

Document Output Security

A White Paper

Equitrac Corp.
December 2006
Copyright © 1997-2006 by Equitrac Corporation

Identification

Document title: Document Output Security: A White Paper

Document ID: WP-2007-DOS-10

Copyright

This document is copyright © 1997-2006 by Equitrac Corporation. All rights to this document, domestic and international, are reserved by Equitrac Corporation.

Trademarks

Equitrac is a registered trademark of Equitrac Corporation. Equitrac Office, Equitrac Express, Follow-You Printing and PageCounter are trademarks of Equitrac Corporation.

Canon is a trademark of Canon Inc.

Hewlett-Packard is a registered trademark of Hewlett-Packard Company.

IBM is a registered trademark of IBM Corporation.

Lexmark is a registered trademark of Lexmark Corporation.

Active Directory, Microsoft, Windows and Windows Server are registered trademarks of Microsoft Corporation.

NetWare is a registered trademark and eDirectory is a trademark of Novell, Inc.

Okidata is a registered trademark of Oki Electric Industry Company, Ltd.

Oracle is a registered trademark of Oracle Corporation.

Ricoh is a registered trademark of Ricoh Company, Ltd.

Xerox is a registered trademark of Xerox Corporation.

All other brands and their products are trademarks or registered trademarks of their respective holders, and should be noted as such.

Abstract

Most medium and large organizations have made the transition to networked printing environments; and as more document production goes digital, printing continues to replace copying. The growth of network printing, combined with increased requirements for data confidentiality and regulatory compliance, has made organizations more aware of the need for document output security.

These security requirements are highlighted by developments such as the IEEE P2600 hardcopy security standard working group, ongoing introduction of security-focused products, and manufacturers' efforts to gain security certifications for their output devices.

This white paper describes key security issues relating to document output in the office environment, methods to addressing those issues, and guidance for implementing a secure print management and tracking system such as Equitrac Office 4.

Introduction

A review of basic security concepts and the external requirements driving the security needs for output devices will help in understanding how to implement network printing security.

Security requirements

The use of networked output devices has increased the vulnerability of devices to attacks: modern printers and multifunction products (MFPs) can be accessed by anyone with physical or network access, whereas legacy personal printers required physical access to an individual's office.

Meanwhile, companies are increasingly being forced to invest in securing their computing infrastructures – both from denial-of-service attacks such as network worms, email viruses or attacks on hardcopy devices and from attacks on document confidentiality.

Regulatory requirements – such as those in the Sarbanes-Oxley Act, Gramm Leach Bliley Act, European Union directive 95/46/EC, METI Policy on Protection of Personal Information, Health Insurance Portability and Accountability Act (HIPAA) and Personal Health Information Protection Act (PHIPA) – impose a burden on many organizations to ensure the confidentiality of the data they work with.

Common Criteria certification

The Common Criteria (ISO 15408) are a standard for computing security, which can also be applied to document output devices. Some device manufacturers have certified their equipment under the Common Criteria process. But because of the process's cost and complexity, certification is often limited in scope to a subset of device functionality – such as hard disk overwrite capability.

And while certification may verify the manufacturer's specific claim of compliance, it does not address the document output security environment. Certification may be useful in confirming the manufacturer's claims of functionality, but is not sufficient in itself for the implementation of a secure document output infrastructure.

IEEE P2600

The IEEE P2600 standards working group is attempting to overcome the limitations of the Common Criteria certification by defining a broad security standard for output devices. Expected to be completed in 2007, this standard will address a variety of computing environments, from small office/home office to enterprise.

This broad industry effort is supported by key players such as Canon, Equitrac, Hewlett-Packard, IBM, Lexmark, Océ, Okidata, Ricoh, Sharp and Xerox.

Level of security and care

In many organizations, internal needs drive the level of security implemented to ensure data confidentiality. In others, however, it is the external regulatory environment that dictates the minimum security level of a document output system.

In many cases, the legislation – such as HIPAA – is not prescriptive; that is, it might mandate that organizations exercise “ordinary care” or “reasonable care” protecting information rather than dictating specific security measures that satisfy that requirement.

