Xerox® FreeFlow® Accxes® Print Server Information Assurance Disclosure Paper Version 1.1

Prepared by:

Jim Gotta
Xerox Corporation
800 Phillips Road
Webster, New York 14580

Document Version: 1.02 (December 2010).

Table of Contents

1 Introduction

The Xerox FreeFlow Accxes Print Server is the controller for the majority of the Xerox Wide Format Xerographic printers and multifunction systems. Systems include the 6279, 6622, and the 6604.

The primary software version covered in this document is Accxes v15.

1.1 Purpose

The purpose of this document is to disclose information for the Wide Format Accxes based products with respect to device security. *Device Security,* for this paper, is defined as how image data is stored and transmitted, how the product behaves in a networked environment, and how the product may be accessed, both locally and remotely. Please note that the customer is responsible for the security of their network and the data being transmitted on it. The Accxes products do not establish security for any network environment.

The purpose of this document is to inform Xerox customers of the design, functions, and features of the Accxes products relative to Information Assurance (IA).

This document does NOT provide tutorial level information about security, connectivity, PDLs, or Wide Format products features and functions. This information is readily available elsewhere. We assume that the reader has a working knowledge of these types of topics.

1.2 Target Audience

The target audience for this document is Xerox field personnel and customers concerned with IT security.

1.3 Disclaimer

The information in this document is accurate to the best knowledge of the authors, and is provided without warranty of any kind. In no event shall Xerox Corporation be liable for any damages whatsoever resulting from user's use or disregard of the information provided in this document including direct, indirect, incidental, consequential, loss of business profits or special damages, even if Xerox Corporation has been advised of the possibility of such damages.

2 Device Description

A wide format system is comprised of an Accxes controller and a printer (a.k.a. image output terminal, marking engine) and potentially a scanner. The Accxes controller provides the network connectivity, prepares files for printing, and if applicable provides the copy and scanning functions.

2.1 Security-relevant Subsystems

2.1.1 Physical Partitioning

The security-relevant subsystems of the product are physically partitioned as shown in Figure 1 below.

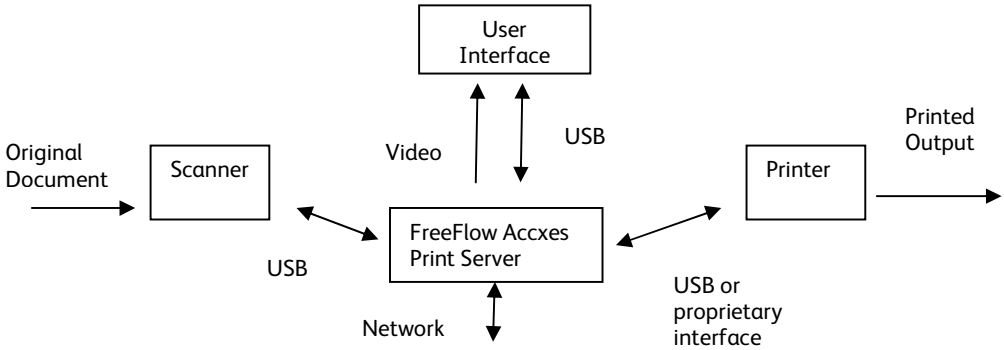

Figure 1 Physical Configuration

2.2 Controller

The FreeFlow Accxes Print Server is the controller for the printer, copier, or multi-function system. It is based upon a customized personal computer which does not include a standard keyboard, display, or mouse. Device setup information is sent to the scanner and printer over USB or proprietary interface in the case of some models which use proprietary protocols. Scanner sends image data to the controller for processing. Print or copy information to be printed is sent to the printer.

2.2.1 Purpose

The Controller provides both network and direct-connect external interfaces, and enables print, copy, and network scans. The copy and scanning features are optional in most configurations.

An Image Overwrite Security kit is available which enables both Immediate and On-Demand overwrite of any temporary image data created on the controller hard drive. The Controller also incorporates a web server that exports a Web Printer Management Tool through which System Administrators can remotely administer the machine. The Controller is sometimes referred to as the Electronic Subsystem (ESS).

Depending upon the configuration, an interface card is used to enable direct host-based printing over a parallel connection. This card is installed in one of two available PCI slots in the Controller.

The Controller runs Fedora Operating System. Unnecessary services are disabled in the OS.

