

**Sharp's MFP Security Suite –
The best of the best in the Market**

April 2010

Specifications are subject to change without notice.

Sharp's MFP Security Suite – The best of the best in the Market



BERTL's 2009 Award
Best Security Solution Suite
for 6 years 2004-2009



BLI Award
Outstanding MFP Security
Solution



BLI Award
The best IT friendly

Topics

- Market & End Users MFP Security Requirements
- MFP Vulnerabilities without Sharp Security
- Sharp Mitigations to MFP Vulnerabilities
- Recommendations to the End User / Purchasing

Why do we need Security on the MFP?

- Organizations spend significant capital to protect digital assets from threats, yet frequently overlook one of the most integral devices in use today - the office Multi-Function Peripheral (MFP).
- The more advanced and integrated MFPs become, the greater the risk to confidential information during the document's life cycle when it is being copied, printed, scanned or faxed.
- For a comprehensive security strategy to be effective, it is imperative for organizations to demand a greater level of protection from MFP vulnerabilities.

COMMON VULNERABILITIES

Some of the most common vulnerabilities associated with an unsecured MFP include:

- Identity Theft
- Stolen information
- Lawsuits
- Mandates Information Security Regulation
 - HIPAA, Sarbanes-Oxley, Gramm-Leach-Bliley Act
- Loss of access
- Unauthorized use
- Loss of productivity

Intellectual capital assets account for over 57% of a corporation's market price

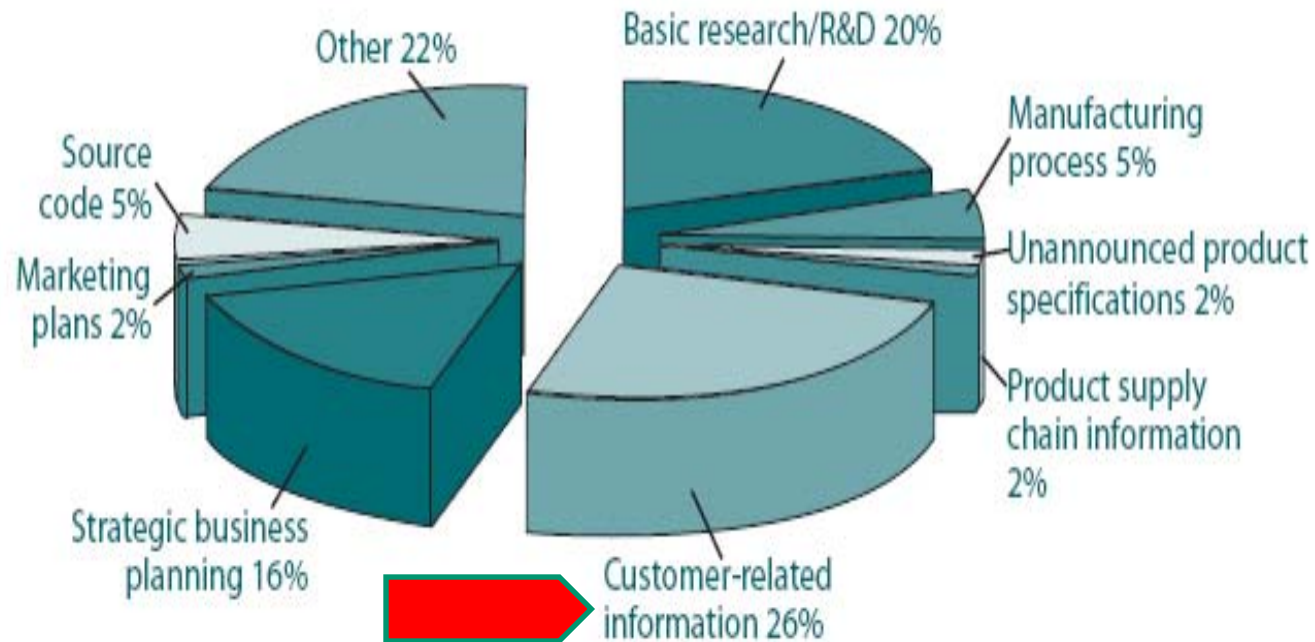


Multi-Function Copier Purchasing Decisions in the Networked Digital Office

- The MFP decision has shifted from facilities management staff, to Computer Information and Network management staff (IT), and to Information Assurance - Security Staff (IA).
- If IA does not approve the connection to the network and the proposed MFPs because of Information and Network vulnerabilities, the acquired product may never be deployed with its full cost saving capabilities.
- If new policies regarding support for new protocols and controls (IPv6, CAC, Remote Administration and Monitoring, Communications, Document and Information Management Interface, etc.) are not addressed by the MFP acquisition team, the product may be obsolete a few years into a long term contract.
- Some Standard Requirements are Common Criteria, NMCI and ONENET certification, legacy networks, HIPAA, new cyber-security regulations, fax, scanning applications, etc.

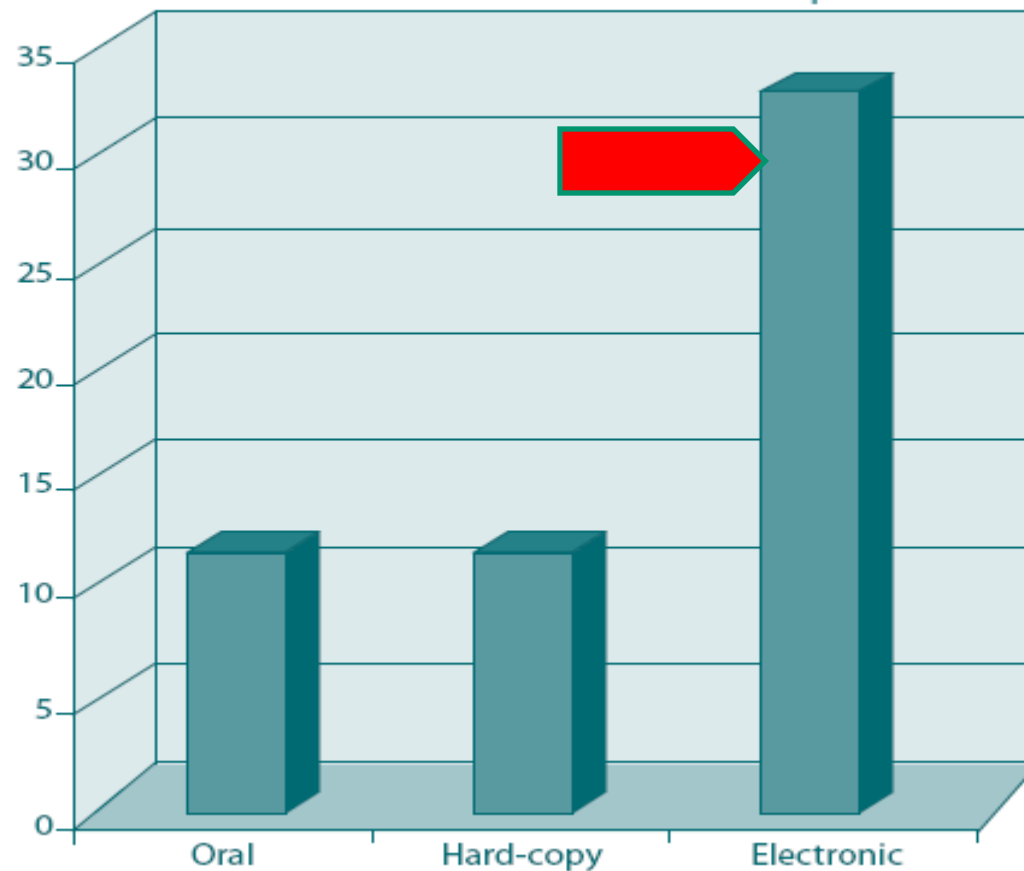
Areas of Reported Theft

Figure 6. Single-Most-Significant Loss Incident Type of Information Asset



Form of Information When it was Compromised

Figure 5. Single-Most-Significant Loss Incident
Form of Information When it was Compromised



Business/National Security Impact of Loss

Table 16. Single-Most-Significant Loss Incident
Business Impact of Loss

	Percentage (%)
Loss of competitive advantage in one product/service	24
Loss of competitive advantage in multiple products/services	10
Loss of core business technology or process	10
Loss of company reputation, image, and/or goodwill	29
Reduced projected/anticipated returns or profitability	14
Loss of information or technology that may weaken U.S. economic and/or strategic military advantage	6
Loss of information that may make the organization more vulnerable to terrorist threats	6
Loss of information or prototypes that may facilitate product counterfeiting	1



Market and End User Requirements

Protection against unauthorized access to intellectual property and confidential information that passes through the MFP

■ The Requirement:

- ❑ To protect sensitive or confidential information (Company or Personal)
- ❑ To protect other users documents
- ❑ To protect 3rd Party Information (medical, financial, etc) to meet Regulatory compliance
- ❑ To protect personal information such as Soc Number, credit card information, e-mail addresses and contact information

O-Kay!



