (It should be noted that commercial PSTN fax transmissions only allow for non-repudiation of the sending device and do not provide either confidentiality or integrity checking. Other fax transmission systems defined by MIL-STD188-161D [B76] or NATO STANAG 5000 [B77] can be used to provide secure fax communications; however these systems do not provide non-repudiation.)

f) Use of Secure/Multipurpose Internet Mail Extensions (S/MIME) ((RFC 2311 [B115]) for HCDs using e-mail communication protocols.

NOTE—Security protocols such as TLS and IPSec can support many different encryption algorithms and can use encryption keys of various lengths. Some operational environments may impose restrictions on the type of encryption algorithm and key length that may be sufficient for that environment. Some of these encryption algorithms may also have export restrictions on the algorithm or the key length used with the algorithm that could limit their use or sale in commercial products to some geographic locations. Other operational environments may require the certification of the encryption algorithms or modules used in the HCD (e.g., the FIPS 140-2 certification in the U.S. and Canada).

A more complete discussion of the particular protocols and their features can be found in the following sources:

- *Network Security, Private Communication in a Public World* [B73]
- *TCP/IP Tutorial and Technical Overview* [B138]
- NIST SP 800-52 [B94]

A.4.3 Recommended practices for IT professionals

The following strategy can be employed by IT professionals to mitigate the risk of loss of integrity or confidentiality:

a) Use the manufacturer provided capabilities to secure network communications

A.5 Best practices for configuration management

A.5.1 Introduction

Historically, HCDs have been designed not only to perform their intended function, but also to make the device and the function as easy to configure, use, maintain, and service as possible. From a security perspective, however, easy to use can also mean easy to abuse. When faced with securing an HCD, there are some traditional design architectures and principles that HCD manufacturers may need to reconsider to provide for more secure or easier secure devices.

A.5.2 Out-of-box configuration

A.5.2.1 Overview

To ease installation, HCDs may leave the factory with an initial configuration aimed at providing the most general and flexible set of functions at its first power-on in the user's environment; however, this configuration can minimize or compromise the security of the device. This insecure configuration includes all supported network protocols for User Document Data transfer and device management activated, all physical ports enabled, and all passwords or PIN numbers set to a global default value.

Unlike PCs, which power on with few if any network protocols installed, HCDs are shipped with multiple active network protocols aimed at supporting a variety of disparate computer and network OS types. This is due to the fact that most networks in operational environments other than Operational Environment D are multi-protocol environments and even though some of the computers or computer clusters on the network do not normally communicate with each other, they are all expected to communicate with and transfer data to and from the networked HCD. The problem with this type of configuration lies in the fact that many of the protocols used for data transfer and device management in these multi-protocol environments were not originally designed with security as a goal. This can result in completely unsecured paths into the HCD.

A.5.2.2 Recommended practices for HCD manufacturers

The following HCD features can potentially enable more secure device installations:

a) The ability to disable *any* physical data connection or port on the HCD. This includes both external ports and internal option and memory connections.

b) The ability to disable individual network protocols over any of the network or local interfaces.

c) The ability to disable or restrict the use of any individual service or function of the device (e.g., the fax capability of a MFD can be completely disabled).

d) Setting the default out-of-box configuration of the hardcopy to a secure configuration instead of an insecure configuration.

e) Requiring that any local password or PIN numbers be configured at first power-on.

A.5.2.3 Recommended practices for IT professionals

The following guideline for IT professionals with relation to the out-of-box configuration for HCDs should be considered:

a) Do not leave the HCD in its out-of-box configuration

b) Change all manufacturer supplied or default passwords

A.5.3 Configuration, upgrade, and update security

A.5.3.1 Overview

Another general design principle or architecture choice for HCDs that can affect the security of the device is the way it is configured, upgraded, and updated.

Many HCDs can be completely configured via the device's local operator panel as well as via remote software utilities over every supported network protocol and physical data interface. This configuration philosophy that was originally intended to provide greater ease of use can create a number of unsecured or under-secured paths that allow unauthorized or malicious configuration changes to the HCD.

Many HCDs are shipped with hidden or undocumented configuration and monitoring ports that can provide very detailed status information about the internal state of the device and its OS. These back doors also can provide for additional control and configuration of the device that wouldn't or shouldn't normally be available to a user or administrator. While intended to help a manufacturer debug and solve user problems in the field, an attacker can exploit these back door entry points as well. Most HCDs also provide very easy firmware upgrades to allow for field problems to be fixed and new features to be added or expanded. The ease of change in the firmware and the integrity of the firmware loaded on the device can also create security exposures for HCDs.

A.5.3.2 Recommended practices for HCD manufacturers

Basic features for HCD configuration and update that may increase the level of security in the device include the following:

a) Limiting the mechanisms and protocols over which the device configuration can be changed or accessed, and providing the capability to disable configuration over specific ports and protocols. Providing a common, possibly single, configuration means to create a "secure configuration" or a configuration checklist for users and installers.

b) Avoiding shipping devices with active hidden back door debug ports or protocols and providing a secure mechanism for these ports to be disabled.

c) Avoiding the installation of firmware and applet updates and downloads that are not properly authenticated and integrity checked and restricting the number of ways (protocols) that firmware can be updated in an HCD.

A.5.3.3 Recommended practices for IT professionals

The following guideline for IT professionals with relation to the HCD configuration, upgrade, and updates should be considered:

a) Use the manufacturer provided capabilities to secure an HCD's configuration, upgrade, and update

A.5.4 Vulnerability management and security updates

A.5.4.1 Overview

Vulnerabilities are weaknesses in the HCD firmware or software that can be exploited to violate the HCD's security policy. Vulnerabilities should be given careful and deliberate handling. See NIST Special Publication 800-40 [B88].

A.5.4.2 Recommended practices for HCD manufacturers

Basic vulnerability management practices for HCD manufacturers should include the following:

a) Identifying vulnerabilities from such sources as internal testing, customer feedback, independent security researchers, and reports from vulnerability reporting centers (e.g., CERT®)[11] and other interested parties.

b) Tracking the source, verification, and correction of vulnerabilities. Due to the sensitive nature of vulnerability information, it may be advisable for manufacturers to manage this process separately from the normal bug fixing process.

c) Implementing corrections and making them available in a timely manner. Unlike normal bug fixes, corrections to critical vulnerabilities should be made available to customers as soon as possible. If necessary, manufacturers may need to provide a workaround for customers to use until a permanent correction can be developed, tested, and distributed. In severe cases, such a workaround may involve disabling HCD features or even isolating the HCD from networks.

d) Responsibly disclose vulnerability information to customers in a timely manner.

A.5.4.3 Recommended practices for IT professionals

IT professionals should consider the following guidelines for handling HCD vulnerabilities:

a) Identifying manufacturers' processes and mechanisms for disclosing vulnerability information and distributing security updates.

b) Monitor a variety of sources for relevant vulnerability disclosures, including the manufacturer but also considering sources such as national incident response centers or independent security research firms.

c) Responding to vulnerability disclosures by employing appropriate workarounds and applying necessary vulnerability fixes.

[11] CERT is registered in the U.S. Patent Office and Trademark Office by Carnegie Mellon University. This information is given for the convenience of users of this standard and does not constitute an endorsement by the IEEE of these products. Equivalent products may be used if they can be shown to lead to the same result.

A.6 Best practices for identification, authentication, and authorization

A.6.1 Introduction

The very first step in any type of security strategy is determining who are the "good guys" and who are the "bad guys." This step also applies to devices, organizations, and objects like computer code and firmware in an IT environment. To do this, the identity of the person, machine, or entity is *authenticated*. As part of organizational security this may be performed via the interview process when hiring new employees or contractors. As part of physical security this verification may be performed by a security guard at the front door, possibly with the assistance of various technical security measures.

The next step of dividing the good guys from the bad that occurs either simultaneously or immediately after authentication is *authorization,* or determining what an authenticated entity can or cannot do.

