PaperCut™

Securing your Print System

A Whitepaper

by PaperCut Software — May 9, 2017

Contents

1.0 Introduction

Long overlooked by the IT security industry, the importance of printing security is now widely understood. A best-practice information security policy must have a comprehensive set of measures to protect the print system.

This fact is highlighted by the increasing number of printing related security attacks reported in the press. In a 2017 Quocirca report,[1] more than 80% of companies report concerns about print related data losses, with 61% reporting actual losses in the past year.

Print systems tend to be complex, spanning multiple devices, networks, and operating systems. At the same time, they perform critical business functions and process confidential and sensitive data. These facts lead to a large attack surface that is attractive to hackers and denial of service attackers. As a result, security audits and penetration tests often highlight the print system as the weak point in an organization's IT security audit. And remember, security attacks and leaks are just as likely to come from inside your organization as outside.

The good news is that effective print security measures are available and well known. As with all good security practices, the approach presented here is multi-layered, covering all parts of the print workflow.

[1] "Print in the digital age" Louella Fernandes, Quocirca 2017

1.1 Print Security Model
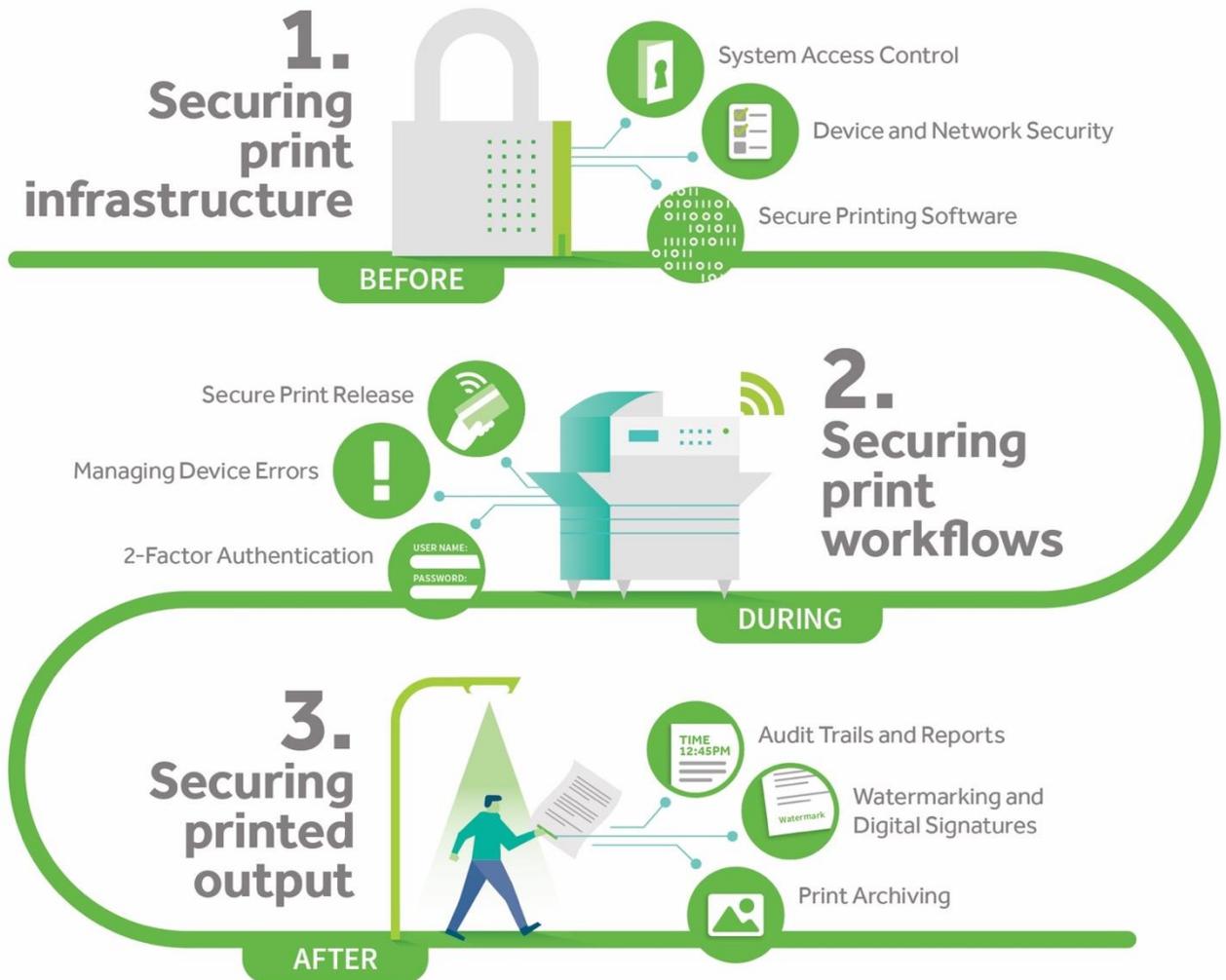
Our print security model covers all phases of the printing lifecycle:

Securing print infrastructure

There are many security measures to be taken before a single document is printed. All parts of the print infrastructure should be secured, including workstations, mobile devices, servers, and networks.

Securing print workflows

While your infrastructure may be hardened against attack, your printing workflows might leave you wide open. We recommend some proven and secure print workflows that are straightforward to implement and pay high dividends.

Securing printed output

Once a document is collected from the printer, how do we keep it secure? Several technologies, such as watermarking and print audit logs, work together to allow traceability and encourage correct user behavior.

1.2 Print Management

Print Management software is commonly used to provide many of the traceability and security features described in this whitepaper. For example, secure print release is an important feature of any print management system. PaperCut NG or PaperCut MF can support all the security measures described in this document.

2.0 Securing Print Infrastructure

When considering end-to-end print security, it makes sense to start with the infrastructure that supports the printing processes. Think of the network and devices that support the print job from the time a user presses "Print" to creating a printed document.

2.1 Print User Authentication

Central to many best practices in security (not just print security) is the ability to uniquely and accurately identify the end user. Desktops should require users to authenticate themselves against a centrally managed source of accounts (i.e. Active Directory, eDirectory, LDAP, Open Directory). This way, you can attribute jobs to these users and control access to various devices as needed.

Identifying the user becomes challenging when she chooses to print from their mobile or BYOD device. And a mobile or BYOD device may not require a user to authenticate before access.

Products like PaperCut's Mobility Print can bridge this gap by ensuring that jobs are correctly authenticated before being accepted by a print server.

2.2 Print Server Security

Most organizations set aside a computer to play the role of the print server, which centralizes printing and make available all the print resources to end users. It's important to consider the security of this server to ensure its availability and reliability, and to reduce the risk of it being compromised.

From an operating system perspective, updates and patches should be regularly applied to address known vulnerabilities. In addition to regularly updating virus definitions on your print servers, print drivers should be kept up-to-date as part of regular maintenance.

The logical location of the server in the network should also be considered as a way of being able to reduce the attack surface and the threat of

attack. Print Servers should be located on the internal network, protected from the internet and DMZ by firewalls. IP addresses on the internal network must not be reachable from an outside network.

Print Queues

A commonly overlooked task is to restrict rights to shared print queues. Rights on shared queues should be configured to ensure users aren't able to take control of each other's jobs or change any of the queue settings. For example, a user should not be able to pause a queue or delete another user's job.

It's also worth noting that not all printing protocols require authentication by design. LPR, as an example, will accept print jobs on port 515 from any client, circumventing the normal access rights a server may use. Some scenarios require the use of LPR and in these cases, we recommend you consider adding controls to restrict which clients that can access the LPR port. Another useful hardening strategy is to add secure print release to an LPR queue.

Print encryption can be a useful way to add an additional layer of security to print jobs in process. One simple way to implement this is to turn on operating system level encryption on the hard drive used to store print queues. This ensures that backdoor access to the hard drive will not lead to sensitive data leaks.

Not all printers should be accessible to all end users. The Principle of Least Privilege recommends you don't grant any user access to a device (server queue) unless they explicitly need it. For example, you might want to restrict access to a printer that uses paper with the company letterhead to limit the risk of misuse.