2.2.2 Hardware

Name	Size	Purpose / Explanation
Processor	NA	Intel Celeron or Core 2 Duo (model dependant)
DRAM	512 MB – 2 GB	The executable software is loaded from disk and runs in this memory. It is also used for temporary storage of data files and images. This information is not backed up and is lost when the power to the copier is removed. Upon power-on the Controller DRAM, is put through a memory test which performs an overwrite function.
Network Controller Hard Disk	80 or 160 GB	This device contains numerous types of data: - All executable code (operating system, PDL interpreters, network protocol, device management, etc.). - Spooled documents in PDL format from the network, as well as Network Scan jobs prior to export - Server IDs, server password, user IDs, user passwords, and file locations (for Network Scanning). - All MIB Objects. The hard disk employs a UNIX-like format. When a job is completed, its reference in the directory table is deleted. If Immediate Image Overwrite is enabled, the sectors containing job image data are overwritten using a 3-pass overwrite algorithm. On-Demand Image Overwrite allows the user to overwrite the entire spooling area of the hard disk. Both IIO and ODIO are available in the Image Overwrite Security Option Kit.
Removable Hard Drive	80 GB	An option is available to replace the normal internal hard drive with a removable hard drive. This enables the system hard drive to be put into a secure location when not in use or enables the use of a hard drive per security classification of work being performed. If multiple removable hard drives are in use, the Accxes Print Server software must be loaded onto each and each one will have its own setup information.

Table 1 Controller Hardware Components

2.2.3 External Connections

Interface	Description / Usage
10/100/1000 Mb Ethernet RJ-45 Network Connector	Network Connectivity
Serial Port	Diagnostic use & Engineering development debug
USB	Ports are used for scanning, printing, power control, and potentially UI buttons and USB to serial adapter for a finisher. External device can be connected in some configurations for scanning to and printing from.
Centronics Parallel Port	Never used
FireWire	PCI board and used for particular scanner model
Video	Connection to touch screen UI if applicable for the configuration

Table 2 Controller external interfaces

2.3 Scanner

2.3.1 Purpose

The purpose of the scanner is to provide mechanical transport of hardcopy originals and to convert hardcopy originals to electronic data.

2.3.2 Hardware

The scanner converts the image from hardcopy to electronic data. The scanner provides enough image processing for signal conditioning and formatting. The scanner does not store scanned images. All other image processing functions are in the Accxes controller.

2.3.3 Control and Data Interfaces

Scanned images are transmitted from the scanner to the copy controller across a USB interface.

2.4 Printer (also known as the Image Output Terminal or Marking Engine)

2.4.1 Purpose

The printer performs copy/print paper feeding and transport, image marking and fusing. Images are not stored at any point in this subsystem.

2.4.2 Hardware

The printer is comprised of paper supply trays and feeders, paper transport, xerographics, and paper output.

2.4.3 Control and Data Interfaces

Images and control signals are transmitted from the Accxes controller to the printer across either a proprietary interface or USB interface.

2.5 System Software Structure

2.5.1 Open-source or third party components

Open-source components in the connectivity layer implement high-level protocol services. The security-relevant connectivity layer components are:

- Java 6.0_03
- JBOSS v6.1.0.Final
- Netsnmp 5.4.1-1
- Samba 3.0.24-11

2.5.2 OS Layer in the Controller

The OS layer includes the operating system, network and physical I/O drivers. The baseline for the product launch version of the Controller operating system is Fedora core 6, kernel version 2.6.22.9-61.fc6

2.5.3 Network Protocols

The following protocols are implemented by the Controller

Network layer
IEEE 802.1, 802.3

Internet layer
IPv4, IPv6

Transport layer
UDP, TCP

Application layer
SNMP v1 & v2, DHCP, HTTP, DNS, LPR, FTP

2.6 Logical Access

2.6.1 Ports

The following table summarizes all potential open ports and subsequent sections discuss each port in more detail.

Default Port #	Type	Service name
21	TCP	FTP
80	TCP	HTTP
135, 137, 138, 139, 445	TCP	Samba
161	UDP	SNMP
162	UDP	SNMP trap
443, 8443	TCP	HTTPS
515	TCP	LPR
631	TCP	CUPS
2000	TCP	raw IP
9100	TCP	raw IP
50000-50100	TCP	FTP

2.6.1.1 Port 21, FTP

FreeFlow Accxes uses FTP for scanning. Xerox's implementation of FTP allows ONLY 'cd', 'ls', 'dir', 'get' and 'mget'. It does not allow a 'put' or 'open' or any other security breaching commands. If FTP is an issue, the customer can use "scan-to-FTP" which allows for specifying preset ftp destinations with usernames and passwords, to which the scanned images are sent. If scan-to-FTP is used, then the FTP port can be disabled by the service engineer via the debug port.

