

P2600 Hardcopy Device and System Security

February 3-4, 2004

1. Attendees

Lee Farrell	Canon Development Americas
Brian Volkoff	Hewlett Packard
Ron Bergman	Hitachi Printing Solutions
Stuart Rowley	Kyocera
Jerry Thrasher	Lexmark
Don Wright	Lexmark
Jean-Claude Longo	Océ
Stefaan Deschrijver	Print 4Sight
Satoshi Fujitani	Ricoh
Shumpei Tamaki	Ricoh
Daniel Manchala	Xerox

2. Administrivia

Don Wright led the meeting and provided the planned agenda topics:

- Opening, Introductions, Attendance
- Review IEEE Patent Policy
- Mailing list and Website
- Review/Approve Operating Procedures
- Election of Officers
- Identify Document Editor(s)
- Requirements Document
- Content Outline
- Assign Sections to Authors/Editors
- Future Meeting Plans

3. Opening/Introduction

Don reviewed the Project Authorization Request (PAR) Scope and Purpose for this activity:

He noted that Lexmark is currently engaging with high-profile, security-aware customers including both commercial and public sector to get their participation in this effort. He encouraged other company representatives to do the same.

4. Review IEEE Patent Policy

The standard two slides discussing IEEE Patent Policy and appropriate meeting behavior were presented and reviewed with the group:

5. Mailing List and Website

The following details were provided:

- P2600 website: <http://grouper.ieee.org/groups/2600>
- Mailing list:
 - * Majordomo run by the IEEE
 - * Archive is available via the website
 - * Subscribe by sending a message to majordomo@ieee.org containing the text: “subscribe stds-2600”
 - * Only subscribers may send e-mail to the mailing list

6. Review/Approve Operating Procedures

Don reviewed the Operating Procedures document that he distributed, and noted that the group needs to agree to adhere to the procedures described in the document.

MOTION: Move to approve the Operating Procedures for the Hardcopy Security Working Group as published on the P2600 Website.

VOTE: The group voted to adopt the Operating Procedures.

7. Election of Officers

Three Officer positions were identified: Chair, Vice-Chair, and Secretary. Each of the positions lasts for a two-year term. Don Wright was nominated as Chair. There were no other nominations.

VOTE: Don Wright was voted in as Chair.

No one volunteered for the positions of Secretary or Vice-Chair. Don suggested that official nominations and elections could be delayed for a while.

Although he could not commit to the position of Secretary, Lee Farrell volunteered to record the Minutes for this meeting.

8. Identify Document Editor(s)

The following people all indicated interest in acting as Editor(s) for the group:

Ron Bergman
Stefaan Deschrijver
Jerry Thrasher
Brian Volkoff

9. Requirements Document

Don listed several components of Hardcopy Security and reviewed his ideas on “Translating Theory to Reality.”

Components of Hardcopy Security:

- Physical

- Authentication
- Authorization
- Privacy
- Integrity
- Monitoring / Auditing
- Device Management
- Document Security
- Restrictive Rules and Legislation
- Customer perceptions (correct or incorrect)

The group discussed the possible course of developing requirements to drive the specification document(s). It was suggested that a parallel path of known requirements and Use Case scenarios (for focusing requirements) should be examined.

It was also suggested that Microsoft (and others?) should be solicited for comments/ideas on the topic.

Don asked the group if anyone had any scenarios to suggest for consideration. Stefaan Deschrijver said that the different security environments would probably have different requirements. It was suggested that a matrix of Environment vs. Requirement should be considered.

During subsequent discussion, it was also noted that the effort of identifying possible security threats would be useful as a first step toward identifying possible requirements.