■ The Threat:

- ❑ Removing or examining documents from an output tray

Market and End User Requirements

Limit Legal liabilities due to new privacy laws and regulations

■ Laws and Regulations:

❑ **Identity theft**

- ❑ HIPAA (Protect patient information)
- ❑ SOX (Sarbanes - Oxley) (Protect financial information)
- ❑ GLB (Gramm-Leach-Bliley Act) (Protect consumer journal information)
- ❑ State Privacy laws

❑ **IEEE 2600™ -2008 security standard**

■ The Mitigation:

- ❑ Confidential Print and Fax
- ❑ Document Control
- ❑ User Authentication
- ❑ Forced sender name and authentication for e-mail
- ❑ Password protect folder and documents
- ❑ Data Security Kit with encryption and overwrite
- ❑ Audit log for all MFP activities (scan, print, copy, fax, e-mail)
E-mail log file includes: from, to, when, what (file name and content)
- ❑ Automated Rights Management
- ❑ Automated Encryption of transmitted documents (scan, print)
- ❑ Comprehensive print and scan audit trail
- ❑ Offer Common Criteria validated solutions



Market and End User Requirements

Curtail user misuse of MFP functions

■ The Requirement:

- ❑ Limit access to stored documents
- ❑ Prevent unauthorized transmission of documents using e-mail
- ❑ Prevent anonymous e-mail transmissions
- ❑ Prevent "Impersonated" e-mail transmissions
- ❑ Protect against easy access to duplicating documents in the output tray

■ The Threat:

- ❑ Open access to the device
- ❑ Unrestricted use for certain operations (Copy, Scan, Fax, Print, Color, Document management, USB memory devices)
- ❑ Inserting unauthorized scanned data into a workflow
- ❑ E-mail sensitive documents to unauthorized users

■ The Mitigation:

- ❑ Strong User and Administrator authentication
- ❑ Forced sender name and authentication for e-mail
- ❑ Password protect folder and documents
- ❑ Audit log for all MFP activities (scan, print, copy, fax, e-mail)
E-mail log file includes: from, to, when, what (file name and content)
- ❑ Confidential Print and Fax
- ❑ Document Control



Market and End User Requirements

Control over how the MFP is accessed via the Network/Fax

■ The Requirement:

- ❑ Protect against unauthorized 3rd party application control of the MFP
- ❑ Protect Login credentials
- ❑ Prevent tapping into a phone line to gain access to network
- ❑ Protect network information such as DHCP, WINS, SMTP server addresses
- ❑ Protect device setting and configuration by unauthorized users
- ❑ Prevent installation of rogue embedded firmware
- ❑ Protect device accounting/audit logs

■ The Threat:

- ❑ Unauthorized 3rd party application control of the MFP
- ❑ Sniffing network traffic to gain access to documents
- ❑ Sniffing network traffic to gain access to credentials
- ❑ Leveraging open ports/protocols to gain access or view clear text
- ❑ Bridging fax modem to Ethernet.

■ The Mitigation:

- ❑ Use of CAC user authentication
- ❑ Comprehensive Network Port/Protocol Management-Firewall
- ❑ SSL/TLS-Secure Socket Layers protocols with authorized digital certificate
- ❑ SNMPv3 for device maintenance support
- ❑ IPv6/IPSEC support
- ❑ SMB protocol for scanning
- ❑ IP/MAC address filtering
- ❑ Password protection for printing and faxing
- ❑ Logical and physical separation of Fax and Network boards
- ❑ Use of fax only (not data modem)

Market and End User Requirements

Protect against D.O.S - Denial of Service – attack

■ The Requirement:

- ❑ Prevent the MFP from being used as a gate to propagate attacks against the network, creating Denial of Service
- ❑ Prevent lock-up of the MFP, requiring the machine to be reset

■ The Threat:

- ❑ Through open access to the device
- ❑ Not providing an address filtering mechanism
- ❑ Use device credentials to access network resources
- ❑ Redirect “bogus” print jobs

■ Recommended Mitigation:

- ❑ Comprehensive Network Port/Protocol Management-Firewall
- ❑ SSL-Secure Socket Layers protocols with Digital Certificate
- ❑ SNMPv3 for device maintenance support
- ❑ 802.1x device authentication support
- ❑ SMB protocol for scanning IP/MAC address Filtering
- ❑ Password protection for printing and faxing
- ❑ Kerberos support for authentication
- ❑ Logical separation of Fax and Network functions
- ❑ Use of fax modem only (not data modem)
- ❑ Ignore junk Fax

Market and End User Requirements

Protection against common Windows[®] / Linux executable viruses and similar infectious programs.

■ Operating System Threats:

- ❑ Primary Source: MFP Network port/line/USB
- ❑ Secondary Source: MFP PSTN (Fax /data modem) port/line

■ Recommended Mitigation:

- ❑ Firmware based OS as opposed to software based OS (e.g. Windows / Linux).
 - ❖ Using embedded firmware that is not based on Windows / Linux or other soft operating system. Therefore, not subject to the same Virus vulnerability and malicious EXE files as

Sharp Multi-Layers of Security

FAX AND NETWORK SECURITY

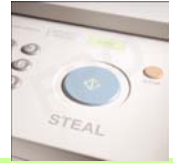
ACCESS CONTROL SECURITY

AUDIT TRAIL SECURITY

DOCUMENT SECURITY

DATA SECURITY





Sharp Multi-Layers of Security (MX Series)

Access Control Security

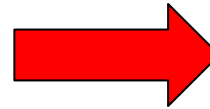
Access Control and Authentications



Usages and Restrictions for Scan, Print, Fax, Copy, Setting, D-F and E-mail, User Authentication, **Access Cards support (CAC-Common Access Card*, HID card*)**

Fax Security

Fax Protected Features



Logical separation between the fax telephone line and LAN.
Prevent Junk Fax and Secure Fax release

Data Security

Memory and Hard Drive protection



Data Security Kit* (optional):
256 bit AES data encryption and anti-copy
CC validation for Sharp Security Suite
Common Criteria

Network Security

Comprehensive Firewall



SSL-Encrypt Network Traffic, Digital Certificate, Port Management & Filtering, Antivirus and D.O.S Resistance
(No security patches required)

Audit Trail security

Auditing & Management



MFP Log for all MFP activities: (Scan, Print, Copy, Fax, E-mail, Setting)
Equitrac Office[®], Express - optional

Document Security

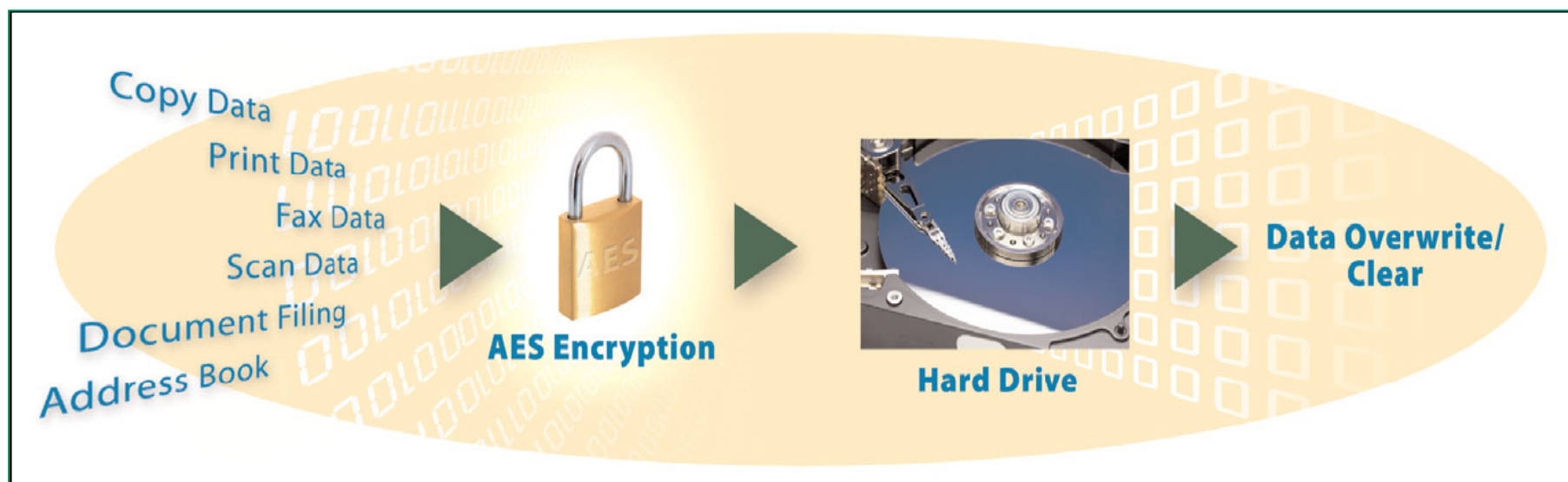
Document Encryption



Encrypted PDF files for scanning and printing, SSL & SMB protocols for scanning, printing, e-mail and setup.

* Optional

Data Security



Sharp's **Data Security Kits** enable highly-sensitive information to be securely printed, copied, scanned and faxed, minimizing your exposure to data theft from memory retention. The Data Security Kit first encrypts (AES 256 bit (FIPS 140-2)) the image data and then overwrites it (up to 7 times) after the job is complete. Today, Sharp has the only office equipment security solution with encryption and overwrite capability validated by the National Information Assurance Program's (NIAP) at EAL4.

Common Criteria (ISO15408) program which is sponsored by the National Security Agency (NSA) and NIST.