The State of Maine, for example, defines ordinary care as follows:

“Ordinary care means, in the case of a carrier, the degree of care that a carrier of ordinary prudence would use under the same or similar circumstances. For a person who is an agent of a carrier, ordinary care means the degree of care that a person of ordinary prudence would use under the same or similar circumstances.”

Essentially, an organization that is required to take ordinary care or reasonable care to ensure security, confidentiality and privacy of data, must take precautions to protect its information against threats, whether from external or internal attackers.

To draw a comparison, a person of “ordinary prudence” would protect his or her credit card through physical security (keeping the card in a wallet or purse); by requiring authentication (not providing the card number to unknown persons or web sites); and data protection (destroying or shredding credit card receipts and bills).

However, a person of ordinary prudence would not normally resort to extraordinary measures such as traveling in armored vehicles to increase their physical security, extending authentication by requiring to see the passport of a seller before providing a card, or refusing to purchase goods from anyone outside their immediate family in an effort to completely protect their data.

Similarly, reasonable care must be taken in a commercial environment. Such measures should protect against the highest-risk attacks on document output equipment and activities, without impeding the organization’s productivity and without imposing excessive implementation costs.

Threats

Threats to document output fall into five general categories:

1. Denial of service – removes the document output system from operation or makes it otherwise inaccessible, thereby preventing users from being able to output documents.
2. Resource theft – includes theft of consumables and bypassing of accounting mechanisms to obtain free output.
3. User data theft – in which attackers attempt any number of mechanisms for gaining access to users' confidential data.
4. Security configuration attacks – compromise or alter the document output system's security environment, often enabling an attacker to make further attacks without detection.
5. Environmental attacks – are launched on the network at large by leveraging the document output system.

Protecting against document output threats

Fortunately, several proactive measures are available to address key threats to document output systems in an ordinary office computing environment.

Denial of service

Network-based denial of service

Today, the most common denial-of-service attack on document output systems is an attack on the device's network interface. This attack, which may consist of network floods, crafted malformed network packets or excessive network connections, is essentially identical to attacks on other networked equipment, such as servers, routers or workstations.

Because it is generally difficult to resist such attacks while they are occurring, it is important to secure devices against them in the first place. Acquiring printers and MFPs that can recover from denial-of-service attacks does not reduce the need to protect them. One security strategy is to place the hardcopy devices on a dedicated subnet or VLAN and restrict access to that network to specific servers only. This can significantly mitigate the risk, as network access to those devices will be considerably more difficult to achieve.

However, this approach may require a server-based system for monitoring the printers and MFPs since individual workstations cannot establish SNMP connections to the output devices. Equitrac Office's DME (Device Monitoring Engine) provides such a server-based capability, providing monitoring even if network access to the output devices is restricted.

Physical denial-of-service

Physical denial-of-service attacks are more common in public-access areas, and are essentially those attacks traditionally described as "vandalism": physically altering or damaging a printer or MFP, or cutting its network connection, whether as a planned attack or in a spontaneous outburst of violence.

Physical attacks on printers and MFPs generally cannot be prevented, but the risk can be substantially reduced by carefully considered placement, ensuring the devices are accessible only to authorized users and placing them in well-lit, visible, areas or within visual range of the organization's staff.

Resource theft

Like physical denial-of-service attacks, resource theft is most common in public environments, and especially so in educational institutions, where the user population often has low or no income, is often well educated and resourceful, and may have rebellious ideas about “beating the system.”

Theft of consumables

Theft of supplies and consumables can only be prevented through physical security: unless the printer or MFP has locking doors and drawers, the only option for mitigating the risk of this attack is by placing the printer or MFP in either a staffed area or in a well-lit location with relatively high traffic.

Circumvent copy accounting

An attacker may attempt to circumvent a copy control and auditing mechanism by replacing the organization’s copy control equipment with a rogue copy control device.

Physically securing the copy control devices – or utilizing embedded software-only copy control mechanisms – can largely protect against this threat. Physical security, as described in the previous section, may also reduce opportunities for this attack.