Including the items presented by Don, the following ideas were raised:

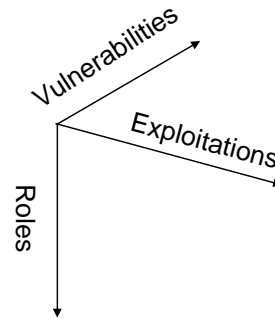
- Encryption of content both to and from device
- Identification of users at device
 - * Magstripe, smartcards, proximity cards, etc.
 - * Passwords, PINs
 - * Biometrics
- Physical protection of input forms/paper and output
 - * Locks
 - * Print and Hold
- Management and Configuration
 - * Turning off unnecessary protocols and ports
 - * Securing necessary ports (e.g., running IPsec over FTP)
 - * Restricting reconfiguration
 - * Management Web page security/protection
 - * Protection against unauthorized firmware updates
 - * Remote management and configuration ports (network, POTS etc.) on H/C devices could be used as access points into network
 - * Security implications of automated configuration (BOOTP, DHCP, etc.) both hacking the server and spoofing
- Digitally signed documents
 - * To the device
 - * From the device
- Protection of residual data
- Fax to Network path control and protection
- Monitoring and Auditing

- Redistribution of viruses, Trojan horses, etc. by hardcopy devices
- Control over embedded Java, scripting, other execution languages within the device. Granular control vs. global on/off
- Over-the-wire security (e.g., end-user digital certificates) for standard and proprietary protocols. Varies from protocol to protocol
- Denial of service (e.g. looping PostScript code, corrupted resident/permanent font download, corrupt firmware download)

As some of the specific potential “attacks” were discussed, it was noted that different “vulnerabilities” were being identified—sometimes being exploited by using different methods. Jerry Thrasher suggested that the group should note the different areas of vulnerability—and use that list to help generate more requirements.

Three orthogonal dimensions were identified:

- Vulnerabilities
- Exploitations
- “Roles” (e.g., Print/Scan/Fax/Copy/Manage, etc)



Some Vulnerabilities and sample exploits were identified:

- Denial of Service
 - * Exploit: downloading corrupt firmware, looping PostScript, packet flooding
- Exposure of print and scan data
 - * Exploit: taking output from output tray, steal printer, read hard disk
- Using device as gateway into the network
 - * Exploit: spreading viruses, Trojan horses, etc.
- Theft of Service
 - * Exploit: steal printer, steal memory/hard disk, etc.

During the discussion, the concept of “levels of security” was raised. The group generally agreed that they should avoid recommending what level of security might be appropriate or adequate for a given environment (e.g., small business)—because there will always be exceptions. Instead, it was agreed that the three dimensions above should be focused upon first. If necessary, “Environment” will be addressed later.

The group then decided to address a single Role and attempt to identify its relevant Vulnerabilities.

Print Vulnerabilities:

- Denial of service
- Unauthorized access to print data (on network, on hard disk, on paper)
- Theft of service / unauthorized usage of service and/or resources
- Theft of user identity (e.g., capturing magstripe information)
- Corruption/alteration of print data

It was noted that there are many possible variants of “denial of service.”

Scan Vulnerabilities:

- Denial of service
- Unauthorized access to scan data (on network, on hard disk)
- Theft of service – unauthorized usage of service and/or resources
- Theft of user identity (e.g., capturing magstripe information)
- Corruption/alteration of scanned data
- Using scanner as a data generator for denial of service elsewhere
- Theft of input document(s) (if operator walks away)

While discussing scanning vulnerabilities, it was noted that some scanners are smart enough to detect—and deny—the scanning of currency. Should such attempts be considered a vulnerability? It was decided that this should be classified as “policy”—and out of scope.

It was noted that the group had not yet considered the topic of monitoring and leaving an audit trail of device usage – as a possible tool for tracking and discovering potential security breaches.

Copy Vulnerabilities:

- Denial of service
- Unauthorized access to scan data (on network, on hard disk) (e.g., Java applet that secretly sends copied data to e-mail address(es))
- Theft of service – unauthorized usage of service and/or resources
- Theft of user identity (e.g., capturing magstripe information)
- Corruption/alteration of copier data (e.g., adding information to a document making it look like it was copied—or even created—at a different date/time/place than it really was)
- Theft of physical input or output document(s) if operator walks away

There was some discussion about whether a Copier really had any unique characteristics that might create any vulnerabilities different than a Scanner.

