July 2016

The Future of Enterprise Printing

Securing Hardcopy Documents in the Digital Age

Yash Sunit Joshi

The Future of Enterprise Printing

Securing Hardcopy Documents in the Digital Age

Despite technological advances, the printed document is still the predominant form of trusted communication. Unfortunately, the printed document is inherently insecure: well-known security mechanisms such as firewalls and passwords do not apply in the hardcopy space. This article presents some considerations for secure enterprise printing, chiefly focusing on the often-neglected domain of hardcopy document security, and proposes a framework based on Recommendation X.800 of the International Telegraph and Telephone Consultative Committee (CCITT/ ITU-T). This article also describes how CrimsonLogic's Phidélity product suite forms the basis of a comprehensive and secure enterprise printing solution.

FOR ALL THE ADVANCES that electronic communication technologies have made over the past few decades, the printed document is still the predominant form of trusted communication in today's world [1]. Unfortunately, our reliance on the hardcopy comes with a downside: hundreds of security breaches such as unauthorized printing, document theft, document counterfeiting, and document leakage are reported yearly [2]. Security, which has become increasingly central to information technology in recent times, is also a prime concern in the context of the printed document.

The printing industry has long embraced secure printing for high-value items such as banknotes, passports, and postage stamps. These items, and the processes used to manufacture and store them, are made highly secure through the use of physical access control, customized printing substrate, and special-purpose equipment for the reproduction of features such as holograms and intaglio [3].

Many other industries also deal with sensitive hardcopy documents but do not commonly use banknote-like special-purpose features, owing largely to cost considerations. On the other hand, cloud-based printing, while gaining traction, is associated with several risks [4] [5] and may not prove suitable for sensitive content. It is clear that secure enterprise printing is a problem that needs a major re-think for today's business environments.

Two key considerations apply. Firstly, some of the techniques used to protect high-value documents have in recent years become available in commercial printers that use digital platforms such as PostScript; the capabilities of such platforms can and should be exploited to

the fullest. Secondly, the adoption of secure printing among enterprises can be accelerated by building on the existing printing infrastructure and ingrained user behavior that are characteristic of an enterprise environment.

There are already several innovative solutions on the market that counter specific threats; this paper describes a framework to unify these disparate security mechanisms. Quocirca's 2011 report entitled "Closing the Print Security Gap" [1] stated that "the market landscape for print security is complex with little standardization, characterized by a mix of hardware capabilities and proprietary software… although larger enterprises are stepping up their efforts to improve their protection, many companies have much work still to do". The situation persists to this day; the utility of such a framework is thus evident.

A Framework for Secure Enterprise Printing

CCITT Recommendation X.800 [6] lays down the Open Systems Interconnection (OSI) security architecture. The OSI architecture provides a systematic framework focusing on security threats, attacks, mechanisms and services. These can be defined briefly as follows [7]:

- Threat: A potential violation of security.
- Attack: Any action that compromises the security of information owned by an organization.
- Security mechanism: A process (or a device incorporating such a process) that is designed to detect, prevent, or recover from a security attack.
- Security service: A processing or communication service that enhances the security of the data processing systems and the information transfers of an organization. Security services are intended to counter security attacks, make use of one or more security mechanisms, and implement a security policy.

In the information security landscape, threats include spoofing, tampering, repudiation, information disclosure, denial of service and elevation of privilege [8]. While *electronic* documents such as PDF files are stored as data and as such are concerned with precisely these threats, we realize that the *printed* document is different. Narrowing our concern to the more specialized domain of hardcopy document security, we distinguish more specific threats faced by enterprise documents during and after the printing process. The following threats are identified [1]:

1) *Unauthorized printing* circumvents copyright, leads to the wastage of supplies, and vastly increases the probability of paper-related security breaches.
2) *Electronic eavesdropping*, or 'wiretapping', can lead to the disclosure of print job information while it is under transmission from workstation to printer. If the document is

generated via a web application, it is also vulnerable to interception while under transmission from the server to the workstation.