Common Criteria Validation

- **What is it?:** International standard for IT security validation. CC labs in Japan are validating Sharp MFPs against Sharp security claims.
- **Why Sharp needs it?:** It is a requirement by the USA & Canada governments and other enterprise companies.
- **CC validation** process takes one (1) year from start to finish.
- **Current Status:** All Sharp products from 23 ppm and up that have CC DSK or are in the validation process.

Common Criteria Validation Site

CCEVS Home | NIAP Home | About Us | Contact Us | Help | Site Map

CCEVS Big Picture

- Defining the CCEVS
- CCEVS Objectives
- Eval/Validation Primer
- CCEVS Validation Body
- Historical Perspective
- Guidance to Consumers
- CC Testing Labs (CCTL)
- Candidate CCTLs
- CCRA & Partners
- Acronyms & Terms
- Upcoming Events
- The OR/OD Process

CCEVS Products

- Validated Products List
- Validated Protection Profiles

Validated Products List (by Vendor)

View by: [Technology Type](#) | [Assurance Level](#) | [Product Name](#) | [Vendor](#)

The following products have been evaluated and validated in accordance with the provisions of the NIAP Common Criteria Evaluation and Validation Scheme. Products on this list have been evaluated and accredited at licensed/approved evaluation facilities in the U.S. for conformance to the Common Criteria for IT Security Evaluation (ISO Standard 15408). Products that have been evaluated and granted certificates (up through EAL4) under CCRA partnering schemes are recognized by the CCEVS; US Customers (accreditors, integrators, etc) may treat these mutually- recognized evaluation results as being equivalent. For the complete list of products which have received Common Criteria certifications, please visit the [Common Criteria Portal](#).

Common Criteria certificates issued for IT products apply only to the specific versions and releases of those products.

Certificates are not endorsements of the "goodness" of an IT product by NIST, NSA, or any other organization that recognizes or gives effect to the certificate. A certificate represents the successful completion of a validation that product met CC requirements for which it was issued.

Readers are advised to carefully read the Validation Report and Security Target of the product to determine what configuration.



For USA CC-Certification

For non-USA CC-Certification

Mutual Recognition Statement

The Common Criteria Portal is successfully up and running and in order to harmonize with other CC certifying nations, NIAP Staff is no longer posting certified products by other certifying nations. The Portal recognizes products that have been evaluated under the sponsorship of other signatories and in accordance with the International Common Criteria for Information Technology Security Evaluation Recognition Arrangement (CCRA) for EAL 1-4 only.

For a complete listing of products which have received Common Criteria certifications outside the U.S. please visit the [Common Criteria Portal](#).

Common Criteria Validation/MX Series

JISEC Japan IT Security Evaluation and Certification Scheme

Certificate

is awarded to

Sharp Corporation

Common Criteria Certification at EAL3+

Certification Number: C0227

Product Name: MX-FR11

Version: C.10

Type of IT Product: Data protection function in Multi Function Device

Evaluation Criteria:
- Common Criteria for Information Technology Security Evaluation Version 3.1 Revision 2 **

Evaluation Methodology:
- Common Methodology for Information Technology Security Evaluation Version 3.1 Revision 2 **

Assurance Level: EAL3

Protection Profile Conformance: None

**Name of CCTC: Information Technology Security Center
Evaluation Department**

Date of Certification: July 27, 2009

The IT product identified in this certificate has been evaluated at an approved evaluation facility established under the Japan IT Security Evaluation and Certification Scheme in accordance with the Common Methodology for Information Technology Security Evaluation Version 3.1 Revision 2, for conformance to the Common Criteria for Information Technology Security Evaluation Version 3.1 Revision 2. This certificate is issued to the specific version and release of the product in its evaluated configuration and in conjunction with the complete certification/validation report. This evaluation has been conducted in accordance with the provisions of the Japan IT Security Evaluation and Certification Scheme and the conclusions of the evaluation facility in the evaluation technical report are consistent with the evidence adduced. This certificate is not an endorsement of the IT product by the Information-technology Promotion Agency or by any other organization that recognizes or gives effect to this certificate, and no warranty of the IT product by the Information-technology Promotion Agency or by any other organization that recognizes or gives effect to this certificate, is either expressed or implied. The misuse of this certificate, including its use regarding the IT Product or system or PP of a version differing from that appearing in this certificate or the use of certificate for publications, such as advertisements and catalogs, in an incorrect or misleading manner may result in withdrawal of this certificate.

Original Signed
Koji Nishigaki
Chairman

Information-technology Promotion Agency, Japan

IPA

Date: August 17, 2009

IEEE Standard

- Security standard for Hard Copy Device (IEEE 2600[™]-2008).
- It is the first security standard requirements from 7/2008.
- **Markets that are effected by this standard:** Government, Enterprise and Corporate companies.
- Sharp is the first in the industry to meet the standard requirements.

P2600

Hardcopy Device and System Security

The Hardcopy Device and System Security Working Group is an approved standard project sponsored by the IEEE Information Assurance Standards Committee of the IEEE Computer Society.



**New
Security
Standard
from 2008**

3 **1. Overview**

4 **1.1 Scope**

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

12 **1.2 Purpose**

13 In today's Information Technology environment, significant time, and effort are being spent on security for
14 workstations and servers. However, today's hardcopy devices (printers, copiers, multifunction devices, etc.)
15 are connected to the same local area networks and contain many of the same communications, processing
16 and storage components, and are subject to many of the same security problems as workstations and
17 servers. At this time, there are no standards to guide manufacturers or users of hardcopy devices in the
18 secure installation, configuration, or usage of these devices and systems.

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

- 20
- 21 1) To provide guidance in the secure architecture, design, and out-of-box configuration of
22 hardcopy devices for manufacturers;
- 23 2) To provide guidance in the secure installation, configuration, and use of hardcopy devices
24 for end users and their supporting organizations; and,

CAC-Common Access Card/MX-EC50

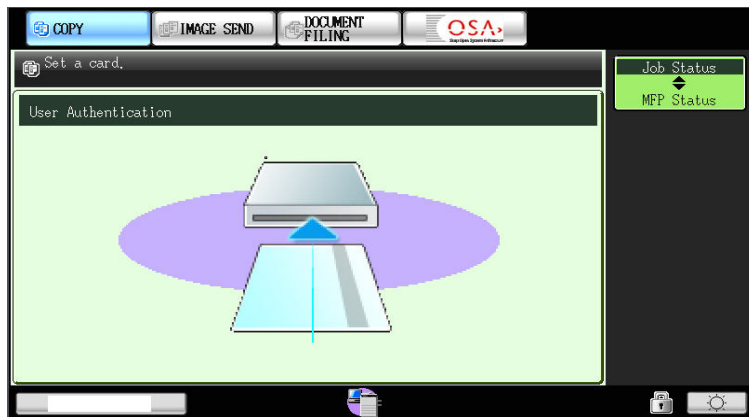


Main Features

- Comply to HSPD-12 specifications
- CAC and PIV cards support
- Authenticate CAC cardholder against user PIN
- Block all MFP Functions unless user authenticates
- Auto insertion of user's e-mail address
- Scan only to card user
- Supports group policy and/or user policy
- Secure Print-job release with use of CAC card
- LDAP SSL Authentication
- PKI/OCSP server Authentication
- Extract user certificate
- Digital Signature using user private key
- E-mail encryption using recipient public key

Background information

- The **Common Access Card (CAC)** was developed in response to **HSPD-12 Homeland Presidential Security Directive** and is used by the Department of Defense (DoD) and other federal departments as an identification for active-duty military personnel, reserve personnel, civilian employees, non-DoD other government employees, State Employees of the National Guard and eligible contractor personnel.
- The CAC is used as an identification card as well as for authentication to enable access to DoD computers, MFPs, networks and certain DoD facilities.
- The CAC card stores user e-mail address, credentials and user private key.



Supported MFP Models

MX-M283/M363/M453/M503 N Series (only)

MX-M623/M753 (Q2-2010)

MX-2600/3100

MX-4100/4101/5001

DX/MX-C311/C401

Multi-Function Device Purchase Criteria

The Classic Issues

- Cost of Ownership
- Contracts
- Reliability
- Features
- Maintenance
- Brand
- Physical Size
- Applications
- Output Quality
- Speed

Today's New Issues

- Security
- Print and Copy Specific Security
- Risk Management
- Scan Specific Security and Authentication
- Privacy Law Compliance
- IEEE P2600 security standard
- Common Criteria Certification (EAL)
- Reports on NIST Vulnerability Database
- IPv6, SNMPv3, Windows Vista[®] compatibility...
- Access Control - Common Access Card
- Insider Abuse Controls and Audit Features
- Network Security
- Communications Security

Look for a new generation of Security and IT Awards presented To MFP manufacturers.



BLI Award
The best IT friendly



BLI Award
Outstanding MFP Security
Solution



BERTL's 2007 Award
Best Security Solution Suite

Data Security Kits for MFPs – Not all are alike!

- Multiple overwrites of data in magnetic memory (hard drives) up to seven (7) times vs. just clearing a directory or overwriting one to three times.
- Use of encryption to protect buffered data so that if overwrites do not execute, data is protected. Failure to execute usually requires service access.
- Use of encryption for print mailboxes and stored documents.
- Auto lockout after three failed password attempts for Admin, document file retrieval, encrypted PDFs Just like your computer.
- Document copy and scan control to disable reproduction of sensitive documents (print control pattern for color systems) ... refuses to copy / scan.
- Option to force Print and Fax hold operations - Policy
- Restricted access to Address lists and configuration data - not just docs.
- Certification - Common Criteria - At What EAL?- Does it work as advertised?