2.6.1.2 Port 80, HTTP

The embedded web pages communicate to the machine through a set of unique APIs

The HTTP port can only access the HTTP server residing in the Controller. The purpose of the HTTP server is to:

- Give users information of the status of the device;
- View the job queue within the device and delete jobs;
- Allow remote administration of the device. Many settings that are on the Local UI are replicated in the device's web pages. Users may view the properties of the device but not change them without logging into the machine with administrator privileges.

The HTTP server can only host the web pages resident on the hard disk of the device. It does not and cannot act as a proxy server to get outside of the network the device resides on. Hence the server cannot access any networks (or web servers) outside of the customer firewall.

When the device is configured with an IP address, it is as secure as any device inside the firewall. The web pages are accessible only to authorized users of the network inside the firewall.

This port and Web service may be disabled by the CSE (Customer Service Engineer).

2.6.1.3 Ports 161, 162, SNMP

These ports support the SNMPv1 and SNMPv2 protocols. Please note that SNMP v1 does not have any password or community string control. SNMPv2 relies on a community string to keep unwanted people from changing values or browsing parts of the MIB. This community string is transmitted on the network in clear text so anyone sniffing the network can see the password. Xerox recommends that the customer change the community string upon product

installation. SNMP is configurable, and may be explicitly enabled or disabled through the Web Printer Management Tool.

2.6.1.4 Port 443, HTTPS / SSL

This port is open, but currently is not utilized.

2.6.1.5 Port 515, LPR

This is the standard LPR printing port, which only supports IP printing. It is a configurable port, and may be explicitly enabled or disabled.

2.6.1.6 Port 631, CUPS

This port is used by the Controller to send a print job to a different printer on the network.

2.6.1.7 Port 2000, 9100, raw IP

This allows downloading a PDL file directly to the interpreter. This port has limited bi-directionality (via PJL back channel) and allows printing only. These are configurable ports and may be disabled.

2.6.2 IP Filtering

The devices contain a static host-based firewall that provides the ability to prevent unauthorized network access based on IP address and/or port number. Filtering rules can be set by a CSE using the serial debug port.

3 System Access

3.1 Authentication Model

There are a few ways that user authentication and passwords come into play within an Accxes Printer Server.

3.2 Login and Authentication Methods

3.2.1 System Administrator Login

The System or Device Administrator password is not enabled at initial installation. If desired, a password can be entered. The password is numeric between 0 and 99999.

This password is stored on the Controller hard drive in non encrypted form. It is recommended that this password be changed from its default value immediately upon product installation.

3.2.2 User authentication

The only user authentication that is available is associated with the accounting feature (see JBA section 4.1).

3.2.3 Service (CSE) authentication

The serial debug port service account password is available to customers on a need to know basis and can be changed by using the "passwd" command after logging into CSE / service account on serial port. The new service serial port password would have the following restrictions:

- Minimum of 6 characters
- Can't be a dictionary word or even based on a dictionary word
- Can't be set to all letters or all numbers
- Can't be simple sequence like "123456" or "asdfgh"

3.2.4 Root password

The "root" password is closely guarded and we do not give it to anyone. If deemed necessary, the system can be installed with a root password of "root" that can then be changed by a knowledgeable IT administrator.

3.3 System Accounts

3.3.1 Scan to Mailbox [Multifunction models only]

A user can define Scan to mailbox. When a mailbox is defined, a password can be assigned to that mailbox. The password can apply to scanning into the mailbox, for retrieving files from the mailbox, or both. The password is stored on the hard drive in an encoded format.

3.3.2 Scan to FTP [Multifunction models only]

Scan to FTP requires the device to connect to a FTP server. A device administrator defines up to four locations a user can scan to. Locations include server name, directory, user name, and password. Any user is permitted to use any of the four predefined FTP locations. The FTP setup information is stored on the hard drive in encoded format.

3.3.2.1 Device log on

Scanning feature	Device behavior
Scan to FTP, Public Template	The device logs in to the scan repository as set up by the SA in Web Printer Management Tool

Please note that when the device logs into any server the device username and password are sent over the network in clear text.

3.3.2.2 Scan Template Management

Passwords are not stored as part of templates.