Circumvent print tracking

An attacker may also attempt to steal resources by bypassing the document accounting or auditing mechanisms for printing. This type of attack, if successful, also bypasses the print tracking mechanism, thus compromising the integrity of the system audit trail.

Protection against the print tracking bypass threat can be achieved by ensuring that the system incorporates robust datastream interpreters or device feedback mechanisms to ensure that an attacker cannot spoof the tracking system – for example, by injecting of rogue PostScript comments.

Such a print tracking system should also rely, as much as possible, on the existing network authentication infrastructure, rather than easily-guessed user or account codes.

Finally, to prevent an attacker from avoiding print tracking by bypassing the print server, the printers and MFPs should be configured to accept connections only from authorized print servers whenever possible. Alternatively a VLAN or dedicated subnet with a router can be used to limit access to the hardcopy devices only to authorized print servers.

User data theft

Network sniffing

The most commonly recognized attack on user data confidentiality is network sniffing. In its most basic form, this involves capturing network packets on an unswitched Ethernet network using either a commercial or open-source network sniffer tool.

The risk of this particular threat can be mitigated through the deployment of an end-to-end switched Ethernet infrastructure, thus precluding trivial sniffing of network traffic from other sources and destinations – with the side benefit of improved performance for network users.

For increased security, and to protect against attacks where an attacker taps into the network between the output device and its network jack, the traffic between the printer or MFP and its print server should be encrypted. Standards-based strong encryption, such as IPsec, should be used whenever supported by both the print server and the output device, as the IPsec encryption overhead for typical printing traffic is small enough to be insignificant in practice.

EM sniffing

In higher-security environments – though rarely at the level of “ordinary care” – additional measures may be taken to prevent the detection of the electromagnetic emissions from network cabling or output devices (referred to as EM sniffing). For these types of applications, fiber-based networks are frequently selected to eliminate the electromagnetic emissions.

Hard disk analysis

A user data threat also often considered serious in high-security environments is the removal of the MFP’s or printer’s hard disk, and the retrieval of its contents. In the case of a device that does not encrypt or thoroughly erase the data on the hard disk, nor protect against its removal, an attacker may simply connect the disk to a computer to retrieve images of printed or copied documents from that disk.

More advanced attackers, who are targeting very high-value assets, may even perform advanced data recovery or electron microscopy operations to extract data that has been erased from the disk. These advanced attacks can only be protected against by preventing the removal of the hard disk from the hardcopy device.

Access to physical documents

The final type of user data threat is the removal of physical documents from the input or output tray of an MFP or printer. While this type of attack does not generally have the profile of a network sniffing attack, it is easier to perform, requiring no specialized tools or knowledge; documents printed by users from their desktops often sit in the printer’s output tray for minutes or even hours, allowing anyone with physical access to the output device to either inspect or remove them.

Protection against the removal of printed documents can be achieved relatively easily by implementing Follow-You Printing™ with Secure Document Release. This solution holds documents in a secure queue on the print server until the appropriate users authenticate themselves at their output device of choice. Only after the system has validated the user’s identity, and thus ensured that the user is physically present at the device, are the documents printed out.

Security configuration attacks

Unauthorized configuration changes

If an attacker is able to access an MFP's basic security configuration and alter it, the device's overall security may be seriously compromised. One variation of this threat is an attack on an MFP's network scanning address book: by altering the underlying addresses in the address book, an attacker may be able to divert a copy of the network scans to a rogue email address and thus gain access to the contents.

To mitigate the risk of this attack, the administrative user IDs and passwords selected for use on the MFPs and printers should be strong and not accessible to non-administrative users. And any remote configuration of output devices should be done through an encrypted network connection.

Alteration of audit trail

The audit trail – whether for authentication, printing or copying – is a critical part of the security environment. The integrity of the log, often held on the print server, must be protected to ensure that it accurately describes all authentication and document output activity on the network. The log's contents must be protected from unauthorized access to protect the privacy of users whose activity is recorded in the audit trail.