2.3 Device Security

Multifunction Devices (MFDs) and Multifunction Printers (MFPs) are extremely powerful but also vulnerable to misuse and attack. A range of measures are needed to ensure your printer and MFD are hardened against security threats.
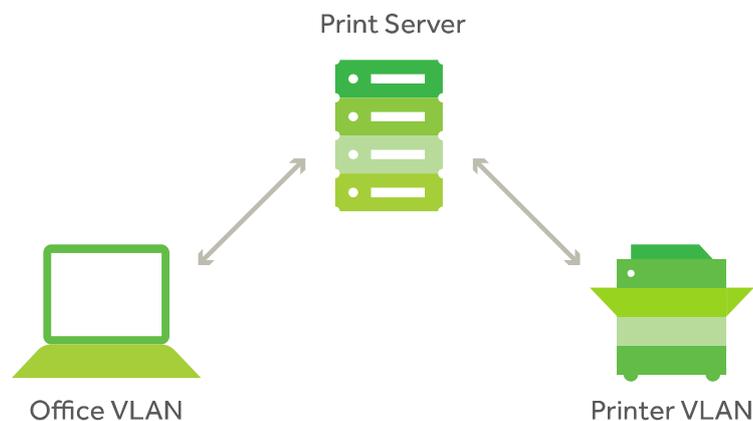
Network

MFDs generally need access to your organization's network to perform functions such as user directory lookup (eg. Active Directory), email/send services, and so on. Make sure you use a service account with the correct

level of access. Using a user level account can make you vulnerable as they are a hacker's prime target.

In a similar context to securing the print server, the logical network location of the MFDs or MFPs themselves should be considered to reduce their attack surface. Does your printer really need to be accessible from the internet, or even from your Brockway or Ogdenville offices?

Conversely, does your printer need internet access or access to the rest of your internal network? Limiting routability of network traffic from a printer subnet can significantly reduce the impact of an infected rogue device.

We recommend that you use your print server as a gateway to all print devices. Use VLANs or subnetting to ensure that the only device that can see the printers is the print server. This ensures that, as a Systems Administrator, you control access to the device via your server. This can also be achieved using Access Control Lists (ACLs) for account level permissions, or IP filtering for preventing access from specific IP ranges, or other creative means to ensure printers cannot be reached directly.

Print Server

Office VLAN   Printer VLAN

Secure Connections

Where there is an option, devices should be configured to use secure, encrypted network connections (e.g. using HTTPS), especially when sensitive data, such as documents and passwords, are transmitted. While PaperCut NG/MF allows for both HTTP and HTTPS, HTTP Strict Transport Security (HSTS) is available to ensure access is allowed only via an HTTPS connection.

Passwords should never be sent over any network connection in clear text. Configure your network to use the most recent TLS protocols

supported by your devices. Certain older protocols, such as SSL v3 and older ciphers such as RC4, have known vulnerabilities and should be disabled.

To avoid <u>man-in-the-middle</u> attacks, SSL connections should ideally require that verified certificates are in place to positively identify the authentication host (such as the host running PaperCut MF). Where a man-in-the-middle attack is assessed as being a low risk, an automatically generated private cert can be used and the other benefits of SSL, such as encryption are still obtained.

One factor that is becoming increasingly important is knowing your device. MFD manufacturers are offering more and more options for connectivity, such as Bluetooth, Wi-Fi direct, or NFC printing. Of course all of these features are nice, but from a security standpoint, they add to the complexity and risk surface. Make sure you know the capabilities of your devices, and you know what risks you're open to.

Physical Security

The physical location of a printer is also as important as the logical network location. Printing productivity can be seriously hampered if printers are constantly exposed to physical damage due to placement in insecure public areas.

Locating printers in places accessible only by authorized users is a simple way to reduce the risk of security breaches.

Campus and school locations can be particularly vulnerable, especially where printers are accessible by the student population. Additional physical security measures that may be taken include:

- Securing the printer to the building, to prevent theft
- Disabling the inbound USB port(s), to prevent direct printing over USB, or direct access to the printer hard drive.
- Protecting the network connection. For example, some sites even use super-glue to secure the network cable in place.
- Locking the paper trays

Device Access

Modern MFDs and printers can be thought of as Internet of Things (IoT) servers and are vulnerable to a range of IoT attacks. All modern devices are shipped with a rich set of protocols and services, most of which may never be used by your organization. To reduce the surface area of attack, we recommend turning off any unused device protocols and services.