3.4 Diagnostics

3.4.1 Service [All product configurations]

To access onboard diagnostics from the local user interface, Xerox service representatives (CSE) must enter a unique 4-digit password. This PIN is the same for all product configurations and cannot be changed.

The CSE can connect a laptop to the serial debug port. A service password must be entered. This can be changed per Section 3.2.3.

3.4.1.1 Accessible Data

There are several sets of data the CSE can store to a USB thumb drive. These are for diagnostic purposes as well as saving and restoring configurations over system upgrades. Customer image data is not accessible.

- Application and kernel debug logs
- System setup (includes device administrator password, scan to FTP setups, and scan to mailbox passwords if they exist)
- Printer objects which includes raster stamps, fonts, etc.
- Job accounting database which includes user and project IDs

4 Security Aspects of Selected Features

4.1 Xerox Job Based Accounting

Xerox Job Based Accounting (JBA), intended primarily for use as an accounting service, can be used as a lite internal authorization service. JBA tracks copy, scan, and print usage by individual user. The system administrator can enable/disable the feature via the Web Printer Management Tool. Users and projects are defined using the Account Management Tool. If JBA is enabled and required, a walk-up user must enter a valid JBA User ID before being allowed access to the device. The device will confirm that the entered JBA ID matches an authorized user, and that the user is authorized to bill the entered project number. In this sense, JBA acts as an authorization service. The system administrator can limit access to device services by either user or project IDs.

When JBA is enabled and required, before a print job is submitted, either through a printer driver or Accxes Client Tools, a JBA user ID and project number must also be entered. The user and project IDs are sent to the Controller for validation along with the print job. If the submitted IDs are valid, the job will print. If the submitted ID is invalid, the job is deleted and an error sheet is printed in its place.

Using the Account Management Tool, the SA will be able to download a report that shows activity for all of the users. The SA can add, modify or remove users and their projects at any point.

4.2 Image Overwrite

The Image Overwrite Security Option provides both Immediate Image Overwrite (IIO) and On-Demand Image Overwrite (ODIO) functions. Immediately before a job is considered complete, IIO will overwrite any temporary files associated with print, copy, or network scan jobs that had been created on the Controller Hard Disk. The ODIO feature can be executed at any time by the SA and will overwrite the entire document image partitions of the Controller Hard disk.

If IIO is enabled, certain system features such as InstantAccxes, re-print and hold queues will be disabled.

4.2.1 Algorithm

The overwrite mechanism for both IIO and ODIO conforms to the U.S. Department of Defense Directive 5200.28-M (Section 7, Part 2, paragraph 7-202. The algorithm for the Image Overwrite feature is:

- Step 1: Pattern #1 is written to the sectors containing temporary files (IIO) or to the entire spooling area of the disks (ODIO). (hex value 0x35 (ASCII “5”)).
- Step 2: Pattern #2 is written to the sectors containing temporary files (IIO) or to the entire spooling area of the disks (ODIO). (hex value 0xCA (ASCII compliment of 5)).
- Step 3: Pattern #3 is written to the sectors containing temporary files (IIO) or to the entire spooling area of the disks (ODIO). (hex value 0x97 (ASCII “ú”)).
- Step 4: 10 % of the overwritten area is sampled to ensure Pattern #3 was properly written. The 10 % sampling is accomplished by sampling a random 10 % of the overwritten area.

4.2.2 User Behavior

This feature is available as the Image Overwrite Security Option Kit (please see your Xerox Sales representative for pricing and ordering details). This kit provides overwrite functionality for the Controller Hard Disk in this set of products.

Once enabled, IIO is invoked automatically immediately after the completion of a print or copy.

ODIO is invoked from the Web Printer Management Tool. Network functions will be delayed until the overwrite is completed. Copying is unavailable while the overwrite itself is underway.

4.2.3 Overwrite Timing

The ODIO overwrite time is dependent on the size of hard disk in the product. The overwrite and reset average time is about 60 minutes for an 80 GB HD and over 1 ½ hours for 160 GB, but longer times are possible. The device is not usable during this time and the main services screen will be displayed when the overwrite has completed.

IIO is performed as a background operation, with little reduction in copy, print or scan performance.

5 Responses to Known Vulnerabilities

5.1 Security @ Xerox (www.xerox.com/security)

Xerox maintains an evergreen public web page that contains the latest security information pertaining to its products. Please see www.xerox.com/security

5.2 Viruses, Worms, and Trojans

People often use the term virus to also refer to worms and Trojans, so the following info will assume the same.