To effectively protect the integrity and contents of the audit trail on the server, the auditing server's application and database security should be based on the network authentication infrastructure, with its underlying security policies. Access to the auditing application, and to its database, should generally be restricted to authorized security administrators only.

Rogue software updates

The final security configuration threat is a particularly perilous one: the threat of installing a rogue firmware image or a rogue embedded software applet on the output device. If an attacker were to be able to install such a software module on a printer or MFP, that rogue module could then be utilized as a launch pad to initiate a variety of other types of attacks, ranging from denial of service to compromising user data.

Protection against the installation of rogue software or firmware on the output device is best gained by ensuring that the device will only accept the installation of firmware images or embedded applets after the presentation of valid security administrator credentials, and, even then, validate the uploaded image or applet using a digital signature or similar technology in order to ensure its authenticity.

Environmental attacks

In an environmental attack scenario, an attacker will utilize a printer or MFP as a springboard to propagate an attack on the rest of the network, whether denial of service or otherwise – akin to the original Morris worm.

Defenses for environmental attacks are essentially the same as for network-based denial-of-service threats and security configuration threats: limit network access to output devices by placing them on dedicated subnets or VLANs; restrict network connections to the devices to known print servers; utilize encrypted links wherever possible; and deploy strong passwords for all administrative functions.

Implementing a secure printing system

By following best practices in implementing Equitrac Office 4† – learned through the three decades' experience of over 10,000 Equitrac customers worldwide, organizations can achieve a secure printing system with a comprehensive print tracking audit trail and Follow-You Printing with Secure Document Release.

Follow-You Printing with Secure Document Release

As noted in the previous section, one of the largest unaddressed security threats today is the unrestricted access to hardcopy output at the printer or MFP, typically sitting in the output tray, waiting for the user to arrive.

Implementing Follow-You Printing with Secure Document Release as part of an Equitrac Office deployment can effectively mitigate this risk, ensuring that documents are not printed until users enter a password or PIN or swipe an ID card to authenticate themselves at the output device, confirming they are physically present to retrieve their documents.

The requirement to perform an authentication before printing may at first meet some user resistance. However, users generally accept this step to realize the roaming benefits of Follow-You Printing, which allows users to authenticate and retrieve documents at the output device of their choice anywhere on the organization's print network – including across servers and geographic locations.

Authentication mechanism

The selected authentication mechanism will apply to both Follow-You Printing as well as the authentication required for copying, faxing and scanning. A variety of authentication mechanisms can be selected, one single-factor and three two-factor:

- Primary PIN (or card swipe) only
- Primary PIN (or card swipe) and secondary PIN
- Network user ID and password
- Primary PIN (or card swipe) and network password

For increased security, one of the last three options should be selected. The use of cards, as with the second and fourth options, greatly increases end user convenience, thus reducing user resistance to the authentication system.

When identification cards are implemented, relatively tamper-proof cards such as Mifare or Legic contact-less smart cards can provide significantly greater security than easily-duplicated magnetic stripe cards.

End user security choice

In some environments it is desirable to let end users select at print time whether a particular document should be "secure" or "standard" – essentially whether or not the document should be held in the secure Follow-You Printing queue pending user authentication.

This choice is best implemented by creating a second companion print queue, with Secure Document Release disabled. Availability of a separate queue allows users to quickly select secure or standard printing, without having to click through a series of dialog boxes.

† While this section refers to Equitrac Office 4, note that all discussion is also applicable to Equitrac Express 4.

Further, a separate queue enables the use of Windows security to limit access to the standard queue to specific groups of users, and the use of Windows spooler configuration to limit access to the standard queue to specific operating hours. Finally, the Equitrac Office detailed audit trail can provide tracking on what documents each user printed to both the secure and standard print queues.

The rules and routing capability of Equitrac Office can also be used to restrict access or to redirect documents from the standard to secure queue, based on user group membership, document title, originating application and other criteria.

Audit trail

The second key security benefit of Equitrac Office is its detailed audit trail for all document output activities in the organization. Audited activities are stored in the central database for comprehensive reporting, using either the solution's standard customizable reports, or external reporting tools such as Crystal Reports.