Fax Vulnerabilities:

- Denial of service
- As an agent for a POTS denial of service
- Unauthorized access to faxed data (on network, on hard disk) (e.g., Java applet that secretly sends data to e-mail address(es) or another phone number)
- Theft of service – unauthorized usage of service and/or resources (both sending and receiving faxes)
- Theft of user identity (e.g., capturing magstripe information)
- Corruption/alteration of fax data or metadata (e.g., adding information to a document making it look like it was faxed at a different date/time/phone number than it really was)
- Theft of physical input document(s) if operator walks away

10. Schedule

Don explained that the PAR includes estimates of the end-points of the schedule:

- Sponsor Ballot: June 2005
- Submission to RevCom: Feb 2006
- Meetings every 6-8 weeks

- Some meetings aligned with other industry/standards meetings

He acknowledged that this is probably an aggressive schedule goal—but thinks that the market will be demanding results before the group is complete.

11. Future Meeting Plans

Don raised the topic of future meetings, and discussed the possibility of trying to coordinate with the Printer Working Group (PWG) during the year. The discussion resulted in the following schedule:

Mar 10-11	Piscataway, NJ
Apr 19-20	with PWG – Washington, D.C.
May 27-28	with PWG – Tokyo? [or without PWG Jun 2-3, TBD]
Jul 22-23	with PWG – Montreal
Sep 1-2	TBD
Oct 6-7	Lexington, KY
Nov 18-19	with PWG – TBD

12. Scope

During the discussion of the future schedule, Stuart Rowley commented on the potential of the Scope of this activity being very large. He is concerned about possible “feature creep” over time. Don agreed that it is a reasonable concern, and he said that he is comfortable with the group refining the intended scope over the next few meetings. He did not think it was likely that the group would be able to adequately define the scope before/during the first meeting.

The group will need to be specific about how to “lock down” the devices. It is likely that each Printer/Device manufacturer will need to explain the details of how the “lock down” can be achieved on their individual products.

13. Expectations of Microsoft Contribution

Don explained that he has been in contact with Thomas Nielsen of Microsoft. Nielsen requested that the group should identify any detailed expectations of what they hope to achieve with Microsoft’s participation.

Some expectations were listed:

- An understanding of the system side requirements and capabilities of print security
 - * How can the spooler be secured?
 - * Securing print jobs from the client to the server is probably out of scope for this project but from a customer’s perspective it is a real issue as a part of the total Hardcopy Security area
 - * What are other standards bodies doing that affect spooler/print security?
- Without a total system perspective, work done to secure the hardcopy devices and the content to and from them is ineffective
- This group would be a good forum for the exchange of security requirements both from and to Microsoft
- Awareness of new tools and capabilities in future OS releases that could be used by the Hardcopy industry to implement security capabilities

Stuart expressed doubt about the practicality of including the effort of securing print jobs from client to server in the scope of the group activity. Don agreed that he is not interested in broadening the scope, but he thinks it is still valuable to obtain Microsoft's perspective from a system viewpoint. One individual questioned whether Microsoft—or any other OS vendor—is actually willing to revamp their system to support the desired security.

14. Requirements Document – cont'd

The group spent most of the remainder of the day with the discussion about Role Vulnerabilities. This time, individual “Exploits” were also identified.