Providing secure hardcopy systems can require the authentication and authorization of many entities that interact with the system or device. The most obvious need for authentication and authorization is of course deciding if a person can or cannot use the services or functions that the HCD provides. Other events that may require authentication and authorization of a person, device, or other object include the following:

a) Deciding if a person has administrative rights to change the configuration of the HCD

b) Validating that a firmware update or applet that is being added to the HCD is from an authenticated source

c) Deciding if another computer system is indeed a valid system that should be able to communicate with the HCD

d) Validating that the User Document Data being sent to or from the HCD are from authenticated sources

A.6.2 Local authentication at the hardcopy device

A.6.2.1 Overview

Authentication of a person's identity or his level of authorized access is necessary for accounting or auditing as well as for controlling access in conjunction with the access control techniques.

Authentication mechanisms operate on the following three factors:

a) What you know (password or PIN number)

b) What you have (a token or smart card)

c) Who you are (fingerprint)

Typical levels of authorization in an HCD environment are as follows:

1) Scan and copy users (e.g., who can make copies)

2) Print users (e.g., who can release a stored job for printing or open a given print job delivery box)

3) Administrators and key operators (e.g., who can change functional configuration)

4) Service technicians (e.g., who has access to the internal components of a device or system)

5) The correlation of physically entered authentication data with authorization may be done within the device, or may use the same network-based services used for network access authentication discussed later in this sub-clause.

Note that ISO/IEC 27001:2005 [B71] deals with many of these considerations. Section 2 of that standard, System Access Control, provides guidance on the following:

- To control access to information
- To prevent unauthorized access to information systems
- To ensure the protection of networked services
- To prevent unauthorized computer access
- To detect unauthorized activities
- To ensure information security when using mobile computing and tele-networking facilities

Indeed, in this case and many others, the information provided for computer systems is directly applicable to hardcopy imaging devices.

A.6.2.2 Recommended practices for HCD manufacturers

A.6.2.2.1 Passwords and PINs

The terms *password* and *PIN* (personal identification number, which may not always be a number) are used fairly interchangeably, although a PIN is intended to identify an individual and a password is a character based key that can identify a position (e.g., administrator) rather than an individual. PINs are used extensively for ATMs and Web accounts, and most people are familiar with them. They typically range four digits to 12 alphanumeric characters. These are the easiest authorization mechanisms to implement, but particularly in the case of the 4-digit form, fairly easy to break. Indeed, because people need to remember these codes, they tend to use the same PIN in multiple places and to use sequences like their birth date, telephone number, or address. Therefore, with a fairly basic social engineering or brute force attack, an individual’s PIN can often be determined. Even authority-issued PINs are susceptible, since they are usually derived by some algorithm using some other number associated with the individual. See *Decimalization table attacks for PIN cracking, Technical Report 560* [B15].

The entering of PINs on HCD consoles is another vulnerability, since “casual” observation (or viewing via a video camera) can often determine the code by correlating the authorized person’s hand position as the characters are entered. This can be somewhat alleviated by using longer codes, by using a touch screen and “jumbling” the number positions, or by using alphanumeric sequences. Of course, as with many techniques to improve security, they also make it more difficult for authorized users to use.

Nevertheless, PINs and passwords are easy to implement and therefore are used extensively. Many guidelines, as well as vulnerability references, exist. Some of these include the following:

a) *Computer Security Art and Science* [B7]

b) “Sample Password Policies” [B140]

c) “Password Protection: Is This the Best We Can Do?” [B106]

d) Bank ATMs Converted to Steal IDs of Bank Customers [B6]

A.6.2.2.2 Password strength

A poor, weak password has the following features:

a) Contains less than eight characters

b) Is a word found in a dictionary (any language)

c) Is a common usage term such as:

    1) Name of family member, pet, friend, co-worker, fantasy character, etc.

    2) Computer term or name, command, site, company, hardware, software

    3) Name, contraction, or abbreviation of a place such as a city

    4) Birthday and other personal information such as address or phone number

    5) Word or number pattern such as: aaabbb, qwerty, zyxwvuts, 123321, etc.

    6) Any of the above spelled backwards

    7) Any of the above preceded or followed by a digit (e.g., secret1, 1secret)

A strong password has the following features:

- Contains both upper and lower case characters (e.g., a-z, A-Z)
- Has digits and punctuation characters as well as letters (e.g., 0-9,! @#$%^&*()_+|~-=\‘{}[]:”;’<>?,./)
- Is at least eight alphanumeric characters in length
- Is not a word in any language, slang, dialect, jargon, etc.
- Is not based on personal information, names of family, etc.
- Is still easily remembered

A.6.2.2.3 User education

It is recommended that users be warned to protect their PINs with statements such as: “The PIN serves as your identifier to let you access an HCD’s services. Because your PIN serves as your electronic signature, you should not give it to anyone.” Provide warning against the following:

a) Writing down a password or PIN on something accessible to others

b) Storing a password online

c) Using a word found in a dictionary

d) Using a word from a dictionary followed by 2 numbers

e) Using the names of people, places, pets, or other common items

f) Using the same password for more than one account, and for an extended period of time

g) Using the default password provided by the vendor

h) Sharing your password or hinting at its form with someone else under *any* circumstances:

   1) Over the phone to *anyone*

   2) In an e-mail message

   3) To the boss

   4) In questionnaires or security forms

   5) With family members

   6) To co-workers while on vacation

A.6.2.2.4 Password/PIN management

The following suggestions apply both to the design of the HCD, in terms of how passwords are entered and supported, and to the administrator who oversees password assignment and maintenance.

a) Store local passwords encrypted

b) Require a minimum password length

c) Limit reuse of old passwords

d) Expire passwords

e) Lock out users and log after so many login errors to ID (dictionary attack)

f) Exponentially back off before allowing another login after each failed login attempt

g) Lock out users and log after so many consecutive login errors to *any* ID (ID=PW attack)

h) No default passwords preloaded into HCD (e.g., "public" for the SNMP community name)

i) Require stronger passwords and more stringent control for higher levels of access

j) Require customer settable key sequence or password to service or maintenance mode rather than allowing default values

A.6.2.2.5 ID card/smart card/integrated circuit card authentication

Unlike magnetic stripe technology where the data on the stripe can easily be read, written, deleted, or changed with OTS equipment, the smart card usually contains an embedded 8-bit microprocessor, which actually communicates with the host computer. This allows access security checks to be conducted between the card and the device without the need of online mainframe-based computer networks for verification and processing.

Smart cards are used in many environments throughout the world where multi-factor authentication is necessary. Examples include: the U.S. Department of Defense for access authorization; the Transportation Security Administration (TSA) for identification; financial services organizations for smart payment and credit cards; transit operators for fare collection; and in universities, the entertainment industry, and other enterprises for identifications.

There are many variations to and implementation of the basic smart card technology. In considering hardcopy equipment, it would be most appropriate to use a format common to computer equipment so that users could have just one card to identify themselves. The PC/SC Working Group [12] was formed by some major contributors to the industry to specifically address the application of smart card technology to the PC environment. It has the specific objectives to:

a) Provide ICC (smart card) and IFD compatibility requirements

b) Document standard interfaces for interface devices (IFDs)

c) Document high level interfaces that abstract services supported by an ICC and associated device sharing and control mechanisms

d) Recommend general purpose ICC-based cryptographic and storage devices, designed to support existing PC and Internet standards

PC/SC Specification Version 2.0 is currently available for review.[13] There is also a Presentation of the Interoperability specification for ICCs and Personal Computer Systems, Revision 2.0.[14]

Figure A.1 indicates the basic architecture of a smart card system. Partitioning of this architecture can range from including all components of the system, the card reader (IFD), drivers (IFD handler), and the authentication infrastructure (ICC aware applications) as part of the HCD; to simply including the reader in the HCD and leveraging some external authentication server via a secure channel.

[12] See www.pcscworkgroup.com for more information.
[13] Available from: www.pcscworkgroup.com/specifications/specdownload.php.
[14] Available from: \http://www.pcscworkgroup.com/library/files/PCSC2_0WhitePaper.doc.