Ensure default administrator passwords are periodically changed and use secure passwords for machine settings, such as IP address, to prevent alteration by users or malicious code on the network. Often, factory default passwords are well known to hackers, leaving devices highly vulnerable to attack.

Many devices allow print jobs to be stored on an internal hard disk or internal memory for re-printing. If this feature is used, clear policies are needed to ensure that only public documents are stored, or that documents are adequately password protected. In many cases, it may be prudent to disable this feature. Alternatively, if you do not want to store jobs for re-use, most MFDs provide a data overwrite feature. This allows print data to be overwritten or removed, either immediately, on demand, or at scheduled intervals.

Many modern MFDs have a feature to encrypt all partitions of the hard drive that might contain customer data with Advanced Encryption Standard (AES) encryption. You should ensure this feature is enabled.

Some MFD manufacturers bundle these features (print job deletion, data overwrites and data encryption) into Data Security Kits which may be optionally purchased. If you need these features, you must ensure the appropriate Data Security Kit is purchased and installed.

Two-Factor Authentication

MFDs and some printers provide for user authentication at the device through card swipe, ID number or other methods. This is an important safeguard to prevent unauthorized access to a device.

Two-factor authentication provides an additional layer of security by requesting a user for additional authentication information. PaperCut MF, for example, provides for a PIN number to be entered as the second factor to authenticate a user after swiping their card or entering their ID number.

Firmware

Printer manufacturers are becoming increasingly conscious of security and are actively updating their firmware to address security issues reported against their devices. A practice of regularly updating device firmware is needed to ensure you benefit from any security fixes from the manufacturers.

The cryptographic technology on MFDs varies and sometimes lags behind current best practice. However the industry is becoming more security

aware and keeping your MFD firmware up-to-date is important to ensure your MFDs use the most up-to-date ciphers available for the device.

Older ciphers, such as RC4, are susceptible to security breaches. By default, PaperCut MF is configured to support a wide variety of SSL ciphers for compatibility purposes. PaperCut is bundled with a recent version of the Java SE Runtime Environment, which incorporates the latest security fixes from Oracle. When PaperCut connects to a device, the two communicate and pick the most secure cipher that is mutually supported.

2.4 Print Management Solution Security

Regardless of which product you choose to account for or control your printing (naturally, we recommend PaperCut NG or PaperCut MF), there are some considerations and recommendations we would make here as well.

Sensitive information should be secure while being transmitted between the application components. Check for protocols such as HTTPS being supported when accessing administration interfaces and between embedded applications and servers.

Data that is stored, is also an important consideration. Are you free to use and secure a database of your choice and manage backups to your organization's standards?

PaperCut NG and PaperCut MF were developed from the ground-up with security in mind. With a strong heritage in the education market, the software has been battle-tested and security-hardened over years of student attacks at schools and universities around the world.

PaperCut retains a strong security culture, with both proactive and reactive security practices built into our company's processes. We regularly review third party components for security vulnerabilities. All incoming security reports are immediately reviewed by our PaperCut Security team. Any mitigating or defensive workarounds are put in place and fixes implemented and published typically within days.

We respectfully recommend you look for strong security credentials with any print software you introduce into your workflow.

Specific security hardening measures used by PaperCut NG/MF and other security minded solutions include:

- **Process isolation** — print management software should run in isolated processes away from the operating system kernel. Processes should run under the minimum necessary user privileges. For example, it should not be necessary to run long-running tasks under the root or administrator user.
- **Secured APIs** — public APIs should have multiple layers of security. PaperCut uses authentication tokens coupled with IP address filtering to ensure that API calls are properly authenticated and are from a trusted source.
- **Code signing** — your installers and code should be code-signed by the vendor to give assurances that you are running unmodified code that is authored directly by the vendor.
- **Sandboxing** — when there's even a small risk that aspects of the solution could become compromised, we work to engineer the solution to anticipate the threat and contain any damage. Sandboxing is one method where VMs, or process-level isolation techniques, are used to add layers into the system so that a compromise in one area/ component does not open up a whole system.
- **Secure web pages** — web pages should have built-in protections against SQL injection, Cross-Site forgery and Cross-Site Scripting attacks.
- **Directory Services** — (such as AD, LDAP, etc) should be leveraged to authenticate users in preference to storing passwords in the print management system. If users are defined outside a directory service (e.g. guest printing accounts), the password should be securely encrypted. PaperCut NG/MF uses Bcrypt for this purpose.
- **Fail-Closed Design** — an important security principle is to shut down access, such as the network connection from an MFD to the authentication server, whenever a failure occurs. With a "fail-open design", a simple action like removing a network cable, could render a device open to attack. PaperCut NG/ MF uses a "fail-closed design" as a core design principle in all print security areas.

Maintaining a Secure Print System

It is important to recognize the business critical nature of your print infrastructure and apply standard IT best practices to your print systems, including your print management system. Some examples of best practices include:

- Regular security audits to ensure vulnerabilities to print exploits have not crept in.
- Regular backups of print management databases.

- Maintenance and patching of your print management software.
- A tested Disaster Recovery Plan.

3.0 Securing Print Workflows

While your infrastructure may be hardened against attack, your printing workflows may leave you wide open. We present a range of secure print workflows that are easy to implement and highly effective.

3.1 Print Policy

What are the right print policies for your organization? Should print jobs printed out of normal business hours be allowed? Should certain users have restricted printing permissions? Once you have a clear idea of the policies you need to implement, you can then focus on implementing these policies and business rules.

North Shore High School would like to allow their students to print some documents for free, but only during class time, and only selected documents. The best way to implement this is for teachers to approve (or deny) all student printing. Using PaperCut NG/MFs print policies, North Shore High School can enforce the use of a teacher's approval code for all student print jobs.

Implementing business printing policies can take many forms. Printing out key policies and distributing them prominently across your organization can be a useful exercise, but does not guarantee that all employees and guests will follow this guidance. An application like PaperCut NG/MF allows an organization to implement these print policies and business rules automatically, via built-in and customizable recipes.

3.2 Secure Print Release

In a standard printing environment, print jobs are sent directly to the printer for immediate printing. A large proportion of these jobs are typically not required and end up left on the printer or put in the waste bin. Any jobs not collected immediately are a security risk, if the documents are sensitive or confidential.

Secure Print Release is a simple solution that places jobs in a holding state until the user authenticates and releases the job at the printer. Users should be able to either manually select jobs to release or have jobs automatically print after successful authentication. Sensitive jobs will then not sit uncollected at the printer!

Secure Print Release, sometimes also called mailbox printing, is an important feature to consider when designing your print workflow. This feature allows the user who printed the document to release the document only when they are physically located in front of the MFD or printer. Most MFDs support this functionality. However, to achieve a consistent user experience across your fleet of devices, a print management solution, such as PaperCut NG or PaperCut MF, is recommended.

PaperCut NG and PaperCut MF also offer Find-Me printing. Find-Me printing provides a roaming print solution where users print to a single queue. All print jobs are then "pulled" to the specific printer at which a user identifies herself, e.g. by swiping an access card.

Print Release Example:

Stephanie White from White & Turner Legal Services has sent a confidential contract to a printer. After she has sent the document, a colleague stops by for a chat so she cannot get to the printer straight away. With Secure Print Release, she is not concerned as she knows the document will not be printed until she releases the document at the printer.

3.3 Prevent the release of print jobs to a printer in error

Secure Print Release is an essential capability of a secure printing environment. But what happens when jobs are released to a printer that is in an error state? For example, a printer that has a paper jam or is out of toner? What would happen if the printer error got resolved, and these jobs started printing automatically in the absence of the authorized user? These jobs should not print automatically when the printer error is resolved after the user has walked away.

PaperCut NG/MF offers the ability to prevent the release of jobs when a printer is in error. When the printer error is resolved, the user must then re-release the job, thus giving control back to the user about when their job prints and eliminating the possibility of sensitive data being leaked.