Managed Device Vulnerabilities:

- Integrity of device's logs
 - * Unauthorized access to or alteration of a transaction log
 - * Unauthorized deletion of log(s)
- Configuration management
 - * Unauthorized firmware updates
 - * Unlocked operator panel
 - * SNMPv1 with “public” community name
- Security management
 - * BOOTP Server spoofing
 - * Unlocked Operator Panel
 - * Unauthorized firmware updates
- Denial of service
 - * Disabling ports and/or protocols
 - * Starting a flash memory update cycle without ever finishing
- Agent for a denial of service attack
 - * Setting a very short interval on a network operation (e.g. service discovery broadcasts)
- Theft of security information (e.g. user lists, passwords, etc.)
 - * Use of management application to create backdoor to steal identity information

There was general acknowledgement that it is sometimes difficult to distinguish between some “vulnerabilities” vs. “exploits.” For example, is “unauthorized configuration changes” an exploit, or a vulnerability? It was noted that sometimes one vulnerability is actually an exploit to another [higher] level vulnerability.

Network Device Vulnerabilities:

- Agent for a denial of service attack (packet flooding, etc.)
 - * Assuming the IP address of a device to cause perpetual network errors operation
- Theft of device's identification (e.g. spoofing)
 - * Masquerade as a hard copy device and capture all the device's jobs/traffic
 - * Change DNS server to point printer DNS name to another device to capture network traffic
- Unauthorized access to the network
 - * Bridging fax modem to Ethernet
 - * Remote access phone line bridged to Ethernet
 - * Bridging two separate networks together using two network adapters in device

- Being capable of being infected by a virus or Trojan Horse
 - * Running an embedded version of a popular operating system which is susceptible to viruses/Trojan horses
- Spreading viruses or Trojan horses
 - * Support for executing common file formats
 - * Device provides open mail relay
- Denial of service
 - * Change IP address to be the same as another device on the network
 - * Replace Cat5 cable with Cat3 cable
- Agent for unauthorized network usage
 - * Telnet-ing into a device that has a general purpose OS embedded—and then using its rights and OS functions for unintended operations

At this point, the previous Role Vulnerabilities were revisited, and specific exploits were added. During this process, it was noted that many of the vulnerabilities and exploits appear to be common to many “roles.” It was suggested that only a few examples should be done by the group as a whole, and that a homework assignment for everyone would be to think up additional examples for submission via e-mail.

While noting some of the denial of service exploits that require physical access to the device (e.g., unplugging power cord, scratching scan head, etc.), it was suggested that identifying methods for resolving Physical security issues should be considered out of scope.

Print Vulnerabilities:

- Denial of service
 - * Looping PostScript job
 - * PJJ and other device control language
 - * Unauthorized firmware update
 - * Unplug device power cable, data cables, etc.
 - * Take device offline with control panel
- Unauthorized access to print data (on network, on hard disk, on paper)
 - * Network sniffing of print job
 - * Reading residual data off the hard disk
 - * Steal output from hopper
 - * Compromised user id means (pin #, proximity card, etc.) causing job to be released
- Theft of service / unauthorized usage of service and/or resources
 - * Stolen check stock from input tray
 - * Unauthorized user access to color printing capability
- Theft of user identity (e.g., capturing magstripe information)
 - * Network sniffing of user id information from printer to LDAP server
- Corruption/alteration of print data
 - * Man-in-the-middle capture/alter/resend print job
 - * Unauthorized replacement of e-form or the variable data on the e-form
 - * Font alteration to turn all characters into blanks (print signed, blank checks)

Scan Vulnerabilities:

- Denial of service
 - * Looping execution occurring on other roles (e.g., Looping PostScript job on Printer leaves no cycles for scanning)
 - * Unauthorized firmware changes
 - * Destination device full (ftp server, mail server, etc.)
- Unauthorized access to scan data (on network, on hard disk)
 - * Network sniffer
 - * Secretly send copies of scanned data to other destination(s)
- Theft of service – unauthorized usage of service and/or resources
 - * Unauthorized use of scanner
- Theft of user identity (e.g., capturing magstripe information)
 - * Network sniffing of user id information on the way to the LDAP server
- Corruption/alteration of scanned data
 - * Man-in-the-middle capture/alter/resend
 - * Capture ftp server userid/password and replace scanned file
- Using scanner as a data generator for denial of service elsewhere
 - * Scan large document to all e-mail addresses in corporate address book
- Theft of input document(s) (if operator walks away)
 - * Cause operator to walk away, and then take input document