The audit trail typically includes the following auditing information for each printed and copied† document:

- Network user ID
- Printer or MFP utilized
- Date and time
- Activity type
- Number of pages
- Job size (KB)
- Page details: color/monochrome, duplexing, paper size, media type
- Job details: stapling, punching, folding

By performing reporting or analysis on the detailed audit trail, organizations can identify document output patterns and exceptions that should be further investigated.

Rules and routing

Equitrac Office enables administrators to define rule sets, which are then applied to one or more output devices.

These rules can then be used to restrict access or to redirect documents to specific devices, based on criteria such as group membership, document title, originating application or document size. For example, output from specific applications might be permitted on particular output devices only.

† The amount of audit detail on copied documents is dependent on the MFP manufacturer and the technology used to capture that activity.

Networking infrastructure

Network topology

As noted in the Network-based denial of service (page 2), placing output devices on a dedicated network or VLAN helps mitigate the risk of a denial-of-service attack.

Locating Equitrac PageCounter terminals, if applicable, on the same dedicated network is also advisable, as these devices, could also be targets of a denial-of-service attack, causing loss of access to printing and copying. Placing them on a dedicated subnet or VLAN significantly reduces this risk.

Database connection

Equitrac Office supports multiple database types (Microsoft SQL Server, Microsoft SQL Express, MSDE and Oracle).

Where possible, in environments using the Microsoft database types, the database connection should be configured to use Windows Authentication . SQL Authentication for the database should be disabled, and the database access rights should be restricted to only the user ID under which the Equitrac CAS service is running.

Should the database be located on a distinct physical server from the one running the Equitrac CAS service, for maximum security an IPsec connection should be enabled between the CAS and database servers.

Directory security

To ensure the integrity of the Equitrac Office installation, the directory security on \Program Files\Equitrac and its subdirectories should be set to allow read-only access to those files and directories to the user ID(s) running the Equitrac Office services, and no access to other users.

The default DRE spool directory (for Follow-You Printing) location is under the DRE user's Documents and Settings directory:

```
... \Local Settings\  
Application Data\  
Equitrac\  
Equitrac Platform Component\  
4\  
EQDRESrv\  
EQSpool
```

This directory is, by default, secured for the user ID under which DRE is running. However, should an alternate directory location be used, care must be taken to ensure that its security is sufficient to prevent read or write access to other users.

Service credentials

Each of the system services in Equitrac Office can run under arbitrary user credentials.

To minimize the security exposure, create a specific user ID (or set of user IDs) for the services to run under, restricting the rights granted to those user IDs to the minimum required.

All services are able to run with local user IDs; however, the scheduler service may require domain access. Also, remote management of the system is greatly simplified if a domain user ID is used for the services, as a local user ID will not be able to validate the group membership of the user establishing the management tool connection.

The following two services have specific rights requirements:

- Equitrac CAS service requires domain access to perform pass-through authentication to Active Directory. If pass-through authentication will not be utilized, the CAS service can run under a local user ID.
- Equitrac DRE service requires the right to manage print jobs on the local server in order to submit the jobs for printing.
- Equitrac scheduler service requires domain access in order to perform Active Directory synchronization. If synchronization will not be implemented, the scheduler can run under a local user ID.

Windows Firewall

The Windows Firewall, built into Windows Server 2003, can be used to enhance the security of the Equitrac Office installation, and to increase its resistance to denial-of-service attacks. The following provides a guideline for configuring the Windows Firewall exception rules for the Equitrac Office system services:

- For Equitrac CAS service, limit the scope of the exception to the local subnet. If workstation clients are not used, limit the scope to the IP addresses for the list of DRE, DCE and DME servers, plus the workstations used for management (whether System Manager, Accounts Manager, Reports Manager or Device Management Console), deployed on the network.
- For Equitrac DCE service, limit the scope to the subnet(s) containing the output devices and the PageCounter devices, if applicable.
- For Equitrac DRE service, limit the scope to the subnet(s) containing the output devices and the PageCounter devices, if applicable. If Release Station software is utilized, also include workstations running that software in the scope.
- For Equitrac DME service, limit the scope to the subnet(s) containing the output devices and the PageCounter devices, if applicable.