Sharp Security Suite Awards

Most comprehensive security offering in the market



We're "IT Friendly" with easy integration and lower support costs



Why Sharp Delivers the Best Value to their Customers?

Benefits of the Sharp Solution

- **Sharp's leadership in Data Security** helps ensure against identity theft, cyber attacks and network threats.
- **Sharp's experience in gaining Common Criteria Certification** will assist in ensuring that the process be successful and take the minimal amount of time.
- **The certified EAL3+ Data Security Kit (DSK)** delivers powerful protection
- **Common Access Card (CAC) solution** will make access easier for those users with assigned rights on the equipment.
- **The proven high reliability of Sharp equipment**, combined with the service team's responsiveness, ensures optimal uptime.
- **Sharp offers the latest in technology** at a very competitive total cost of operation.

Sharp's Security Information on SharpUSA/SharpSPC

Security



The Sharp multi-layer approach to securing documents and data protects your assets from vulnerability.

[Learn More >](#)

An MFP is a powerful asset in your office's environment. Left unsecured however, an organization. Just consider the types of documents that are copied, printed, faxed or statements, confidential reports, e-mails, memos, customer data, and employee information.

Intellectual property, private and personal information becomes portable once processed from both internal and external threats. While not all risks to confidential information are from inadequate protection can be only a matter of time.

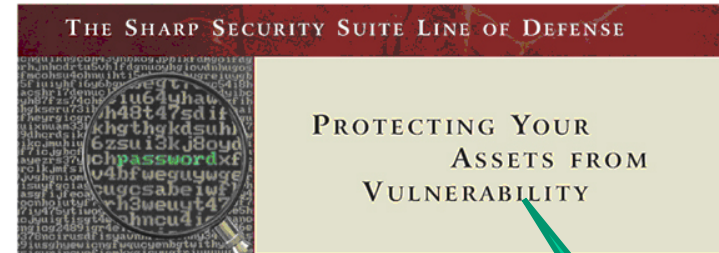
Common Vulnerabilities

Some of the most common vulnerabilities associated with an unsecured MFP include:

- Loss of productivity
- Regulatory non-compliance
- Loss of access
- Stolen information
- Lawsuits
- Unauthorized use

Sharp offers the following Security products, tools and applications:

- [Sharp Security Suite](#)
- [Sharp Data Security Kit \(DSK\)](#)
- [Sharp Secure Network Interface](#)
- [Sharp Security Library](#)



Sharp Security Suite

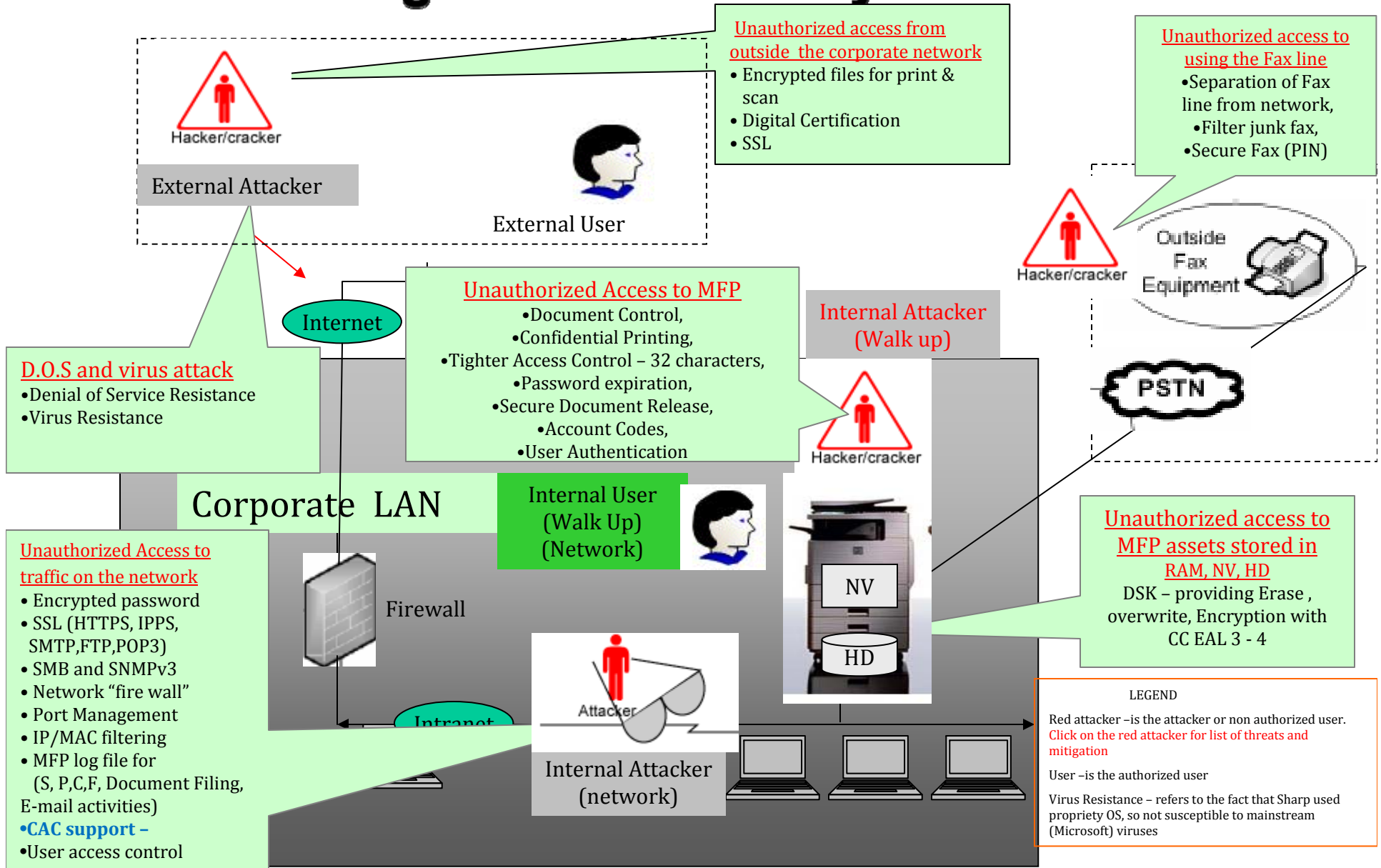
As an industry leader in document security, Sharp® Electronics recommends that businesses take a multi-layer approach to securing their documents and data. This has never been more important as the proliferation of e-mail and the Internet has made it need to monitor and safeguard document workflow a top priority.

SHARP USA

SHARP SPC

Security in Details

Mitigations to Security Threats



Data Security cont.

◆ DSK for the MX Series

- ❑ **Commercial DSK with enhanced access control:**
 - ❑ Document / Copy control: Printing control pattern to disable duplication of sensitive documents. (only MX series with DSK)
 - ❑ Restrictions on printing Sender Address List and all other configurations
 - ❑ Option to Force Print and Fax Hold option
 - ❑ Admin password protection :
(lock admin or document filing user after 3 tries)
 - ❑ Document filing password protection (lock document filing after 3 tries)
 - ❑ Encrypted PDF file password protection (lock document after 3 tries)
 - ❑ FTP setup authentication
- ❑ **Benefits:** Support Security and Government accounts that require Data Security and Data Encryption

Enhanced Access Control

■ Enhanced Access Control :

- ❑ Full password and user name (32 alphanumeric characters) for all MFP activities (Scan, Print, Fax, Copy, Document filing and USB activities)
- ❑ Log file for all MFP activities (Scan, Print, Copy, Fax, E-mail, Document filing)
- ❑ Document Filing enhanced access control and restrictions
- ❑ Scanning restrictions (HDD, USB and other)
- ❑ Restriction on Firmware update (USB or PAU)
- ❑ Support of Common Access Card (Smart Card) with MX-EC50 or DCL310S (optional)

*Select the function

Authority Group Registration

No.03 ABC Group

Select a function setting up authority.

<input type="button" value="Copy"/>	<input type="button" value="Printer"/>
<input type="button" value="Image Send"/>	<input type="button" value="Document Filing"/>
<input type="button" value="Common Functions"/>	<input type="button" value="System Settings"/>

O-Kay!



Authority Group Registration / Image Send

No.03 ABC Group

Approval Settings for Each Mode

Set up the transmission to be approved.

<input checked="" type="checkbox"/> E-mail	<input checked="" type="checkbox"/> FTP	1/2
<input checked="" type="checkbox"/> Desktop	<input checked="" type="checkbox"/> Network Folder	↑
<input checked="" type="checkbox"/> USB Memory	<input checked="" type="checkbox"/> PC Scan	↓

Authority Group Registration / Image Send

No.03 ABC Group

Approval Settings for Each Mode

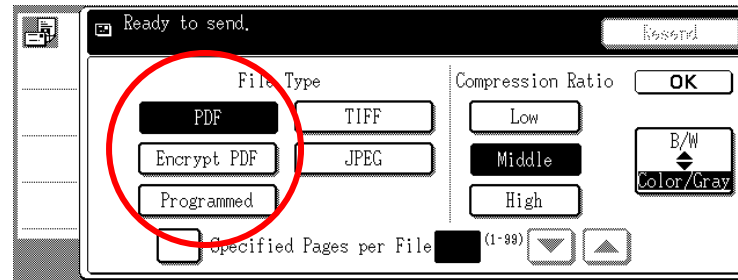
Set up the transmission to be approved.