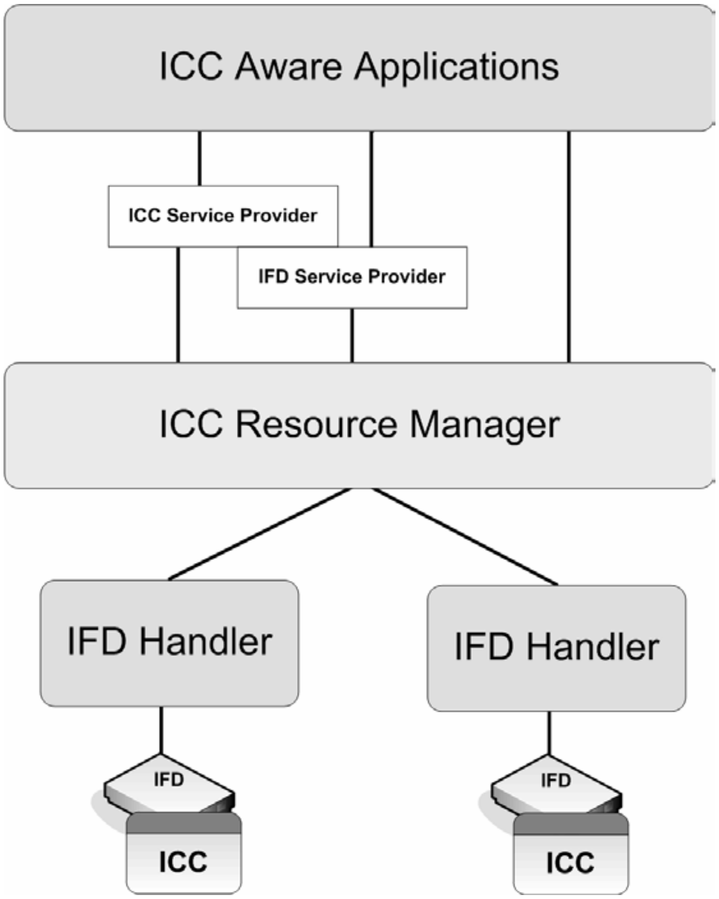

Figure A.1—ICC basic architecture

There are extensive standards and documents relating to smart cards dealing with physical issues, communication, contents, encoding or encrypting, etc. The basic technology has been largely standardized with respect to the contact (ISO/IEC 7816 [B48] to [B61]) and contactless (ISO/IEC 14443 [B62] to [B65] and ISO 15693 [B66] to [B68]) versions. However different industries and agencies have created their own standards for format, coding etc.

a) ISO 7810 Identification cards—Physical characteristics

b) ISO/IEC 7812 Identification cards—Identification of issuers

c) ISO/IEC 7816 Identification cards—Integrated circuit(s) with contacts (Parts 1-3 define the communication of cards with contacts for both memory and processor cards. Parts 4-6 are related to specification of processor card OS and are by their nature contact independent. Parts 7 and 8 will be the extensions of parts 4 and 6.)

d) ISO/IEC 10536 Identification cards—Contactless integrated circuit(s) cards [This standard specifies close coupling (slot and surface) cards communication (parts 1-3).]

e) ISO/IEC 10373 Identification cards—Test methods

f) ISO/IEC 14443 Remote coupling communication cards

g) ISO TC 68 Banking and related financial services SC 6 [15] [responsible for financial transaction cards, related financial instruments and operations, and is representing the interests of smart payment card issuers; the group is developing the standard series ISO 10202 Financial transaction cards—Security architecture of financial transaction systems using ICCs (parts 1-8)]

h) EN 742 Identification cards: location of contacts for cards and devices used in Europe [specifies the format ID-000 used for GSM subscriber identity module (SIM)]

i) EN 726 Terminal Equipment (TE); Requirements for IC cards and terminals for telecommunication use. (This standard is the technical basis for smart cards in Europe.)

j) ETSI specified also the GSM SIM. The standard has two names: GSM 11.11 and I-ETSI 300045

k) National Institute of Standards and Technology (NIST)[16] has published FIPS 140-2 [B23]

l) The Swedish government is standardizing a smart card for use by its citizens called the Secure Electronic Information in Society (SEIS) card [17]

m) Several leading credit card companies have formed a working group to create their own Integrated Circuit Card Specifications for Payment Systems, commonly called “EMV’96” or just “EMV” [18]

n) Java Card™ Forum maintains specifications for the Java Card [19, 20]

o) Leading OS vendors have also formed a group of smart card manufacturers to produce a specification for the use of smart cards on PCs and workstations called PC/SC for Personal Computer/Smart Card [21]

p) Secure electronic transactions (SET) [22] and card secured electronic transactions (C-SET) (specifications include descriptions of the smart cards they use [23]

q) Visa has published specifications for Visa Cash and the Visa Integrated Circuit Card [24]

r) USENIX Proceedings of the 1st Workshop on Smartcard Technology, May 10-11, 1999 [25]

s) The Smart Card Alliance has many publications on all facets of smart card use [26]

t) Contact-less cards based on ISO 14443 and ISO 15693

[15] Available from: www.iso.ch/meme/TC68SC6.html.

[16] See www.csrc.nist.gov/ for more information.

[17] See www.seis.se/arkivUK.html for more information.

[18] See www.mastercard.com/emv/emvspecs02.html for more information.

[19] See www.javacardforum.org for more information.

[20] Java Card is a trademark of Sun Microsystems, Inc. in the United States and other countries. This information is given for the convenience of users of this standard and does not constitute an endorsement by the IEEE of these products. Equivalent products may be used if they can be shown to lead to the same result.

[21] See www.smartcardsys.com/doc/content.html for more information.

[22] See www.mastercard.com/set/specs.html for more information.

[23] See wwwusers.imaginet.fr/~cb-mail/ for more information.

[24] See www.visa.com/cgi-bin/vee/nt/chip/visdownload.html for more information.

[25] See www.usenix.org/publications/library/proceedings/smartcard99 for more information.

[26] See www.smartcardalliance.org for more information.

A.6.2.2.6 Biometric authentication devices

Whereas the password relies upon knowing some code and the smart card relies upon having an identifying (or authorizing) object, only a device measuring some distinct physical parameter of the individual can actually claim to authenticate whom the person is. Biometric devices have the advantages of the following:

a) Providing reasonably accurate identification of a unique individual, rather than relying on some property that can be easily duplicated or passed around

b) Not requiring that the individual remember a code or have a card on their person

The disadvantages of this approach are the following:

1) It is generally more costly to implement and support than the other techniques

2) It is more difficult to register users

3) There may be user concern about using techniques associated with law enforcement, or with perceived invasions of personal privacy, or perceived dangers

Various biometric parameters are used, such as the following:

- Face
- Multimodal
- Fingerprint/palm print/thumbprint
- Retinal
- Hand and finger geometry
- Vein
- Handwriting
- Iris
- Voice/speaker

The architectures may use the same basic approach as for smart cards, with either system contained within the HCD and programmed to accept a small base of users, to allow HCDs to pass the output of biometric readers to system resources to do the authentication and return permission or denial information to the HCD.

References on biometric features and organizations include the following:

- NIST ITL May 2001 Bulletin on Biometrics [27]
- NIST Biometrics Resource [28]
- The Biometics Consortium [29]
- BioAPI Consortium—Developed under the BioAPI Consortium, BioAPI V1.1 was recently (February 13, 2002) approved as an American National Standards Institute (ANSI) standard: ANSI INCITS 358-2002, Information technology—BioAPI Specification (Version 1.1).[30]

[27] See www.itl.nist.gov/lab/bulletns/bltnmay01.htm for more information.
[28] See www.nist.gov/biometrics for more information.
[29] See www.biometrics.org/ for more information.

- The InterNational Committee for Information Technology Standards (INCITS) M1—Biometrics Technical Committee [31]
- The Common Biometric Exchange File Format (CBEFF), published in January 2001 as a NIST publication, NISTIR 6529 [32]
- The International Biometric Industry Association (IBIA) [33]
- The Biometrics Institute [34]
- International Association for Biometrics [35]

A.6.2.3 Recommended practices for IT professionals

The following guideline for IT professionals with relation to identification, authentication, and authorization should be considered:

a) Based on a security assessment of the particular environment, the IT professional should select HCDs that provide appropriate capabilities for the identification, authentication, and authorization; and deploy them per the manufacturer's recommendations.