3.4 Job Timeout

Print output left sitting in a printer tray is not the only way sensitive print data can be accessed by someone other than the owner. Spool files stored on the print server waiting to be released may also be viewed if accessed by malicious individuals. While the measures outlined in the "Securing the Print Infrastructure" section can help protect against this, jobs should be automatically removed from the hold release print queue after an appropriate period of time. This also allows you to reduce the load on your print server and save paper and toner by eliminating printing of jobs that are no longer needed.

PaperCut NG/MF allows you to define how long a print job stays in this hold release print queue before it is automatically deleted.

3.5 Accountability to the User

There is nothing like knowing that what you print can be tracked and audited to prevent people from printing their favorite thesis on whether Captain Kirk or Captain Picard is the better captain in Star Trek, including all 55 full color pages of the Starship Enterprise schematics!

While this capability is available through operating system audits (e.g. Windows event viewer), it can be a manual, time-consuming and error-

prone process. PaperCut NG/MF allows you to centrally manage this process for all devices and users.

PaperCut NG/MF allows you to share some or all of a user's printing history with them in several ways. You can simply share their print history with them or you can quota their printing ability and have them initiate a request and justification for more printing once they hit their limit.

3.6 Print Privacy

Gossips are relentless. The last thing you want is to have weeks of secretive work all undone because the document titled "Surprise Employee Bonuses.docx" is seen sitting in a print queue, waiting to be printed! Where possible, you should hide your sensitive data.

While you could solve this via a complex LPD/LPR setup, Papercut NG/MF allows you to hide the document names either at an individual print queue level or across your entire print server. Your employee surprise bonuses will remain a surprise now!

4.0 Securing Printed Output

Keeping information secure is never easy, but it gets a whole lot harder once in printed form! All's not lost, however, as there are several technologies and best practices available that can significantly improve the traceability and security of printed documents and prevent document theft.

As users are in control of printed documents, security measures for printed documents must effectively drive user behavior. For example, a policy document sitting in a drawer is unlikely to prevent a private medical record being left behind in the hospital cafe. But if the medical record contained a prominent digital signature that could easily trace the document owner, more care would be taken by that person before printing the material and abandoning it at a public place.

Document security best practice is to use a range of complementary measures, which include:

- Audit trails and reports of printing activity
- Watermarking and digital signatures
- Electronic archiving of printed documents

4.1 Audit Trails and Reports of Printing Activity

A secured print system should keep a comprehensive record of all user print jobs. This should include information identifying the user who printed the document, the document name, the computer used to generate the print job, the output device, and the date and time of printing.

The existence of this audit trail enhances accountability and traceability, and encourages users to act with integrity.

PaperCut NG/MF retains detailed information in logs and archives. In addition, PaperCut NG/MF offers a wide range of audit reports detailing all transactions that have occurred in the system.

System Activity

PaperCut retains detailed system level information in the following logs:

- <u>Audit logs</u> — all operations against user accounts are recorded in an audit log. These audit records capture the date, details, and the user who performed the operation.
- **Application log** — PaperCut NG/MF retains a complete history of system events including, errors, notifications, alerts, new printers or devices, etc.

User Activity

At the user level, PaperCut NG/MF provides the following logs to track user activity:

- **Job log** — a log of all the print, copy, fax, and scan jobs, capturing information about the user, date, and details for each job.
- **Transaction log** — a record of all the financial transactions, including print job charges and account balance transactions.

Reporting

Regular, scheduled reports can be used to alert administrators of unusual printing behavior or contravene an organization's printing policies.

PaperCut NG/MF offers a wide range of comprehensive <u>reports </u>that can be generated on demand or automatically emailed to management on a daily, weekly or monthly schedule.

4.2 Watermarking and Digital Signatures

Watermarking is a technology that augments a printed page with text added at the time of print. A watermark may contain information such as the user who printed the document, the date on which it was printed, and the printer used. In this way, watermarking can act as a reminder to users that the source of a document can be identified and traced back to them.