<input checked="" type="checkbox"/> Internet Fax	<input checked="" type="checkbox"/> PC-I-Fax	1/2
<input checked="" type="checkbox"/> Fax	<input checked="" type="checkbox"/> PC-Fax	↑
		↓

Scanning Security

■ Scan and E-mail Security:

- ❑ Scan encrypted PDF file
 - ❑ Securely Scan encrypted and password protected file directly from the MFP without the need for other software or products.



- ❑ Log file for all e-mail activities (From, To, When, What (file content))
- ❑ Access Control and restrictions on Scan to USB memory
- ❑ Support SMB, FTPS, SMTPS, POP3S protocols for enhanced scanning security
- ❑ Secure scan to FTP sites using FTPS tunnel with Sharpdesk® 3.2X
- ❑ Support of Common Access Card (Smart Card) with MX-EC50 and DCL310S (Optional)
- ❑ Support of a variety of Access Cards (Proximity, RF, Biometric, Smart Card) (Optional)

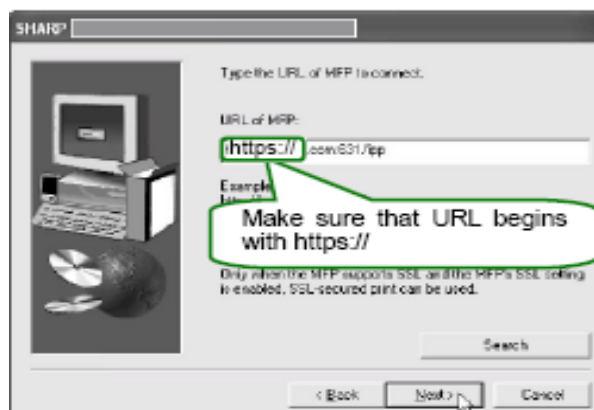
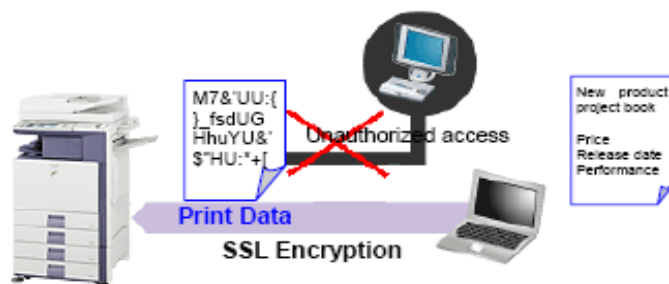
Printing Security

■ Printing Security

- ❑ Print encrypted and password protected PDF file
- ❑ Securely Print Directly from:
 - ❑ Printer Driver
 - ❑ FTP Pull Print
 - ❑ E-Mail Push print
- ❑ Direct print from Job status
- ❑ Print using IPPS protocol.

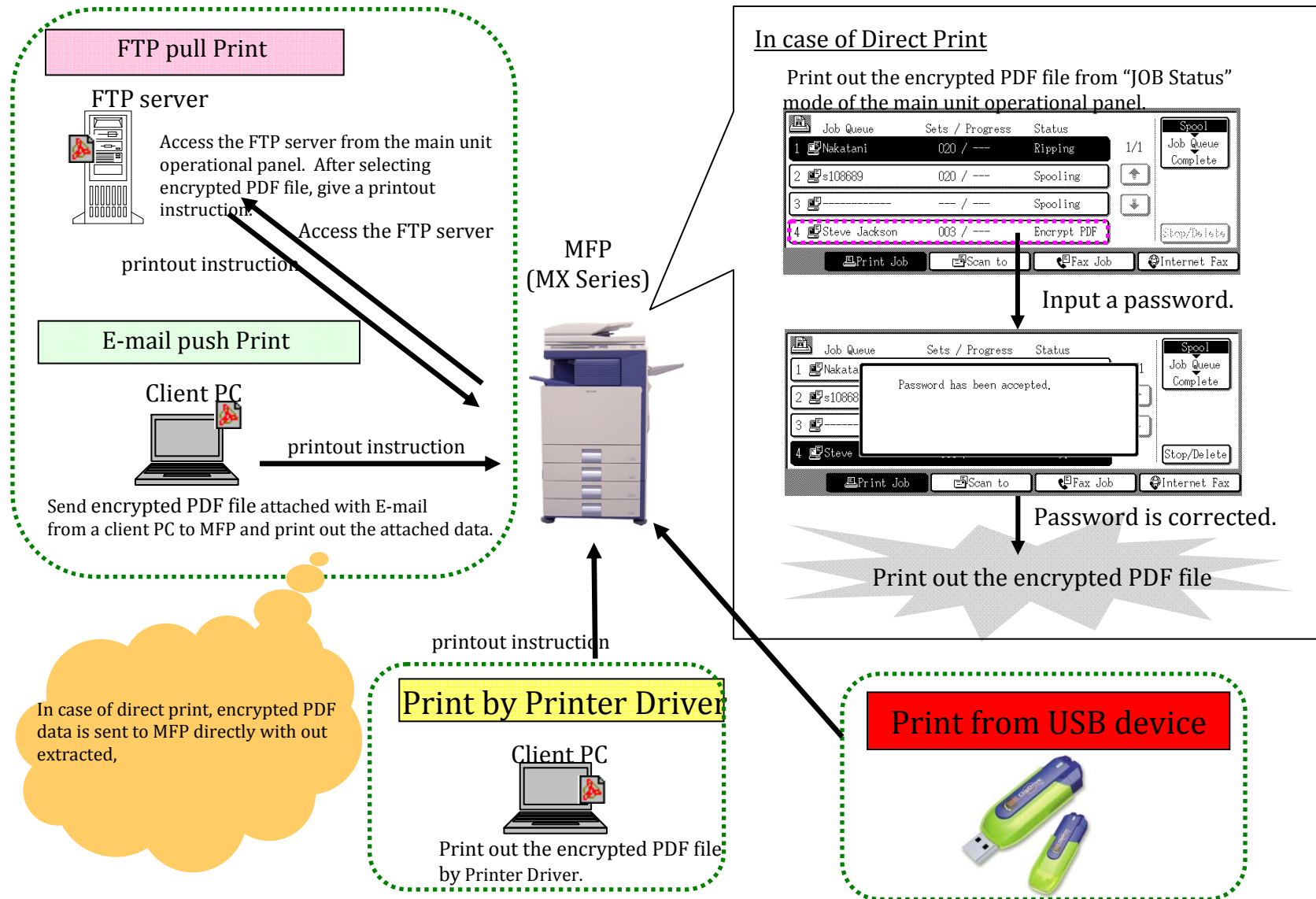
Chapter 1: SSL Encryption of Print Data

Page 2-Page 5



Printing Security—Cont.

Method for encrypted PDF file printing



Fax Security

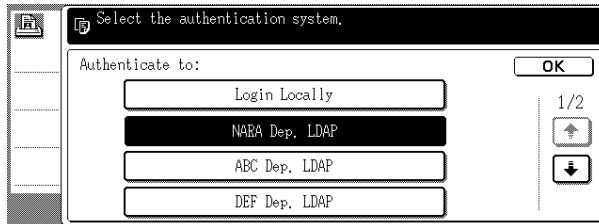
- Fax Security
 - ❑ Confidential Fax printing (password protected)
 - ❑ Ignore Junk Fax
 - ❑ Separation of Fax from Network
 - ❑ Optional log in to send a fax

Network Security

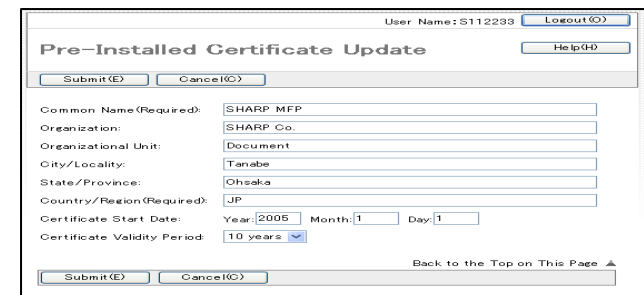
■ Network Security:

- ❑ SNMP-v3 for Device Maintenance support
- ❑ SMB support for Scanning (MX series)
- ❑ 802.1X for Device authentication (similar to the wireless)
- ❑ User Authentication from a selection list
(Company LDAP or Company Server or any other)

*"Authenticate to" select Screen

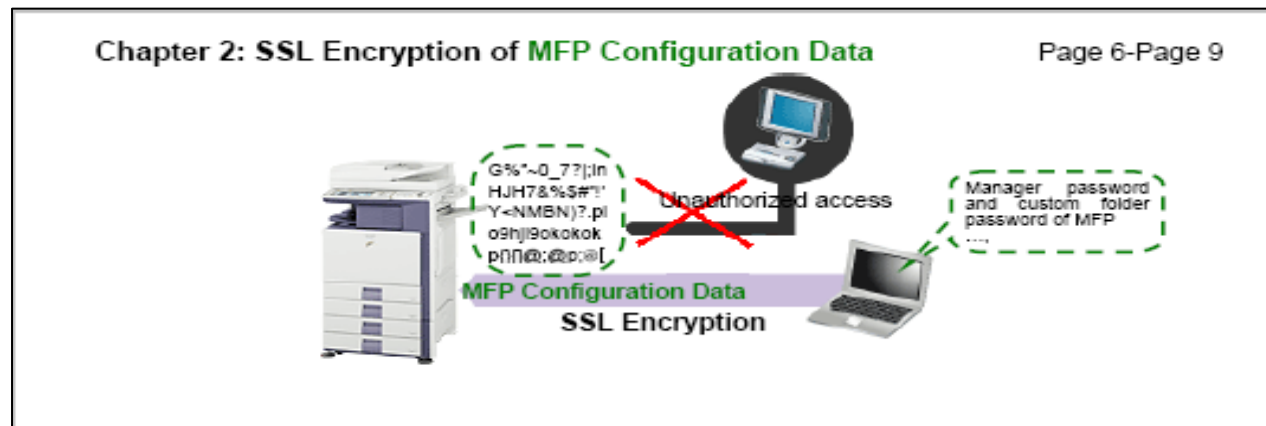


O-Kay!