A.6.3 Remote authentication and access control over the network

Since many of an HCD's most useful functions are accessed remotely, it is also necessary to provide the same authentication and authorization capabilities for users and devices that communicate with them over remote (i.e., LAN) connections, as that required for locally accessed functions. It should be noted that when deciding on a remote authentication mechanism, it is important to define exactly what or who needs to be authenticated. Some authentication mechanisms, (i.e., MAC address filtering and some lower level protocols) verify the identity of the device or computer that is communicating with the HCD, not the identity of the user that is actually sitting at that device and initiating the communication.

A.6.3.1 Recommended practices for HCD manufacturers

Common mechanisms for *client* or *server* authentication or access control over network include the following:

a) Mac address filtering, IP address filtering (accept connections only from predefined addresses) provides only access control and is subject to spoofing and man-in-the-middle attacks.

b) Use of protocols that support authentication at the Network Layer {e.g., VPNs using IPSec (RFCs 2401 [B116] to 2412 [B127] and 2451 [B128])}.

c) Use protocols that support authentication such as at the transport layer using SSL (client authentication only) or TLS Handshake Protocol, or protocols that support SSH. These may include the following:

    1) Applications that run over an HTTPS connection.

[30] See www.bioapi.org for more information.
[31] See www.incits.org/tc_home/m1.htm for more information.
[32] See www.nist.gov/cbeff for more information.
[33] See www.ibia.org/ for more information.
[34] See www.biometricsinstitute.org/bi/index.htm for more information.
[35] See www.afb.org.uk/ for more information.

2) Internet Printing Protocol (IPP) v1.1 (RFC 2911 [B132]), IPP uses SSL/TLS as an underlying secure protocol to provide security.

3) Network management SNMP v3 (RFCs 3411 [B133] to 3414 [B136]), SNMP 3 provides authentication of origin of data using a HMAC-MD5-96 or HMAC-SHA-96 protocol (data integrity is provided using MD5 and confidentiality is provided using CBC-DES symmetric encryption protocol).

4) Authenticated Post Office Protocol (APOP) (RFC 1734 [B110], RFC 1939 [B112]).

5) Secure Shell (SSH) is a program that is used to run commands from a remote machine securely. These commands include rlogin, ftp, telnet, rcp, etc. It uses 3DES for encryption and DSA for authentication using digital signatures.

6) Extended SMTP (ESMTP) (RFC 1869 [B111], RFC 2822 [B130]).

7) Secure MIME (S/MIME) (RFC 2311 [B115]), S/MIME provides authentication of the originator by allowing the recipient to verify the signature over a signed multipart MIME message. It is based on public key cryptography; the public key being certified using an X.509 certificated, and signatures provided using Diffie-Hellman DSS algorithms. Confidentiality is also provided using encryption algorithms like 3DES over an application/pkcs7 message.

8) Secure LDAP (LDAPS) (RFC 2251 [B114]), or applications that leverage it. The Lightweight Directory Access Protocol (LDAP) is an Internet protocol used to look up a principal identity's information that is based on the X.500 model. The protocol is made secure using SSL/TLS.

d) Use of protocols that provide or support authentication:

1) Remote Authentication Dial-In User Service (RADIUS) (RFC 2865 [B131]); RADIUS is an authentication and accounting protocol. A user name, password and other information is sent from the client to a server maintained by an Internet service provider (ISP). The password is hashed using a one-way hashing function like MD5 along with a shared secret and a pseudo random number. The Diameter Protocol (RFC 3588 [B137]) was developed to address some of the drawbacks of the RADIUS protocol. It is backwards compatible with RADIUS.

2) Terminal access controller access control system (TACACS) (RFC 1492 [B108]), TACACS is an authentication protocol for use over some networks. It is replaced by TACACS+, a protocol that provides authentication, access control, and accounting. Authentication is done using a challenge response protocol and the use of MD5 one-way hash algorithm. Accounting information provided by TACACS+ is used to bill the user for connection time.

3) Kerberos (RFC 1510 [B109]), Kerberos (Version 5) is a network authentication protocol between client and server applications using symmetric key cryptography. A central server called the *key distribution center* (KDC) maintains shared secret keys with each client or server application. When a client authenticates to a server, it proves that it is in possession of a session key provided to it by the KDC, by using the session key to encrypt an authenticator consisting of the current time, a checksum, and other information and sending it to the server application. Confidentiality is obtained using an encryption key that is exchanged between the client and server within the authenticator.

4) IPSec (RFCs 2401 [B116] to 2412 [B127] and 2451 [B128]), While SSL/TLS provide security at the transport level of the TCP/IP protocol stack, IPSec or the security protocol of IPV6 provides security at the Internet protocol level. The entire packet is encrypted using

symmetric keys that in-turn are encrypted using public keys. Thus IPSec depends upon a public key infrastructure.

e) Include password/certificate based authentication mechanism in the application.

NOTE—These transactions can be spoofed or replayed if they are not transmitted over a secure channel.

A.6.3.2 Recommended practices for IT professionals

The following guideline for IT professionals with respect to remote authentication should be considered:

a) Based on a security assessment of the particular environment, the IT professional should select HCDs that provide appropriate capabilities for remote network authentication and access control, and deploy them per the manufacturer's recommendations.

A.7 Best practices for data security

A.7.1 Introduction

Equally important to the protection of data that is "in transit" to and from an HCD, is the protection of data that is stored both temporarily and permanently in the HCD. Many HCDs use the same or compatible architectures and components, as PC systems. These hardcopy systems often contain HDDs, flash ROM, or other nonvolatile memory and can retain information related to a particular print, copy, or scan job even after processing of the job is finished. Other information that may be stored in the nonvolatile memory or hard disk of an HCD includes: user IDs, passwords, copyrighted font information, job history and configuration logs, as well as encryption keys for transport protocol algorithms.

Physical security mechanisms in some environments (i.e., Operational Environment A or B) may not be sufficient to protect the information stored in these HCDs. In these environments, technical measures (e.g., encryption and integrity checking) may be required to provide protection of the stored data. Some environments may also require special measures to ensure that no residual information encrypted or not, is recoverable from an HCD's nonvolatile memory at a later time. Examples of events that may require these measures include when the HCD is being serviced or when the device is at the end of its useful life and is being discarded.

A.7.2 Protecting data stored in the hardcopy device

A.7.2.1 Overview

Encryption algorithms and message integrity code (MIC) generation mechanisms that are used to protect data as it is transferred over the network can also be used to protect data stored in an HCD's nonvolatile memory. The major difference in the mechanisms used is that the protocol overhead for authenticating each party and exchanging encryption keys is not required; however HCDs are still required to address the issue of key generation and management when implementing encrypted file systems.

Encryption algorithms that use block ciphers (e.g., AES or 3DES) are generally better suited for the protection of data stored in an HCD rather than the various stream ciphers that are sometimes used over a network connection; however either can be used or may be appropriate for a particular environment. As with data transferred over a network connection, encryption provides only privacy of the data being stored; a MIC is still required to ensure that the data is not corrupted.

A.7.3 Disposing of data in the hardcopy device

A.7.3.1 Overview

Clearing of residual data in memory, or sanitization of nonvolatile memory in HCDs is required in some user environments regardless of whether the device has implemented an encrypted file system within its OS or not.

Functional requirements of these environments generally include the following:

a) The ability of the HCD to overwrite (sanitize) memory or storage that has been de-allocated by the device before its subsequent reuse during the normal operation of the device

b) The ability to administratively initiate or schedule a complete sanitization of all memory or storage in the HCD

Note that, in practice, clearing residual data from nonvolatile memory or HDDs to the extent that it is impossible to recover can only be accomplished by destruction of the memory or disk media or by degaussing (for magnetic media). A discussion of data recovery techniques for magnetic and other memories, as well as a recommend memory overwrite technique that can make data recovery prohibitively difficult is provided in *Secure Deletion of Data From Magnetic and Solid-State Memory* [B29], and *Data Remanence in Semiconductor Devices* [B28]. The overwrite technique suggested in these documents requires 35 independent overwrite passes of the memory block to be cleared to provide recovery protection. Another source of information for memory sanitization techniques is NIST Special Publication 800-88 [B103].