FreeFlow Accxes is unaffected by today's Viruses, Trojans and Worms because:

- Local users are not allowed (trusted root/service only),
- Most of the ports are locked down
- Most of the libraries that may open security risks are not even installed.

Linux type systems are also less likely to ever be infected because of reasons really well described in this article. http://librenix.com/?inode=21

We do not include a Virus Checker on FreeFlow Accxes for the following reasons:

- Though there are virus checkers available for the OS, these are primarily aimed at servers. They use the same virus descriptions as windows checkers - ideal for checking for windows based viruses on email-servers or file servers. As FreeFlow Accxes does not store files for passing between machines in this way or support mounting of directories, this checking would be irrelevant.
- More importantly, for a virus to be a threat it has to get onto the system. This is usually done by convincing a user to run an application on the system, often arriving by email attachment, or falsely identified download. As FreeFlow Accxes is not used as a workstation no users run programs on it. Someone would have to go out of their way to try and do this, which would require malicious intent from someone with physical access to the machine, or an SSH remote login (from someone who has access to the LAN to which FreeFlow® Accxes® is connected, remembering FreeFlow® Accxes® is not designed to be connected to the internet). The former risk is already reduced as FreeFlow Accxes does not have a keyboard or mouse attached, and even if they could be the console does not function and there is no browser capability.

If there is still a concern and the above scenarios are considered a risk then preventative measures should be taken, e.g.:

- The Xerox CSE can disable SSH.
- You can lock FreeFlow® Accxes® in a secure computer case to prevent access to the hardware
- You can use managed switches on the network to control what remote systems can communicate with Accxes.
- The risk of virus attacks is still further reduced in Accxes, as it does not rely on many popular services (daemons), which would be prime targets for worms when security vulnerabilities are found. With a standard configuration only a select few services are network accessible, and this number can be reduced by the engineer depending on customer requirements. Ultimately the only essential ports (e.g. 2000, ftp

and http) are required and these are all managed by FreeFlow Accxes code and not standard services, so any worms written to exploit security holes in these will not succeed with Accxes.

In the highly unlikely event a FreeFlow® Accxes® controller was compromised, since it does not act as a customer data store, or connect to file servers, it could not delete customer files. It can be rebuilt quickly by an engineer and as long as the customer ensures there network is secure enough for their requirements (firewalls etc, which should be implemented as a matter of course anyway) it is physically impossible for FreeFlow® Accxes® to send information to the outside world.

6 APPENDICES

6.1 Appendix A – Abbreviations

API	Application Programming Interface
CAT	Customer Administration Tool
CCITT	Comite Consultatif International de Telegraphique et Telephonique (International Telegraph and Telephone Consultative Committee) [now ITU-T]
CSE	Customer Service Engineer
DC	Digital Copier
DHCP	Dynamic Host Configuration Protocol
DNS	Domain Name Server. A centralized database that maps host names to static IP addresses.
DDNS	Dynamic Domain Name Server. Maps host names to dynamic static IP addresses.
DRAM	Dynamic Random Access Memory
EGP	Exterior Gateway Protocol
GB	Gigabyte
HP	Hewlett-Packard
HTTP	Hypertext transfer protocol
IIO	Immediate Image Overwrite
IIT	Image Input Terminal (the scanner)
IT	Information Technology
IOT	Image Output Terminal (the marking engine)
IP	Internet Protocol
IPX	Internet Protocol Exchange
ITU	International Telecommunications Union
JBA	Job Based Accounting
LAN	Local Area Network
LED	Light Emitting Diode
LPR	Line Printer Request
LZ	Lempel Ziv (a type of compression)
MAC	Media Access Control
MIB	Management Information Base
n/a	not applicable
NVRAM	Non-Volatile Random Access Memory
NVM	Non-Volatile Memory
ODIO	On-Demand Image Overwrite
PDL	Page Description Language
PIN	Personal Identification Number
PROM	Programmable Read-Only Memory
PWBA	Printed Wire Board Assembly
PSW	Portable Service Workstation
PWS	alternative acronym for Portable Service Workstation
RFC	Required Functional Capability

ROM	Read Only Memory
ROS	Raster Output Scanner
SA	System Administrator
SIMM	Single In-line Memory Module
SLP	Service Location Protocol
SNMP	Simple Network Management Protocol
SRAM	Static Random Access Memory
SSL	Secure Sockets Layer
TCP	Transmission Control Protocol
TIFF	Tagged Image File Format
UI	User Interface
URL	Uniform Resource Locator
UDP	User Datagram Protocol