Network Security cont.- (SSL)

- Secure Socket layer (SSL) support (MX series CR2 and B&W3) for:
 - ❑ IPP (IPPS): encrypt the printing for out of network users
 - ❑ SMTP (SMTPS) for outgoing e-mail
 - ❑ POP3 (POP3S) for incoming e-mail
 - ❑ LDAP (LDAPS) for LDAP authentication
 - ❑ FTP (FTPS) for scanning to FTP site
 - ❑ HTTP (HTTPS): encrypts the network traffic to secure Imager Home Page activities (Security and network setting and configuration)
 - ❑ Digital Signature Certificate for SSL (Local or import from external security authority (e.g. VeriSign®, RSA® or other)
 - ❑ Example: HTTPS



Network Security- Cont. (Port Control)

SHARP MX-2700N	User Name: Administrator <input type="button" value="Logout"/>	
	<input type="button" value="Help"/>	
Port Control		
<input type="button" value="Submit(U)"/> <input type="button" value="Update(R)"/>		
Server Port		
<input type="checkbox"/> Top Page	HTTP:	<input type="button" value="Enable"/> Port Number: <input type="text" value="80"/> (0-65535)
<input checked="" type="checkbox"/> Status	HTTPS:	<input type="button" value="Disable"/> Port Number: <input type="text" value="443"/> (0-65535)
<input checked="" type="checkbox"/> Address Book	FTP Print:	<input type="button" value="Enable"/> Port Number: <input type="text" value="21"/> (0-65535)
<input checked="" type="checkbox"/> Document Operations	Raw Print:	<input type="button" value="Enable"/> Port Number: <input type="text" value="9100"/> (0-65535)
<input checked="" type="checkbox"/> Job Programs	LPD:	<input type="button" value="Enable"/> Port Number: <input type="text" value="515"/> (0-65535)
<input checked="" type="checkbox"/> User Control	IPP:	<input type="button" value="Enable"/> Port Number: <input type="text" value="631"/> (0-65535)
<input checked="" type="checkbox"/> System Settings	IPP-SSL:	<input type="button" value="Disable"/> Port Number: <input type="text" value="443"/> (0-65535)
<input checked="" type="checkbox"/> Network Settings	Tandem Copy Receive:	<input type="button" value="Enable"/> Port Number: <input type="text" value="50001"/> (0-65535)
<input checked="" type="checkbox"/> Application Settings	PC Scan:	<input type="button" value="Enable"/> Port Number: <input type="text" value="52000"/> (0-65535)
<input checked="" type="checkbox"/> E-mail Alert and Status	SNMPD:	<input type="button" value="Enable"/>
<input type="checkbox"/> Storage Backup	Telnet:	<input type="button" value="Enable"/>
<input checked="" type="checkbox"/> Job Log	NBT/WINS:	<input type="button" value="Disable"/>
<input checked="" type="checkbox"/> Security Settings	JCP:	<input type="button" value="Disable"/>
<input type="checkbox"/> Password Change	RARP:	<input type="button" value="Enable"/>
<input type="checkbox"/> Port Control	SMTP:	<input type="button" value="Enable"/>
<input type="checkbox"/> Filter Setting	BMLinks:	<input type="button" value="Enable"/>
<input checked="" type="checkbox"/> SSL Settings		
<input type="checkbox"/> Custom Links		

Network Security- Cont. (Port Control)

SHARP
MX-2700N

User Name: Administrator [Logout\(\)](#) [Help](#)

Services Settings

[Update\(R\)](#)

WINS	SMTP	SNMP	
Kerberos	SNTP	mDNS	DNS

[Submit\(U\)](#)

DNS Settings

Primary Server:

Secondary Server:

Timeout: seconds(0-60)

Domain Name: (Up to 64 characters)

[Submit\(U\)](#)

[Update\(R\)](#)

[Back to the Top on This Page](#)

- Top Page
- Status
- Address Book
- Document Operations
- Job Programs
- User Control
- System Settings
- Network Settings
 - Quick Settings
 - General Settings
 - Protocol Settings
 - Services Settings
 - Print Port Settings
 - LDAP Settings
 - HTTP Access Settings
 - View Login User
- Application Settings

Network Security - Cont. (Port Filtering)

- ▢ Top Page
- Status
- Address Book
- Document Operations
- Job Programs
- User Control
- System Settings
- Network Settings
- Application Settings
- E-mail Alert and Status
- ▢ Storage Backup
- Job Log
- ▾ Security Settings
 - ▢ Password Change
 - ▢ Port Control
 - ▢ Filter Setting
 - SSL Settings
- ▢ Custom Links
- ▢ Operation Manual Download

Filter: Disable ▾

IP Address Filter Settings

Filter Mode: Allow ▾

	Start IP Address	End IP Address
Filter Address 1	<input type="text" value="0.0.0.0"/>	<input type="text" value="0.0.0.0"/>
Filter Address 2	<input type="text" value="0.0.0.0"/>	<input type="text" value="0.0.0.0"/>
Filter Address 3	<input type="text" value="0.0.0.0"/>	<input type="text" value="0.0.0.0"/>
Filter Address 4	<input type="text" value="0.0.0.0"/>	<input type="text" value="0.0.0.0"/>

MAC Address Filter Settings

	MAC Address
Filter Address 1	<input type="text" value="000000000000"/>
Filter Address 2	<input type="text" value="000000000000"/>
Filter Address 3	<input type="text" value="000000000000"/>
Filter Address 4	<input type="text" value="000000000000"/>
Filter Address 5	<input type="text" value="000000000000"/>
Filter Address 6	<input type="text" value="000000000000"/>
Filter Address 7	<input type="text" value="000000000000"/>
Filter Address 8	<input type="text" value="000000000000"/>
Filter Address 9	<input type="text" value="000000000000"/>
Filter Address 10	<input type="text" value="000000000000"/>

Audit Log Security

MFP Job Log Sample Report for Activities (MX Color and Hercules)

Top Page										
Status										
Address Book										
Document Operations										
Job Programs										
User Control										
System Settings										
Network Settings										
Application Settings										
E-mail Alert and Status										
Storage Backup										
Job Log										
Save/ Delete Job log										
View Job Log										
Security Settings										
Custom Links										
Operation Manual Download										
Job Log:		206								
Display Items:		500								
		Sorting in Descending Order								
Previous(M)		1 / 1							Next(N)	
Job ID	Job Mode	Computer Name	User Name	Login Name	Date		Total Count			
					Start	Complete	Black & White	Full Color	2 Color	
206	Scan to Desktop	N/A	No Authentication	No Authentication	2006-02-17T10:00	2006-02-17T10:00	1	0	N/A	
205	Scan to E-mail	N/A	No Authentication	No Authentication	2006-02-17T09:57	2006-02-17T09:57	1	0	N/A	
204	Scan to Desktop	N/A	No Authentication	No Authentication	2006-02-17T09:56	2006-02-17T09:56	1	0	N/A	
203	Scan to E-mail	N/A	No Authentication	No Authentication	2006-02-17T08:31	2006-02-17T08:32	22	0	N/A	
202	Scan to E-mail	N/A	No Authentication	No Authentication	2006-02-17T08:28	2006-02-17T08:28	0	0	N/A	
201	Metadata Send(Desktop)	N/A	No Authentication	No Authentication	2006-02-16T14:42	2006-02-16T14:42	0	1	N/A	
200	Metadata Send(Desktop)	N/A	No Authentication	No Authentication	2006-02-16T14:38	2006-02-16T14:39	0	1	N/A	

SSL Settings

C-Frontier, MX Series-II and B&W III

<ul style="list-style-type: none"> ▢ Top Page ▸ Status ▸ Address Book ▸ Document Operations ▸ Job Programs ▸ User Control ▸ System Settings ▸ Network Settings ▸ Application Settings ▸ E-mail Alert and Status ▢ Storage Backup ▢ Device Cloning ▸ Job Log ▾ Security Settings <ul style="list-style-type: none"> ▢ Password Change ▢ Port Control ▢ Filter Setting ▾ SSL Settings <ul style="list-style-type: none"> ▢ Certificate Creation ▢ Make of Certificate 	<div style="border: 1px solid gray; background-color: #f0f0f0; padding: 2px; margin-bottom: 5px;"> Setting of SSL </div> <p>Server Port:</p> <p>HTTPS: Disable ▾</p> <p>IPP-SSL: Disable ▾</p> <p><input checked="" type="checkbox"/> Redirect HTTP to HTTPS in Device Web</p> <p>Page Access</p> <p>Client Port:</p> <p>HTTPS: Enable ▾</p> <p>FTPS: Enable ▾</p> <p>SMTP-SSL: Enable ▾</p> <p>POP3-SSL: Enable ▾</p> <p>LDAP-SSL: Enable ▾</p> <hr/> <p>Level of Encryption: Low ▾</p> <p>Notice: Web page may not be displayed if Level of Encryption is set to High on SSL Settings depending on the function of the browser or the connection status. To display the Web page, disable the SSL settings in the System Settings on the operation panel, and then set Level of Encryption to Low or Middle.</p> <div style="border: 1px solid gray; background-color: #f0f0f0; padding: 2px; margin-top: 10px;"> Certificate Information </div>
---	--

Sharp Multi-Layered Security Summary



Sharp MFP Security Levels

SHARP MFP SECURITY LEVELS 
HOW SECURE DO YOU NEED TO BE?