Other disk-wiping techniques may also be applicable and are listed in Table A.1.

Table A.1—Summary of disk overwriting techniques

Writing method	Write/read passes	Description	Ref:
Overwriting with zero data	1	Write each byte to 0x00	
Overwriting with random data	1	Write each byte to random data or pseudo-random data	
U.S. government DoD 5220.22-M	4	Pass 1, Random data Pass 2, Bit-wise complement of 1st pass data Pass 3, Random data again Pass 4, Read verify	[B17]
U.S. government NAVSO P-5239-26 (RLL)	4	Pass 1, 0x01 to all bytes Pass 2, 0x27FFFFFF byte pattern Pass 3, Random data Pass 4, Read verify	[B78]
U.S. government NAVSO P-5239-26 (MFM)	4	Pass 1, 0x01 to all bytes Pass 2, 0x7FFFFFFF byte pattern Pass 3, Random data Pass 4, Read verify	[B78]
U.S. government DoD 5200.28-M	3	Pass 1, ASCII “5” (0x35) to all bytes Pass 2, ASCII complement of “5” (0xCA) Pass 3, ASCII “ú” (0x97) to all bytes	[B18]
U.S. government AFSS 5020	3	Pass 1, Binary “0” (0000 0000) to all bytes Pass 2, Binary “1” (1111 1111) Pass 3, Random character to all bytes	[B1]
German standard: VSITR	7	Pass 1 thru 6, alternate sequences of 0x00 and 0xFF Pass 7, write to 0xAA	[B25]
Russian standard: GOST P50739-95	1	Overwrite each byte with 0x00 or random data sequence	[B26]
Australian ASCI 33	5	Pass 1, Write a character “C” to all bytes, verify Pass 2, Write the character’s complement “–C” to all bytes, verify Pass 3, Write “C” again Pass 4, Write “–C” again Pass 5, Fill with random characters	[B4]
British HMG Infosec Standard No. 5	3	Pass 1 and 2, Write a character then its complement Pass 3, Write with random data, then verify	[B10]
B. Schneier method	7	Pass 1, 0xFF to all bytes Pass 2, 0x00 Pass 3 thru 7, separate passes with encrypted random data	[B142]

A.7.3.2 Recommended practices for HCD manufacturers

The following guideline for HCD manufactures with respect to data security should be considered:

a) Offer one or more of the disk wiping techniques previously described

A.7.3.3 Recommended practices for IT professionals

The following guideline for IT professionals with respect to data security should be considered:

a) Based on a security assessment, use the manufacturer provided capabilities for disposing of data in an HCD

A.8 Best practices for logging and auditability

A.8.1 Usage logs and audit trails

A.8.1.1 Overview

The ability to detect and, to a certain extent, recover from breeches or attempted breeches of security is a necessary complement to the various technical security controls in an HCD. Key to this capability is the logging of the use, or attempted use, of the HCD as well as logging of security relevant events to the HCD or system.

It is important to allow administrative control over the types of security-relevant events that are logged as well as what specific information is included as part of the event record.

A.8.1.2 Recommended practices for HCD manufacturers

Suggested types of events that are security relevant include the following:

a) Any session or connection that is established to the HCD

b) All privileged (administrator) operations, such as:

   1) HCD start or stop

   2) Use of administrator level login to the device

   3) Any changes to the device's audit log configuration

   4) Any change to any user account or account privileges

   5) Any addition or deletion of a user account

   6) Any change in configuration that enables or disables access protocols or ports

   7) Any change in configuration of an access protocol or port that might affect security

   8) Any modification of system software or firmware

   9) Any change to user or administrator level access control (e.g., operator panel passwords)

c) Any access to cryptographic keys

d) Any failed attempt to establish a session or connection

e) Any failed attempt to access or perform privileged operations

f) Results of self-tests conducted by the HCD

g) Exceeding the data limits of HCD and actions taken as a result

h) Any changes or tampering detected to the logs by the HCD

Types of information normally stored in an audit log include the following:

- User ID of the access initiator
- Date and time of the access event (logon) and logoff
- Address or name of accessing system or computer
- Non-confidential document identification, if available
- Type of operation performed or attempted and if it was successful or not
- Informative message about the logged event

NOTE—Audit logs should not include authentication information such as passwords, since the audit logs may be processed or used by individuals that may have different security clearance than those contained in the audit log. However it may be desirable to indicate events such as access attempts with the user ID and password the same (a possible indication of an attack on systems where the user ID and password cannot be identical).

Because of the importance of the audit log as evidence of security relevant events, the integrity and security of the contents of the log are as important as the hardcopy system's most important User Document Data assets. In addition the protection of the integrity of the audit log, a notification mechanism in the event that the audit log malfunctions or in the event of impending failure (e.g., roll-over or running out of storage space) of the audit function is also an important capability of the audit function.

Manufacturers may consider providing formatted audit data that is compatible with intrusion detection systems for offline evaluation as well as providing onboard heuristics for real-time intrusion detection.

Manufacturers may also provide expanded auditing capabilities that include other HCD events besides those that are specifically security related, including detailed print job details and metrics useful for job accounting.

A.8.1.3 Recommended practices for IT professionals

The following guideline for IT professionals with respect to audit logs should be considered:

a) Based on a security assessment of the particular environment, the IT professional should select HCDs that provide appropriate capabilities for logging and auditing, and deploy them per the manufacturer's recommendations.

A.9 Best practices for availability of service

A.9.1 Device availability and system integrity

A.9.1.1 Overview

Another important aspect of the security of an HCD is its continued availability or robustness in the face of intentional or unintentional attempts to interfere with its normal function or to corrupt the integrity of the system. These types of attacks can range from intentional attempts to deny access to the HCD by flooding its network or fax connection with connection requests to users accidentally leaving the device offline. While there may be no way of eliminating the effect of some of these attacks, there are some technical measures that can be implemented to partially mitigate them. Threats from Clause 6 that fall into this category include the T.DOS.SMI.*, T.DOS.PRT.*, and T.DOS.FAX.* set of threats.

A.9.1.2 Recommended practices for HCD manufacturers

Technical measures that may be used in an HCD to mitigate the T.DOS.SMI attacks might include a network monitoring process that tracks all IP connections to the device and restricts the number of simultaneous connections from a single address. Another possibility is providing real-time connection status to an external network traffic monitor or network management device that may be able to detect the presence of an active network DoS attack based on network traffic patterns.

A similar concept to the network monitoring process can be applied to the T.DOS.FAX.TRAIN threat by monitoring the time it takes to complete the modem training processing (i.e., the screeching at the start of a fax/modem connect) as well as monitoring the speed negotiation process itself.

Strategies that may be considered by HCD vendors for mitigating the effect of the T.DOS.PRT and the T.DOS.FAX attacks that are based on User Document Data content include the following:

a) Monitoring the job configuration parameters of incoming jobs with regards to page count, data size, format, etc., to prevent the intentional or unintentional submission of a never-ending print job

b) Monitoring each job’s processing time via a watchdog timer to detect the presence of a never-ending job or a job that is consuming too much device processing time

c) Designing a rolling priority scheme between the major services or functions of the HCD to prevent another service from being locked out (e.g., a large print job locking out the ability to scan or copy)

Since there are some operational environments that require the processing of very time or resource consuming jobs, any timeouts that effect the processing of jobs should be capable of being configured or disabled to prevent the cancellation of legitimately submitted jobs.

Finally, the simplest DoS attack on an HCD is simply placing the device offline from the control panel; vendors may include a capability of an “auto-online” mode to allow a device that has been either accidentally or intentionally left offline, go back online after a timeout, or additionally, placing the offline control of the device in a password protected configuration menu.

A.9.1.3 Recommended practices for IT professionals

The following guideline for IT professionals with respect to availability of HCD services should be considered:

a) Based on a security assessment for the particular environment, the IT professional should select HCDs that can provide appropriate levels of availability and system integrity, and then follow the manufacturer’s guidance for configuring and deploying the devices.

Annex B

(informative)

Bibliography

[B1] Air Force Instruction 33-203, *Communications and Information, Emission Security*, available from: http://www.e-publishing.af.mil/afi33-203_afrcsup1-i.pdf.