Security roles

Equitrac Office provides multiple security roles, using Windows authentication and domain groups to control access to distinct parts of the system. To effectively secure the system, specific domain groups should be created for each of the security roles:

- Admin users have full configuration rights to the system and can change all configuration settings, including the security configuration.†
- Reports users are able to run reports using Reports Manager, including the detailed audit trail.
- Accounts admin users are able to manage user accounts – including secondary PINs – using Accounts Manager.
- Department admin users are able to manage user accounts – including secondary PINs – for their own department only, using Department Manager.
- Device admin users are able to manage DME (Device Management Engine) devices using Device Management Console.
- Print distribution users are able to print for other users using the workstation client's Print for Others capability.

Encryption

Equitrac Office always encrypts PIN codes using 128-bit AES encryption whenever they are transmitted on the network to ensure that the codes cannot be easily sniffed.

However, encrypted storage of the secondary PIN is optional (though enabled by default), and can be configured using System Manager. For maximum security, this encryption should always be enabled. This also ensures that the secondary PIN is encrypted on the network connection between CAS and the database server.

For end-to-end data security, consideration should be given to deploying IPP to the desktop, thus enabling encryption of print jobs between the desktop and the print servers, as well as between the print server and the output device.

† Note that the user ID under which Equitrac CAS service is running will always have admin access. For maximum security, interactive login should be disallowed for the user IDs used for the Equitrac Office system services.

User management

Equitrac Office supports four basic user management methods:

- Manual user management using Accounts Manager.
- External user synchronization using EQcmd-based imports.
- External user synchronization using Active Directory or eDirectory.
- Pass-through authentication using Active Directory, NetWare eDirectory or LDAP.

Each method has somewhat different security implications.

Manual user management

The manual user management method requires one or more accounts administrators to create, update and delete users as required, and to manually manage password (secondary PIN) changes.

The security risks in this user management model stem from the accounts administrator knowing all users' credentials; this user must be trusted to manage this information.

EQcmd-based import

The use of EQcmd to script the import or synchronization of users implies the use of text files generated by an external security authority.

To secure this method, the network connection between the Equitrac Office server, the external security authority, and the directory where the text files are stored must have access rights restricted to only the external authority and the user ID running EQcmd.

External user synchronization Active Directory or eDirectory

Using external user synchronization with Microsoft's Active Directory or Novell's eDirectory (formerly NDS) leverages the role of the network directory as the security authority for the network. With this approach, the user PIN codes are maintained in the network directory, and automatically updated in Equitrac Office whenever they are updated; no external export files need to be created.

Active Directory connections are inherently encrypted. However, if eDirectory synchronization is used, the connection between each of the eDirectory servers and the Equitrac Office CAS server should be based on the use of IPsec encryption.

Pass-through authentication

With pass-through authentication, user credentials are not explicitly stored on the Equitrac Office server; rather, the login credentials are passed through to the network directory server, whether Active Directory or any LDAP-compliant directory. This configuration is normally restricted to the use of a network user ID and password typed at the device.

A variation on this configuration combines it with directory synchronization (to retrieve the primary PIN code from the directory into Equitrac Office), allowing the user to either enter the primary PIN at the device (or swipe an ID card containing that number), and then type in the network password. This provides a combination of user convenience, typically through the use of the ID card, and increased security, by requiring the entry of the network password.

Footnotes

<http://grouper.ieee.org/groups/2600/>

Statutes of the State of Maine, title 24-A, §4301-A

<http://technet2.microsoft.com/WindowsServer/en/library/e903f7a2-4def-4f5f-9480-41de6010fd291033.mspx>

<http://snowplow.org/tom/worm/worm.html>

http://en.wikipedia.org/wiki/Morris_worm

<http://www.microsoft.com/sql/prodinfo/previousversions/securingsqlserver.mspx>



1000 South Pine Island Road, Plantation, FL 33324
P + 1.800.327.0183 | F + 1.954.475.7295 | www.equitrac.com