Standard Level

Who should use it?

- General office
- SOHO
- Public offices

Benefits

- Confirm user access
- Protect user output
- Adds resistance to attack from malicious codes and viruses

Applications

- Access Control Security (accounts codes, PIN printing)
- Network Security (IP/Mac Filtering, Port/Protocol Management)

Heightened Level
(Includes Standard Level)

Who should use it?

- Enterprise companies
- Human Resources
- Financial
- Accounting
- Healthcare
- Insurance
- Legal
- Education

Benefits

- Virtually eliminates latent document images
- Helps protect stored documents
- Access control authentication
- Helps protect documents in transit
- Audit user activity

Applications

- Data Security Kit (DSK)
- Access Control Security (LDAP and active directory authentication)
- Document Security (document encryption)
- Network Security (data and traffic encryption)
- Audit Trail Security (internal and third party log file)

Optimum Level
(Includes Heightened Level)

Who should use it?

- Federal agencies, DOD, state offices
- Research & Development

Benefits

- Helps protect from attackers on fax lines
- Provides assurance claims
- Better user access control authentication

Applications

- Common Criteria Validation (CC DSK)
- Fax security (separation between fax and network lines)
- * ~~DL310S Cryptek CAC Solution~~ (Digital Certificate)

	AR- M257/M277 AR-M267 AR-M317	AR- M366 N/M466N MX- M360 U/M460U MX- M360 N/M460N	MX- M560 A/30700 MX- M560 B/30700 Barcode	MX- M463/M503 MX- M360/M360 M4100 Barcode	MX- 2600N/S 100N MX-CS 11/C401 MX-4100/5001	MX-360 1N/460 1N MX- 6600N/8200 N/F000 N MX-820 1N/700 1N
DSK-Data Security Kit (Optional)						
Function	Copy/Print / Scan/Fax	Copy/Print/ Scan/Fax	Copy/Print/ Scan/Fax	Copy/Print/ Scan/Fax	Copy/Print/ Scan/Fax	Copy/Print/ Scan/Fax
Commercial DSK	AR- FR12U AR- FR24U AR- FR25U	AR- FR22U AR- FR21U MX- FR07U MX- FR09U	AR- FR11U MX- FR5U	MX- FR14U/ MX- FR15U MX- FR28U	MX- FR10U MX- FR13U MX- FR11U	MX- FR01U MX- FR02U MX- FR03U MX- FR05U
Common Criteria DSK	AR- FR12M AR- FR24 AR- FR25	AR- FR22 AR- FR21 MX- FR07 MX- FR09	AR- FR11 MX- FR05	MX- FR14Y MX- FR15Y MX- FR08	MX- FR10 MX- FR13 MX- FR11	MX- FR01 MX- FR02 MX- FR03 MX- FR05
Anti-Copy	No	No	No	Yes	Yes	Yes
Encryption	128 A,EE	128 A,EE	128 A,EE	256/128 A,EE	256 A,EE	128 A,EE
Overwrite Ram & HD	Yes	Yes	Yes	Yes	Yes	Yes
Address book Overwrite	Yes	Yes	Yes	Yes	Yes	Yes
Document Ring Encryption	Not Applicable	Yes	Yes	Yes	Yes	Yes
EAL validation level	EAL3+	EAL3+	EAL3	EAL3	EAL3	EAL3+
Security Features (Standard)						
Confidential Print	Yes	Yes	Yes	Yes	Yes	Yes
Confidential Fax	No	No	No	Yes	Yes	Yes
Encrypted PDF file , BMP&G	No	No	No	Yes	Yes	Yes
Portmanagement BBI TM , BMB SM	Yes	Yes	Yes	Yes	Yes	Yes
Meet IEEE2600™/2003 standard	No	No	No	Yes**	Yes	No
Controller without hard drive	Yes	For U version	No	No	No	No
** Only for MX-M283/M363/M453/M503 Access Control	Access control DC LIDS (CAC)	Access control DC LIDS (CAC)	Access control DC LIDS (CAC)	Access control DC LIDS MX-BC50** (CAC)	Access control DC LIDS MX-BC50 (CAC)	Access control DC LIDS (CAC)
Document Ring Record	Not Applicable	Yes	Yes	Yes	Yes	Yes

* 2010 ** Only for MX-M283/M363/M453/M503

*** only for MX and AR-M257/M317

Sharp Security Suite Competitive Comparison



**Researcher discloses serious Xerox
flaw**

**Security flaw in Work Center multifunction
printers allows access to information being
printed on the machines**

Sharp's Security Suite—The Best

CC EAL # DSK solutions - CC EAL vs. How strong is the Security solution?

3+		SHARP
3		
2		
	1 2 3 4 5	6 7 8 9 10
	Weak Security Solutions	Strong Security solutions

SHARP

National Vulnerability Database

<http://nvd.nist.gov/>

No Issues Reported

Sharp's Firmware Based architecture is more secure.
It is not subject to virus attacks, worms and other attacks that exploit the MFP's ability to run executable files.

NATIONAL VULNERABILITY DATA BASE

<http://nvd.nist.gov/>

The screenshot shows the NVD website with a search bar containing 'Xerox' and various navigation links. The page is sponsored by DHS National Cyber Security Division/US-CERT and NIST. It includes a 'Welcome to NVD!!' section, a search interface, and a 'Resource Status' sidebar.

Welcome to NVD!!
NVD is a comprehensive cyber security vulnerability database that integrates all publicly available U.S. Government vulnerability resources and provides references to industry resources. It is based on and synchronized with the [CVE](#) vulnerability naming standard.

Resource Status
NVD contains:
20129 CVE Vulnerabilities
72 US-CERT [Alerts](#)
1523 US-CERT [Vuln Notes](#)
1162 [Oval](#) Queries
Last updated:
10/25/06
Publication rate:

Search CVE Vulnerability Database (Perform Advanced Search)
Keyword search:
Try a product or vendor name
Try a [CVE](#) standard vulnerability name or [OVAL](#) query
Only vulnerabilities that match ALL keywords will be returned
Linux kernel vulnerabilities are categorized separately from vulnerabilities in specific Linux distributions

Show only vulnerabilities that have the following associated resources:
 [US-CERT Technical Alerts](#)
 [US-CERT Vulnerability Notes](#)
 [OVAL](#) Queries

Automated FISMA and Compliance Metrics (NSA/DISA/NIST Beta Site)!!
The [Security Content Automation Program](#) (SCAP) is a public free repository of security content to be used for automating technical control compliance activities (e.g. FISMA/800-53), vulnerability checking (both application misconfigurations and software flaws), and security measurement.

New CVE Community Service!!
NVD announces a [new service](#) to allow software development organizations to make official statements regarding the set of [CVE](#) vulnerabilities that apply to their products. They can now provide the CVE community (300+ products and services) deeper insight into the vulnerabilities within their products. For example, they can dispute third party vulnerability information, clarify vulnerability applicability, provide configuration and remediation guidance, provide deeper vulnerability analysis, and explain vulnerability