Printed by sally at 08/12/2010 3:46:43 PM   (659d08164bd030cf4b7d9d68acab02e0)
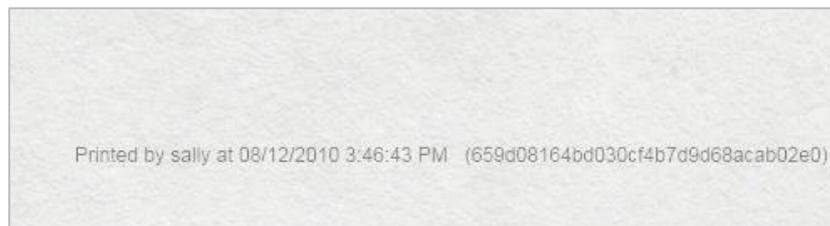
A digital signature is a digital code uniquely generated by taking various print job attributes, such as print time, username, printer name, and document name, and combining them with a secret key. A digital signature applied to a printed document as a watermark can be used to quickly trace a printed document back to a specific entry in the print audit log.

Best practice printed document security combines these three features — watermarking, digital signatures, and a comprehensive print log — to provide full traceability and security of printed documents.

PaperCut NG/MF enhances document security by providing all three features, working in tandem — <u>watermarking</u>, <u>digital signatures,</u> and a comprehensive <u>print log</u> searchable by digital signature.

Watermarking Example:

Damien Turner from White & Turner Legal Services has been working on a high profile divorce case, but much to his horror, has discovered that details of the proposed settlement have been leaked to the press. The magazine in question has provided the source document and because White & Turner Legal Services use PaperCut's digital signature watermarking functionality, which automatically prints a secret key on all documents, Damien is able to identify when and where the document was printed and more importantly, who was responsible.

4.3 Electronic archiving of printed documents

Observing document retention requirements, e.g. <u>HIPAA</u> compliance, is a huge burden on many companies. Maintaining printed archives is both expensive and time-consuming. Automatic electronic archiving of all printed documents is an attractive solution.
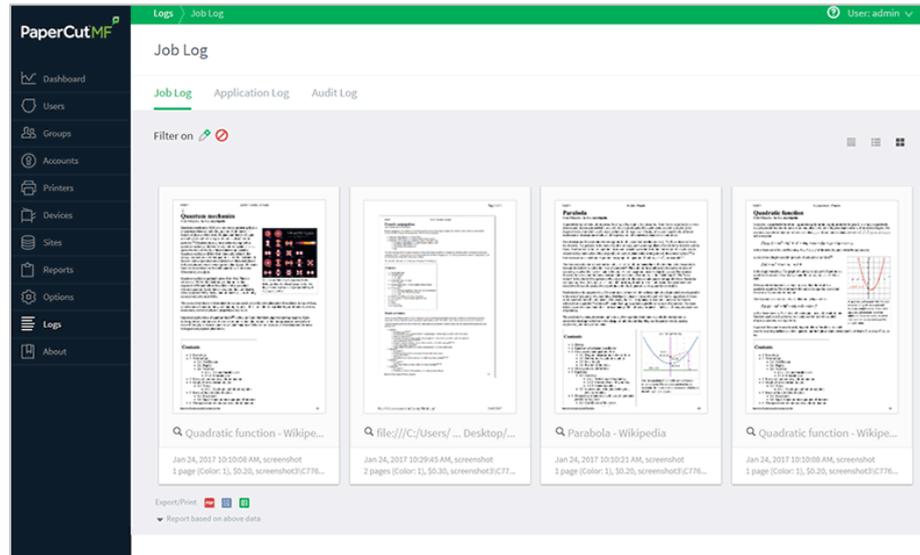
The ability to electronically archive printed documents also adds another layer of print output security. With electronic archiving, the print log is augmented by an image of the printed document, allowing for complete traceability. For example, an archive can positively identify who printed an incriminating or offensive document, since the print logs includes the contents of the print output.

PaperCut NG/MF's Print Archiving empowers approved administrators to browse and review the content of print activity within their environment. Alongside the powerful tracking and reporting functionality built into PaperCut NG/MF, this gives system administrators a wide range of auditing capabilities, such as:

Storing historic records of all printed content.

- Viewing past print jobs in a web browser.
- Having fined-grained access control to archived content.
- Downloading the original spool file for reprinting with 100% fidelity.
- Enabling or disabling archiving for selected printers and users.