[B2] Air Force System Security Instruction (AFSSI) 5020, *Remanence Security*, 20 Aug. 1996; http://cryptome.sabotage.org/afssi5020.htm.

[B3] Alberts, Christopher, and Dorofee; Audrey, *Managing Information Security Risks, The OCTAVE Approach.* Boston MA; Addison-Wesley, 2003.

[B4] ASCI 33, *Australian Government Information and Communications Technology Security Manual*, available from: http://www.dsd.gov.au/_lib/pdf_doc/acsi33/acsi33_u.pdf.

[B5] ASIS International, *The General Security Risk Assessment Guideline*, http://www.asisonline.org/guidelines/guidelines.pdf.

[B6] Bank ATMs Converted to Steal IDs of Bank Customers, http://www.utexas.edu/admin/utpd/atm.html.

[B7] Bishop, Matt, *Computer Security Art and Science.* Addison-Wesley: 2003.

[B8] BITS Financial Services Roundtable Master Security Criteria, http://www.bitsinfo.org/MSCv30sept03.pdf.

[B9] Bluetooth Special Interest Group, Inc., http://www.bluetooth.com.

[B10] British HMG Infosec Standard No. 5, available from: http://www.cesg.gov.uk/site/iacs/index.cfm?menuSelected=8&displayPage=8.

[B11] BS 7799-2: Information security management: Specifications with guidance for use, British Standards Institute.

[B12] Bush, W. R., Pincus, J. D., and Sielaff, D. J., "A Static Analyzer for Finding Dynamic Programming Error," *Software Practice and Experience*, vol. 30, June 2000.

[B13] *Common Sense Guide for Home and Individual Users,* Internet Security Alliance*,* http://www.isalliance.org/resources/papers/ISAhomeuser.pdf.

[B14] *Common Sense Guide to Cyber Security for Small Businesses,* Internet Security Alliance, http://www.isalliance.org/resources/papers/Common_Sense_sm_bus.pdf.

[B15] Decimalization table attacks for PIN cracking, Technical Report 560, University of Cambridge Computer Laboratory, http://www.cl.cam.ac.uk/TechReports/UCAM-CL-TR-560.pdf).

[B16] Department of Homeland Security, *IT Security Essential Body of Knowledge*, http://www.us-cert.gov/ITSecurityEBK/EBK2007.pdf.

[B17] DoD 5220.22-M, National Industrial Security Program Operating Manual (NISPOM), January 1995. www.usaid.gov/policy/ads/500/d522022m.pdf.

[B18] DoD 5200.28-M, *Techniques and Procedures for Implementing, Deactivating, Testing, and Evaluating Secure Resource-Sharing ADP System, Security Manual*, January 1973, ADA 268995; http://handle.dtic.mil/100.2/ADA268995 or http://stinet.dtic.mil/.

[B19] EIA-232-1987, Interface Between Data Terminal Equipment & Data.[36]

[36] EIA publications are available from Global Engineering Documents, 15 Inverness Way East, Englewood, Colorado 80112, USA.

[B20] E-Government Act of 2002, http://thomas.loc.gov/cgi-bin/query/z?c107:h.r.2458.enr: http://frwebgate.access.gpo.gov/cgi-bin/getdoc.cgi?dbname=107_cong_bills&docid=f:h2458enr.txt.pdf.

[B21] EU/95/46/EC, EU Data Protection Directive, http://www.cdt.org/privacy/eudirective/ EU_Directive_.html.

[B22] Federal Information Security Management Act of 2002 (FISMA), U.S. Congress, 2002, http://csrc.nist.gov/policies/FISMA-final.pdf.

[B23] FIPS 140-2, Security Requirements for Cryptographic Modules, http://csrc.nist.gov/publications/ fips/fips140-2/fips1402.pdf.

[B24] FIPS 199, Standards for Security Categorization of Federal Information and Information Systems, http://csrc.nist.gov/publications/fips/fips199/FIPS-PUB-199-final.pdf.

[B25] German standard VSITR, available from: http://www.bmi.bund.de.

[B26] GOST P50739-95, available from: http://www.technormativ.com/main.php?p=gost.

[B27] Gramm-Leach-Bliley Act, http://thomas.loc.gov/cgi-bin/query/D?c106:4:./temp/~c106i6T23B.

[B28] Gutmann, Peter, *Data Remanence in Semiconductor Devices*, http://www.cypherpunks.to/ ~peter/usenix01.pdf.

[B29] Gutmann, Peter, *Secure Deletion of Data from Magnetic and Solid-State Memory*, http://www.cs.auckland.ac.nz/~pgut001/pubs/secure_del.html.

[B30] Health Insurance Portability and Accountability Act of 1996 (HIPAA), http://thomas.loc.gov/cgi-bin/query/z?c104:H.R.3103.ENR.

[B31] Hogland, Greg, and McGraw, Gary, *Exploiting Software: How to break code*. Addison-Wesley, 2004.

[B32] HomePNA, Home Phone Network Alliance, http://www.homepna.org/.

[B33] Howard, Michael, and LeBlanc, David C., *Writing Secure Code,* 2nd edition. Microsoft Press, 2003, ISBN 0-7356-1722-8.

[B34] IEEE P2600.1 (Draft 35a, 7 May 2008), Draft Standard for a Protection Profile in Operational Environment A.[37]

[B35] IEEE P2600.2 (Draft 35a, 7 May 2008), Standard for a Protection Profile in Operational Environment B.

[B36] IEEE P2600.3 (Draft 35a, 7 May 2008), Standard for a Protection Profile in Operational Environment C.

[B37] IEEE P2600.4 (Draft 35a, 7 May 2008), Standard for a Protection Profile in Operational Environment D.

[B38] IEEE 100, *The Authoritative Dictionary of IEEE Standards Terms,* Seventh Edition. New York: Institute of Electrical and Electronics Engineers, Inc.[38, 39]

[B39] IEEE Std 802.3-2005, IEEE Standard for information technology—Telecommunications and information exchange between systems—Local and metropolitan area networks—Specific requirements—Part 3: Carrier Sense Multiple Access with Collision Detection (CSMA/CD) Access Method and Physical Layer specifications.

[37] Numbers preceded by P are IEEE authorized standards projects that were not approved by the IEEE-SA Standards Board at the time this publication went to press. For information about obtaining drafts, contact the IEEE.

[38] IEEE publications are available from the Institute of Electrical and Electronics Engineers, 445 Hoes Lane, P.O. Box 1331, Piscataway, NJ 08855-1331, USA (http://standards.ieee.org/).

[39] The standards or products referred to in this clause are trademarks of the Institute of Electrical and Electronics Engineers, Inc.

[B40] IEEE Std 802.5-1998, IEEE Standard for information technology—Telecommunications and information exchange between systems—Local and metropolitan area networks-Specific requirements—Part 5: Token Ring Access Method and Physical Layer specifications.

[B41] IEEE Std 802.11-2007, IEEE Standard for information technology—Telecommunications and information exchange between systems—Local and metropolitan area networks—Specific requirements—Part 11: Wireless LAN Medium Access Control (MAC) and Physical Layer (PHY) specifications.

[B42] IEEE Std 802.15.1-2005, IEEE Standard for information technology—Telecommunications and information exchange between systems—Local and metropolitan area networks—Specific requirements—Part 15.1: Wireless Medium Access Control (MAC) and Physical Layer (PHY) specifications for wireless person.

[B43] IEEE Std 1284-2000, IEEE Standard Signaling Method for a Bidirectional Parallel Peripheral Interface for Personal Computers.

[B44] IEEE Std 1394-1995, IEEE Standard for a High Performance Serial Bus—Firewire.

[B45] "Improving Security Across the Software Development Lifecycle," Task Force Report, April 1, 2004, *Processes to Produce Secure Software, Towards More Secure Software, Volume I,* Software Process Subgroup of the Task Force on Security Across the Software Development Life Cycle, National Cyber Security Summit, March 2004.

[B46] "Improving Security Across the Software Development Lifecycle," Task Force Report, April 1, 2004, *Improving the Patch Management Process,* Security Across the Software Development Life Cycle Task Force, Patch Management Subgroup, March 2004.