Xerox Vulnerabilities

<p>Resource Status</p> <p>NVD contains: 33991 CVE Vulnerabilities 143 Checklists 158 US-CERT Alerts 2283 US-CERT Vuln Notes 2097 OVAL Queries 16322 CPE Names</p> <p>Last updated: Mon Dec 08 11:47:33 EST 2008 CVE Publication rate: 13.17</p>	<p><u>CVE-2008-3571</u></p>
<p>Email List</p> <p>NVD provides four mailing lists to the public. For information and subscription instructions please visit NVD Mailing Lists</p>	<p>Summary: The Xerox Phaser 8400 allows remote attackers to cause a denial of service (reboot) via an empty UDP packet to port 1900. Published: 08/10/2008 CVSS Severity: <u>7.8</u> (HIGH)</p>
<p>Workload Index</p> <p>Vulnerability Workload Index: 8.24</p>	<p><u>CVE-2008-3121</u></p> <p>Summary: Multiple cross-site scripting (XSS) vulnerabilities in Xerox CentreWare Web (CWW) before 4.6.46 allow remote authenticated users to inject arbitrary web script or HTML via unspecified vectors. Published: 07/10/2008 CVSS Severity: <u>4.3</u> (MEDIUM)</p>
<p>About Us</p> <p>NVD is a product of the NIST Computer Security Division and is sponsored</p>	<p><u>CVE-2008-3122</u></p> <p>Summary: Multiple SQL injection vulnerabilities in Xerox CentreWare Web (CWW) before 4.6.46 allow remote authenticated users to execute arbitrary SQL commands via the unspecified vectors. Published: 07/10/2008 CVSS Severity: <u>6.5</u> (MEDIUM)</p>
	<p><u>CVE-2008-2824</u></p> <p>Summary: Unspecified vulnerability in the Extensible Interface Platform in Web Services in Xerox WorkCentre 7655, 7665, and 7675 allows remote attackers to make configuration changes via unknown vectors. Published: 06/23/2008 CVSS Severity: <u>10.0</u> (HIGH)</p>
	<p><u>CVE-2008-2825</u></p> <p>Summary: Cross-site scripting (XSS) vulnerability in the embedded Web Server in Xerox WorkCentre M123, M128, and 133 and WorkCentre Pro 123, 128, and 133 allows remote attackers to inject arbitrary web script or HTML via unspecified vectors. Published: 06/23/2008</p>

Xerox Vulnerability

- Xerox Security Bulletin XRX09-001
 - **Software update to address Command Injection Vulnerability**
 - v1.0
 - 01/30/09
- **Background**
 - A command injection vulnerability exists in the Web Server. If exploited, the vulnerability could allow remote attackers to execute arbitrary code via carefully crafted input on the affected web page. Customer and user passwords are not exposed.

Canon Vulnerabilities


<p>NVD contains:</p> <ul style="list-style-type: none"> 33991 CVE Vulnerabilities 143 Checklists 158 US-CERT Alerts 2283 US-CERT Vuln Notes 2097 OVAL Queries 16322 CPE Names <p>Last updated: Mon Dec 08 11:47:33 EST 2008</p> <p>CVE Publication rate: 13.17</p>	<p><u>CVE-2008-4279</u></p> <p>Summary: The CPU hardware emulation for 64-bit guest operating systems in VMware Workstation 6.0.x before 6.0 build 109488 and 5.x before 5.5.8 build 108000; Player 2.0.x before 2.0.5 build 109488 and 1.x before 1.0.8; Server 1 before 1.0.7 build 108231; and ESX 2.5.4 through 3.5 allows authenticated guest OS users to gain additional guest O privileges by triggering an exception that causes the virtual CPU to perform an indirect jump to a non-canonical address.</p> <p>Published: 10/06/2008</p> <p>CVSS Severity: <u>6.8</u> (MEDIUM)</p>
<p>Email List</p> <p>NVD provides four mailing lists to the public. For information and subscription instructions please visit NVD Mailing Lists</p>	<p><u>CVE-2008-2803</u></p> <p>Summary: The mozIJSSubScriptLoader.LoadScript function in Mozilla Firefox before 2.0.0.15, Thunderbird 2.0.0.14 a earlier, and SeaMonkey before 1.1.10 does not apply XPCNativeWrappers to scripts loaded from (1) file: URIs, (2) data URIs, or (3) certain non-canonical chrome: URIs, which allows remote attackers to execute arbitrary code via vector involving third-party add-ons.</p> <p>Published: 07/07/2008</p> <p>CVSS Severity: <u>6.8</u> (MEDIUM)</p>
<p>Workload Index</p> <p>Vulnerability Workload Index: 8.24</p>	<p><u>CVE-2008-2665</u></p> <p>Summary: Directory traversal vulnerability in the posix_access function in PHP 5.2.6 and earlier allows remote attacker to bypass safe_mode restrictions via a .. (dot dot) in an http URL, which results in the URL being canonicalized to a filename after the safe_mode check has successfully run.</p> <p>Published: 06/20/2008</p> <p>CVSS Severity: <u>5.0</u> (MEDIUM)</p>
<p>About Us</p> <p>NVD is a product of the NIST Computer Security Division and is sponsored by the Department of Homeland Security's</p>	<p><u>CVE-2008-0303</u></p> <p>VU#568073</p> <p>Summary: The FTP print feature in multiple Canon printers, including imageRUNNER and imagePRESS, allow remote attackers to use the server as an inadvertent proxy via a modified PORT command, aka FTP bounce.</p> <p>Published: 02/29/2008</p> <p>CVSS Severity: <u>6.4</u> (MEDIUM)</p>

Canon Security Patches

Security Bulletins for Canon Office Products

Security Bulletin	Canon Security Bulletin Response	Date Posted	Date Modified
<u>CVE-2000-0303</u>	<u>Vulnerability affecting FTP functions in Canon Controllers</u>	02/28/08	
<u>KB931836</u>	<u>iPR Server/CP GX-100 Patch corresponding with KB931836</u>	02/28/08	
<u>KB918338</u>	<u>iPR Server/CP GX-100 Patch corresponding with KB918338</u>	02/28/08	
<u>MS07-069</u>	<u>iPR Server/CP GX-100 Patch corresponding with MS07-069</u>	02/28/08	
<u>MS07-065</u>	<u>iPR Server/CP GX-100 Patch corresponding with MS07-065</u>	02/28/08	
<u>MS07-064</u>	<u>iPR Server/CP GX-100 Patch corresponding with MS07-064</u>	02/28/08	
<u>MS07-061</u>	<u>iPR Server/CP GX-100 Patch corresponding with MS07-061</u>	02/28/08	
<u>MS07-058</u>	<u>iPR Server/CP GX-100 Patch corresponding with MS07-058</u>	02/28/08	
<u>MS07-050</u>	<u>iPR Server/CP GX-100 Patch corresponding with MS07-050</u>	02/28/08	
<u>MS07-046</u>	<u>iPR Server/CP GX-100 Patch corresponding with MS07-046</u>	02/28/08	
<u>MS07-043</u>	<u>iPR Server/CP GX-100 Patch corresponding with MS07-043</u>	02/28/08	
<u>MS07-042</u>	<u>iPR Server/CP GX-100 Patch corresponding with MS07-042</u>	02/28/08	
<u>MS07-035</u>	<u>iPR Server/CP GX-100 Patch corresponding with MS07-035</u>	02/28/08	
<u>MS07-031</u>	<u>iPR Server/CP GX-100 Patch corresponding with MS07-031</u>	02/28/08	
<u>MS07-022</u>	<u>iPR Server/CP GX-100 Patch corresponding with MS07-022</u>	02/28/08	
<u>MS07-021</u>	<u>iPR Server/CP GX-100 Patch corresponding with MS07-021</u>	02/28/08	
<u>MS07-017</u>	<u>iPR Server/CP GX-100 Patch corresponding with MS07-017</u>	02/28/08	
<u>MS07-013</u>	<u>iPR Server/CP GX-100 Patch corresponding with MS07-013</u>	02/28/08	

Ricoh Vulnerabilities



J-Security Center

[Home](#) > [J-Security Center Home](#) > [T](#)

- Threats and Vulnerabilities
- Microsoft Security Bulletins
- Case Studies and White Papers
- News and Awards
- About Us

Latest Attack Object Updates

IDP Daily Update #1321
posted: 12/02/08

NSM Daily Update #1321
posted: 12/02/08

Deep Inspection 5.3r5 and above, 5.4, 6.0 #1321
posted: 12/02/08

Deep Inspection 5.1, 5.2, 5.3r4 and below #1300
posted: 12/02/08

Deep Inspection 5.0 #1132
posted: 04/01/08

Antivirus
posted: 12/01/08

TITLE: RICOH AFICIO 450/455 PCL PRINTER REMOTE ICMP DENIAL OF SERVICE VULNERABILITY

Severity: HIGH

Description:

The Ricoh Aficio 450/455 is a large, network-attached printer and photocopier.

It is reported that Ricoh 450/455 printers are susceptible to a remote denial of service vulnerability. This issue is due to a failure of the device to properly handle exceptional ICMP packets.

Specifically, if the printer device receives ICMP packets that are larger than 28 bytes, have an ICMP type of 3 (destination unreachable), have an IP header length of less than 5, and an IP protocol type of 6 (TCP), or 17 (UDP), it will reportedly restart. ICMP types including 4 (source quench), 11 (time exceeded), 12 (parameter problem), and possibly others are also reportedly able to restart the printer. Other IP protocol values and combinations may also be sufficient to exploit this vulnerability.

Remote attackers may exploit this vulnerability to restart affected devices. Repeated packets may be utilized to sustain the condition, causing the device to repeatedly restart. Source addresses of the malicious ICMP packets may also be spoofed, reducing the likelihood of locating, or blocking access to the attacker.

Due to code reuse among devices, it is likely that other printers are also affected.

Affected Products:

- Ricoh Aficio 450 PCL Printer 0.0.0
- Ricoh Aficio 455 PCL Printer 0.0.0

SHARP[®]

Sharp Imaging and Information Company of America

Sharp is a registered trademark of Sharp Corporation and/or its affiliated companies. All other trademarks are the property of their respective holders. All Rights Reserved

COPYRIGHT© 2010 BY SHARP ELECTRONICS CORPORATION