Copy Vulnerabilities:

- Denial of service
 - * Looping execution occurring on other roles (e.g., Looping PostScript job on Printer prevents copying)
 - * Unauthorized firmware changes
- Unauthorized access to copied data (on network, on hard disk)
 - * Steal hard disk with residual data from copying
 - * Java applet that secretly sends copied data to e-mail address(es)
- Theft of service – unauthorized usage of service and/or resources
 - * Unauthorized use of copier
 - * Stolen copier access code(s)
 - * Compromise copy counts
- Theft of user identity (e.g., capturing magstripe information)
 - * Network sniffing of user id information on the way to the LDAP server
 - * Steal hard disk containing user lists
- Corruption/alteration of copier data (e.g., adding information to a document making it look like it was copied—or even created—at a different date/time/place than it really was)
 - * Java applet that reduces copy quality to fax quality and adds fax-like headers and footer to a document
 - * Java applet to forge Bates stamp/number on legal documents
 - * Misapplication of signatures, hanko stamps, notary stamps, watermarks, etc.
 - * Printing of barcode containing maliciously incorrect information
- Theft of physical input or output document(s) if operator walks away
 - * Distract operator and steal input document(s)

Fax Vulnerabilities:

- Denial of service
 - * Unplug phone cord
 - * Physical injection of noise on the phone line
 - * Disabling of user id device reader
- As an agent for a POTS denial of service
 - * Unauthorized firmware update that never completes negotiation with remote fax machine
 - * Sending huge documents repeatedly to a fax device
- Unauthorized access to faxed data (on network, on hard disk, on paper)
 - * Java applet that secretly sends data to e-mail address(es) or another phone number
 - * Phone line sniffer installed outside building or in wiring closet, etc.
 - * Take output from device after hours
- Theft of service – unauthorized usage of service and/or resources (both sending and receiving faxes)
 - * Configuration change to disable security
- Theft of user identity (e.g., capturing magstripe information)
 - * Rogue MEAP applet capturing magstripe identity data
- Corruption/alteration of fax data or metadata
 - * Adding information to a document making it look like it was faxed at a different date/time/phone number than it really was
- Theft of physical input document(s) if operator walks away
 - * Distract operator and steal input document(s)

15. Assign Sections to Authors/Editors

Each of the Roles was then assigned to individuals to expand the initial lists of vulnerabilities and exploits:

Print	Jean Claude Longo
Copy	Satoshi Fujitani
Fax	Jerry Thrasher
Network Device	Ron Bergman
Managed Device	Stuart Rowley
Scan	Stefaan Deschrijver

ACTION: The individuals responsible for Role vulnerability/exploit expansion will distribute their results via e-mail on or before March 1 (one week prior to the next meeting.)

16. Content Outline

Don highlighted some agreements reached about the intended content of the Standard:

- Profile based on Common Criteria
- Rationale based on work don on Role/Vulnerabilities/Exploits
- “Extension” of Common Criteria to cover hardcopy unique areas (e.g., output bin locks)

Hardcopy Device and System Security meeting adjourned.

17. Action Item Summary

ACTION: The individuals responsible for Role vulnerability/exploit expansion will distribute their results via e-mail on or before March 1 (one week prior to the next meeting.)

18. Future Meetings and Events

Future Hardcopy Device and System Security meetings are scheduled as follows:

Mar 10-11	Piscataway, NJ
Apr 19-20	Washington, D.C.
May 27-28 or Jun 2-3	Tokyo or <TBD>
Jul 22-23	Montreal
Sep 1-2	<TBD>
Oct 6-7	Lexington, KY
Nov 18-19	<TBD>