[B47] "Information Security Risk Assessment: Practices of Leading Organizations," Government Accounting Office, GAO/AIMD-00-03, November 1999.

[B48] ISO/IEC 7816-1:1998; Identification cards—Integrated circuit(s) cards with contacts—Part 1: Physical characteristics.[40]

[B49] ISO/IEC 7816-1:1998/Amd 1:2003; Maximum height of the IC contact surface.

[B50] ISO/IEC 7816-2:1999; Identification cards—Integrated circuit cards—Part 2: Cards with contacts—Dimensions and location of the contacts.

[B51] ISO/IEC 7816-2:1999/Amd 1:2004; Assignment of contacts C4 and C8.

[B52] ISO/IEC 7816-3:1997; Information technology—Identification cards—Integrated circuit(s) cards with contacts—Part 3: Electronic signals and transmission protocols.

[B53] ISO/IEC 7816-3:1997/Amd 1:2002; Electrical characteristics and class indication for integrated circuit(s) cards operating at 5 V, 3 V and 1, 8 V.

[B54] ISO/IEC 7816-4:1995; Information technology—Identification cards—Integrated circuit(s) cards with contacts—Part 4: Interindustry commands for interchange.

[B55] ISO/IEC 7816-4:1995/Amd 1:1997; secure messaging on the structures of APDU messages.

[B56] ISO/IEC 7816-5:1994; Identification cards—Integrated circuit(s) cards with contacts—Part 5: Numbering system and registration procedure for application identifiers.

[B57] ISO/IEC 7816-6:2004; Identification cards—Integrated circuit cards—Part 6: Interindustry data elements for interchange.

[B58] ISO/IEC 7816-7:1999 Identification cards—Integrated circuit(s) cards with contacts—Part 7: Interindustry commands for Structured Card Query Language (SCQL).

[40] ISO/IEC publications are available from the ISO Central Secretariat, Case Postale 56, 1 rue de Varembé, CH-1211, Genève 20, Switzerland/Suisse (http://www.iso.ch/). ISO/IEC publications are also available in the United States from Global Engineering Documents, 15 Inverness Way East, Englewood, Colorado 80112, USA (http://global.ihs.com/). Electronic copies are available in the United States from the American National Standards Institute, 25 West 43rd Street, 4th Floor, New York, NY 10036, USA (http://www.ansi.org/).

[B59] ISO/IEC 7816-8:2004 Identification cards—Integrated circuit cards—Part 8: Commands for security operations.

[B60] ISO/IEC 7816-9:2004, Identification cards—Integrated circuit cards—Part 9: Commands for card management.

[B61] ISO/IEC 7816-10:1999, Identification cards—Integrated circuit(s) cards with contacts—Part 10: Electronic signals and answer to reset for synchronous cards.

[B62] ISO/IEC 7816-11:2004, Identification cards—Integrated circuit cards—Part 11: Personal verification through biometric methods.

[B63] ISO/IEC 7816-15:2004, Identification cards—Integrated circuit cards—Part 15: Cryptographic information application.

[B64] ISO/IEC 14443-1:2000; Identification cards—Contactless integrated circuit(s) cards—Proximity cards—Part 1: Physical characteristics.

[B65] ISO/IEC 14443-2:2001; Identification cards—Contactless integrated circuit(s) cards—Proximity cards—Part 2: Radio frequency power and signal interface.

[B66] ISO/IEC 14443-3:2001; Identification cards—Contactless integrated circuit(s) cards—Proximity cards—Part 3: Initialization and anticollision.

[B67] ISO/IEC 14443-4:2001; Identification cards—Contactless integrated circuit(s) cards—Proximity cards—Part 4: Transmission protocol.

[B68] ISO/IEC 15693-1:2000; Identification cards—Contactless integrated circuit(s) cards—Vicinity cards—Part 1: Physical characteristics.

[B69] ISO/IEC 15693-2:2000; Identification cards—Contactless integrated circuit(s) cards—Vicinity cards—Part 2: Air interface and initialization.

[B70] ISO/IEC 15693-3:2001; Identification cards—Contactless integrated circuit(s) cards—Vicinity cards—Part 3: Anticollision and transmission protocol.

[B71] ISO/IEC 27001:2005, Information Technology—Code of practice for information security management.

[B72] ISO/IEC TR 15446:2004, Information Technology—Security Techniques—Guide for the production of Protection Profiles and Security Targets.

[B73] Kaufman, C., R., Perlman, and Speciner, M., *Network Security, Private Communication in a Public World.* Prentice Hall, 2002.

[B74] Leveson, Nancy G., *Safeware: System Safety and Computers*. Addison-Wesley, 1995.

[B75] McGraw, Gary, Ph.D., *Software Security White Paper*. Cigital, Inc., 2003.

[B76] MIL-STD188-161D*,* Interoperability and Performance Standards for Digital Facsimile Equipment, available from http://assist.daps.dla.mil/docimages/0001/42/73/188-161D.PD7.

[B77] NATO STANAG 5000, Interoperability of Tactical Digital Facsimile Equipment, available from http://www.nato.int/docu/standard.htm.

[B78] NAVSO P-5239-26, *Remanence Security Guidebook*, U.S. Navy, http://www.fas.org/irp/doddir/navy/5239_26.htm.

[B79] METI Policy on the Protection of Personal Information, http://www.meti.go.jp/english/information/data/IT-policy/privacy.htm.

[B80] NIST Special Publication 800-23, Guide for Security Assurance and Acquisition of Tested/Evaluated Products, http://csrc.nist.gov/publications/nistpubs.

[B81] NIST Special Publication 800-28, Guidelines on Active Content and Mobile Code, http://csrc.nist.gov/publications/nistpubs/800-28/sp800-28.pdf.

[B82] NIST Special Publication 800-30, Risk Management Guide for Information Technology Systems, http://csrc.nist.gov/publications/nistpubs/800-30/sp800-30.pdf.

[B83] NIST Special Publication 800-36, Guide for Selecting Information Security Products, http://csrc.nist.gov/publications/nistpubs.

[B84] NIST Special Publication 800-37, Guide for the Security Certification and Accreditation of Federal Information Systems, http://csrc.nist.gov/publications/nistpubs.

[B85] NIST Special Publication 800-38A, Recommendation for Block Cipher Modes of Operation—Methods and Techniques, http://csrc.nist.gov/publications/nistpubs.

[B86] NIST Special Publication 800-38B, Recommendation for Block Cipher Modes of Operation: the RMAC Mode for Authentication and Confidentiality, http://csrc.nist.gov/publications/nistpubs.

[B87] NIST Special Publication 800-38C, Recommendation for Block Cipher Modes of Operation: the CCM Mode for Authentication and Confidentiality, http://csrc.nist.gov/publications/nistpubs.

[B88] NIST Special Publication 800-40, Creating a Patch and Vulnerability Management Program, http://csrc.nist.gov/publications/nistnubs/800-40-Ver2/sn800-40v2.pdf.

[B89] NIST Special Publication 800-41, Guidelines on Firewalls and Firewall Policy, http://csrc.nist gov/publications/nistnubs/800-41/sp800-41.pdf.

[B90] NIST Special Publication 800-42, Guideline on Network Security Testing, http://csrc.nist.gov/publications/nistpubs/800-42/NIST-SP800-42.pdf.

[B91] NIST Special Publication 800-43, Systems Administration Guidance for Securing Microsoft Windows 2000 Professional System, http://csrc.nist.gov/itsec/guidance W2Kpro.html.

[B92] NIST Special Publication 800-47, Security Guide for Interconnecting Information Technology Systems, http://csrc.nist.gov/publications/nistpubs.

[B93] NIST Special Publication 800-48, Wireless Network Security: 802.11, Bluetooth and Handheld Devices, http://csrc.nist.gov/publications/nistpubs/800-48/NIST SP 800-48.pdf.

[B94] NIST Special Publication 800-52, Guidelines for the Selection and Use of Transport Layer Security (TLS) Implementations, June 2005, http://csrc.nist.gov/publications/nistpubs/800-52/SP800-52.pdf.