Archiving Example:

When Stephanie was at the printer, she noticed another print out of a rather offensive image, but had no idea who had printed it. With electronic archiving, the System Administrator can track down the culprit. The SysAdmin can view an image of every print job to identify the one in question, and once the job is identified, can see who was responsible for printing offensive material in the workplace.

5.0 Summary

Practical and proven methods are available to secure your print system. We recommend a multi-layered security strategy that addresses vulnerabilities before, during, and after each document is printed.

Securing your print infrastructure, through defensive network configuration, secure print queues and protecting device access will help ensure you have a robust print system even before the first job is printed.

Securing your print workflows through print policy, secure print release, and managing jobs released to a printer in error, are effective and widely used tools with the out-of-box solutions readily available.

Securing your print output using a combination of print audit logs, watermarking with digital signatures and electronic archiving, will help drive correct user behavior and force accountability for printed documents.

A comprehensive print management solution, such as PaperCut NG and PaperCut MF will help organizations implement many of these best practices in a cost-effective way to achieve a secure print system. Of course, the print management software must have its own strong security credentials.

Additional up-to-date information may be obtained from PaperCut's web site at:

http://www.papercut.com/kb/Main/Security

Please contact PaperCut support or your local PaperCut reseller if you have specific questions not addressed by this white paper or the online documentation.

PaperCut

✅ Print Security Checklist
Use this checklist to assess the security health of your print system:

1. Securing Print Infrastructure

- [ ] Is there secure network communication between the end user and the MFD?
- [ ] Have you separated the print server from the network to protect traffic from interception?
- [ ] Are you monitoring and investigating any packet sniffing or port scanning behavior on the network?
- [ ] What happens to your print data during network outages?
- [ ] Are you hiding document names in your print queues?
- [ ] Have you disabled the USB ports on MFDs to prevent someone from scanning to USB devices?
- [ ] Has all unused MFD functionality been disabled?
- [ ] Have you applied all patch updates and do you have a security patch update procedure that tackles the latest vulnerabilities as they happen?
- [ ] Is there any sensitive network information stored in your MFDs? Are device passwords (such as the admin password) updated and secure?
- [ ] What happens to your devices at the end of their life? Does the hard drive and internal memory of every printer get erased and securely disposed of at the end of its life? Are you adhering to industry standards, such as specifications established by the US Department of Defense (DoD)?
- [ ] Has your organization invested in any Data Loss Prevention (DLP) technology? If yes, how is this complemented or compromised by your print security?
- [ ] Are the same print security settings employed consistently across all devices from desktop PCs, to tablets and smartphones?
- [ ] Are your MFDs secured or located in a position where CCTV cameras or people can view them so that malicious activity can be both detected and deterred?

2. Securing Print Workflows

- [ ] Can anyone (even a visitor) walk up to your MFDs and copy, scan, or fax any document?
- [ ] Can they scan any document to a folder, email, or fax?
- [ ] Are printed jobs left unattended in the output trays of printers and copiers?
- [ ] Can users bypass the system and print directly from a print server or a local queue on their computer to the IP address of a printer?
- [ ] How are you encouraging and enforcing your print policies?
- [ ] Are you enforcing a secure print release policy?
- [ ] Have you enabled print job timeout for older documents on your print server?

3. Securing Printed Output

- [ ] Do you maintain an audit trail of print, copy, scan, and fax activity? That is: who, what, when, where, and how?
- [ ] When archiving documents, are you using a file format that allows for long-term preservation?
- [ ] Do you use watermark technology to help classify sensitive documents and highlight what is vulnerable? Do you use digital signatures to identify who printed a document?
- [ ] Have all end users been adequately trained, not only in how to use a print system, but also on what your organization's print policies are, and the impacts of policy breaches to your organization?

Thank you

Authors:

Chris Dance (CEO, PaperCut Software)
Geoff Smith (Head of Development, PaperCut Software)
Anthony Nicola (Head of Support, PaperCut Software)
Damien White (Global Technical Services Manager, PaperCut Software)

Contributors:

Mark Hart (ACDI – Director of Business Development / National Accounts)

PaperCut HQ
sales@papercut.com
www.papercut.com

Support
support@papercut.com
www.papercut.com/support