[B95] NIST Special Publication 800-53, Recommended Security Controls for Federal Information Systems, http://csrc.nist.gov/publications/nistpubs/800-53-Rev2/sp800-53-rev2-final.pdf.

[B96] NIST Special Publication 800-55, Security Metrics Guide for Information Technology Systems, http://csrc.nist.gov/publications/nistpubs.

[B97] NIST Special Publication 800-57, Recommendation on Key Management, http://csrc.nist.gov/publications/nistpubs.

[B98] NIST Special Publication 800-60, Guide for Mapping Types of Information and Information Systems to Security Categories, June 2004, http://csrc.nist.gov/publications/nistpubs.

[B99] NIST Special Publication 800-61, Computer Security Incident Handling Guide, http:// http://csrc.nist.gov/publications/nistpubs/800-61/sn800-61/pdf.

[B100] NIST Special Publication 800-67, Recommendation for the Triple Data Encryption Algorithm (TDEA) Block Cypher, http://csrc.nist.gov/publications/nistpubs.

[B101] NIST Special Publication 800-68, Guidance for Securing Microsoft Windows XP Systems for IT Professionals: A NIST Security Configuration Checklist, http://csrc.nist.gov/itsec/guidance_WinXP.html.

[B102] NIST Special Publication 800-70, Security Configuration Checklists Program for IT Products, available from http://csrc.nist.gov/checklists/download_sp800-70.html.

[B103] NIST Special Publication 800-88, Guidelines for Media Sanitations: Recommendations of the National Institute of Standards and Technology, http://csrc.nist.gov/publications/nistpubs/800-88/NISTSP800-88_rev1.pdf.

[B104] NSSTISSAM TEMPEST/1-92, Compromising Emanations Laboratory Test Standard, Electromagnetics, 15 Dec. 1992. http://cryptome.org/nt1-92-1-5.htm.

[B105] OCTAVE, Operationally Critical Threat, Asset, and Vulnerability Evaluation, http://www.cert.org/octave/.

[B106] "Password Protection: Is This the Best We Can Do?," SANS' Information Security Reading Room, http://www.sans.org/rr/whitepapers/authentication/114.php.

[B107] Personal Health Information Protection Act of 2004 (PHIPA), available from http://www.e-laws.gov.on.ca/DBLaws/Statutes/English/04p03_e.htm.

[B108] RFC 1492, An Access Control Protocol, Sometimes Called TACACS. C. Finseth. July 1993.[41]

[B109] RFC 1510, The Kerberos Network Authentication Service (V5). J. Kohl, C. Neuman. September 1993.

[B110] RFC 1734, POP3 AUTHentication command. J. Myers. December 1994.

[B111] RFC 1869, SMTP Service Extensions. J. Klensin, N. Freed, M. Rose, E. Stefferud, D. Crocker. November 1995.

[B112] RFC 1939, Post Office Protocol - Version 3. J. Myers, M. Rose. May 1996.

[B113] RFC 2246, The TLS Protocol Version 1.0. T. Dierks, C. Allen. January 1999.

[B114] RFC 2251, Lightweight Directory Access Protocol (v3). M. Wahl, T. Howes, S. Kille. December 1997.

[B115] RFC 2311, S/MIME Version 2 Message Specification. S. Dusse, P. Hoffman, B. Ramsdell, L. Lundblade, L. Repka. March 1998.

[B116] RFC 2401, Security Architecture for the Internet Protocol. S. Kent, R. Atkinson. November 1998.

[B117] RFC 2402, IP Authentication Header. S. Kent, R. Atkinson. November 1998.

[B118] RFC 2403, The Use of HMAC-MD5-96 within ESP and AH. C. Madson, R. Glenn. November 1998.

[B119] RFC 2404, The Use of HMAC-SHA-1-96 within ESP and AH. C. Madson, R. Glenn. November 1998.

[B120] RFC 2405, The ESP DES-CBC Cipher Algorithm With Explicit IV. C. Madson, N. Doraswamy. November 1998.

[B121] RFC 2406, IP Encapsulating Security Payload (ESP). S. Kent, R. Atkinson. November 1998.

[B122] RFC 2407, The Internet IP Security Domain of Interpretation for ISAKMP. D. Piper. November 1998.

[B123] RFC 2408, Internet Security Association and Key Management Protocol (ISAKMP). D. Maughan, M. Schertler, M. Schneider, J. Turner. November 1998.

[B124] RFC 2409, The Internet Key Exchange (IKE). D. Harkins, D. Carrel. November 1998.

[B125] RFC 2410, The NULL Encryption Algorithm and Its Use With IPsec. R. Glenn, S. Kent. November 1998.

[B126] RFC 2411, IP Security Document Roadmap. R. Thayer, N. Doraswamy, R. Glenn. November 1998.

[B127] RFC 2412, The OAKLEY Key Determination Protocol. H. Orman. November 1998.

[B128] RFC 2451, The ESP CBC-Mode Cipher Algorithms. R. Pereira, R. Adams. November 1998.

[B129] RFC2703, Protocol-independent Content Negotiation Framework [CONNEG].

[41] RFCs are available from: www.ietf.org/rfc.html.

[B130] RFC 2822, Internet Message Format. P. Resnick, Ed. April 2001.

[B131] RFC 2865, Remote Authentication Dial In User Service (RADIUS). C. Rigney, S. Willens, A. Rubens, W. Simpson. June 2000.

[B132] RFC 2911, Internet Printing Protocol/1.1: Model and Semantics. T. Hastings, Ed., R. Herriot, R. deBry, S. Isaacson, P. Powell. September 2000.

[B133] RFC 3411, An Architecture for Describing Simple Network Management Protocol (SNMP) Management Frameworks. D. Harrington, R. Presuhn, B. Wijnen. December 2002.

[B134] RFC 3412, Message Processing and Dispatching for the Simple Network Management Protocol (SNMP). J. Case, D. Harrington, R. Presuhn, B. Wijnen. December 2002.

[B135] RFC 3413, Simple Network Management Protocol (SNMP) Applications. D. Levi, P. Meyer, B. Stewart. December 2002.

[B136] RFC 3414, User-based Security Model (USM) for version 3 of the Simple Network Management Protocol (SNMPv3). U. Blumenthal, B. Wijnen. December 2002.

[B137] RFC 3588, Diameter Base Protocol, J. Loughney, E. Guttman, G. Zorn, J. Arkko, J. A. Ericsson, September 2003.

[B138] Rodriguez, A., et al., *TCP/IP Tutorial and Technical Overview,* 7th Edition, IBM Redbook, Prentice Hall, 2002.

[B139] Ruth, Andy, and Hudson, Kurt, *Security+ Certification.* Microsoft Press, 2003.

[B140] "Sample Password Policies," SANS' Information Security Reading Room http://www.sans.org/resources/policies/Password_Policy.pdf.

[B141] Sarbanes-Oxley Act of 2002, http://thomas.loc.gov/cgi-bin/query/z?c107:H.R.3763.ENR.

[B142] Schneier, Bruce, *Applied Cryptography.* John Wiley & Sons, 1996.

[B143] Schneier, Bruce, *Secrets and Lies: Digital Security in a Networked World*. John Wiley & Sons, 2000.

[B144] Security Focus Newsletter #253, 6/16/04, http://www.securityfocus.com.

[B145] Senate Bill 1386, State of California, 2002, regarding the release of personal information; available from, http://info.sen.ca.gov/pub/01-02/bill/sen/sb_1351-1400/sb_1386_bill_20020926_chaptered.pdf.

[B146] Swiderski, F., and Snyder, W., *Threat Modeling*. Microsoft Press, 2004.

[B147] TEMPEST INC., http://www.tempest-inc.com/.

[B148] USB, Universal Serial Bus Revision 2.0, available from http://www.usb.org/developers/docs/.

[B149] Viega, John, and McGraw, Gary, *Building Secure Software.* Addison-Wesley, 2002, ISBN 0-201-72152-X.

[B150] Wheeler, David A., *Secure Programming for Linux and UNIX HOWTO*, 2003.

[B151] Wi-Fi Alliance, http://www.wi-fi.org.