3) *Document theft.* Once printed, the document hardcopy can be stolen or inadvertently taken by an unauthorized party. This is especially likely to happen when the printout is left unattended at the printer.
4) *Document counterfeiting* refers to the unauthorized replication of a document, typically using optical reproduction techniques such as photocopying.
5) *Document forgery* refers to the unauthorized modification of a document, for instance changing a '3' to an '8'. It can also refer to the creation of a fresh 'fake' containing unverified data, e.g. a forged passport.
6) *Document leakage* refers to the disclosure of potentially confidential printed information to an unauthorized party, whether unknowingly or maliciously.

The following table lists these threats and describes security services that can counter them, along with the security mechanisms that may be used by each service. As far as possible, we retain X.800 terminology.

Threat	Security Service	Security Mechanism
Unauthorized printing	Print Authorisation	Controlled printing, print audit trail
Electronic eavesdropping	Print Job Confidentiality	Print job encryption
Theft of printout	User Authentication	Authenticated pull-printing
Document counterfeiting (reproduction)	Document Authentication	Copy-fragile printed structures
Document forgery (faking or tampering)	Document Integrity	Signed barcodes, lens-based controls, deliberate errors, latent images
Document leakage	Origin Authentication	Document tracking

Table 1: Hardcopy Document Threats, Security Services and Security Mechanisms

Controlled printing refers to the ability to restrict the number of copies of a document that can be printed by a given user. The document creator or administrator must be able to limit this

number; such a mechanism protects copyrighted works, prevents wastage and strengthens security.

A *print audit trail* acts as a deterrent to the unauthorized or malicious user by recording the sequence of system events during the printing process, and typically capturing the user accounts and machines responsible for each event. Such a log provides both a record for forensic examination and a way to track printer fleet usage for billing and analysis.

Encryption is a well-known method to ensure confidentiality and prevent eavesdropping and man-in-the-middle attacks. Print job data should be encrypted when sent across a network. Furthermore, the user should be authenticated at the printer before the printout is dispensed in order to ensure that documents can only be printed by their actual owners. Such *authenticated pull-printing* typically uses a password or smartcard and helps to prevent theft and reduce wastage.

Manual signatures are the traditional form of authentication, but they are insufficient in today's world: high-quality reproduction and skilled forgeries have rendered the old-fashioned signature practically obsolete. *Digital signatures* provide authentication through public-key cryptography, and can be embedded in the printed document through information-carrying printed structures such as barcodes. Digital signatures also ensure the integrity of the document, since the signature is typically derived from a hash of the document content.

Visual cryptography or *screen-angle modulation* can be used to authenticate a document through a customized lens. Other difficult-to-reproduce features such as *deliberate errors* and *latent images* further strengthen the document against forgery. *Copy-fragile printed structures* such as watermarks and microprint can reveal unauthorized attempts to copy a document, since the appearance of these structures in a photocopied document differs from the original.

Finally, after a document is printed, it should be *traceable* to its creator – the ability to identify the original requestor of a printout is critical in forensic investigations of leaked documents. Such traceability necessarily requires information to be embedded in the printout, but a prominent identifier or information-carrying structure may easily be removed or defaced. Subtler methods of information embedding could possibly use background patterns or content manipulation.

The Secure Printing Pyramid

The above security mechanisms form a 'pyramid of requirements' for secure enterprise printing as shown below. Given the nature of the enterprise market, it is imperative that the existing

printing infrastructure and ingrained user behavior be unaffected by the introduction of a secure printing solution – this forms a solid 'base' for the pyramid.

The 'building blocks' of the pyramid are controlled printing, authentication and authorization, secure pull-printing, print job encryption and the print audit trail.

The printed hardcopy must also be secure. The capstone of the pyramid is the ability to verify the originality and integrity of a hardcopy document, which is essential in building trust among partners and customers, coupled with the ability to trace the document to its owner, which is essential in guarding against leakage and establishing accountability.

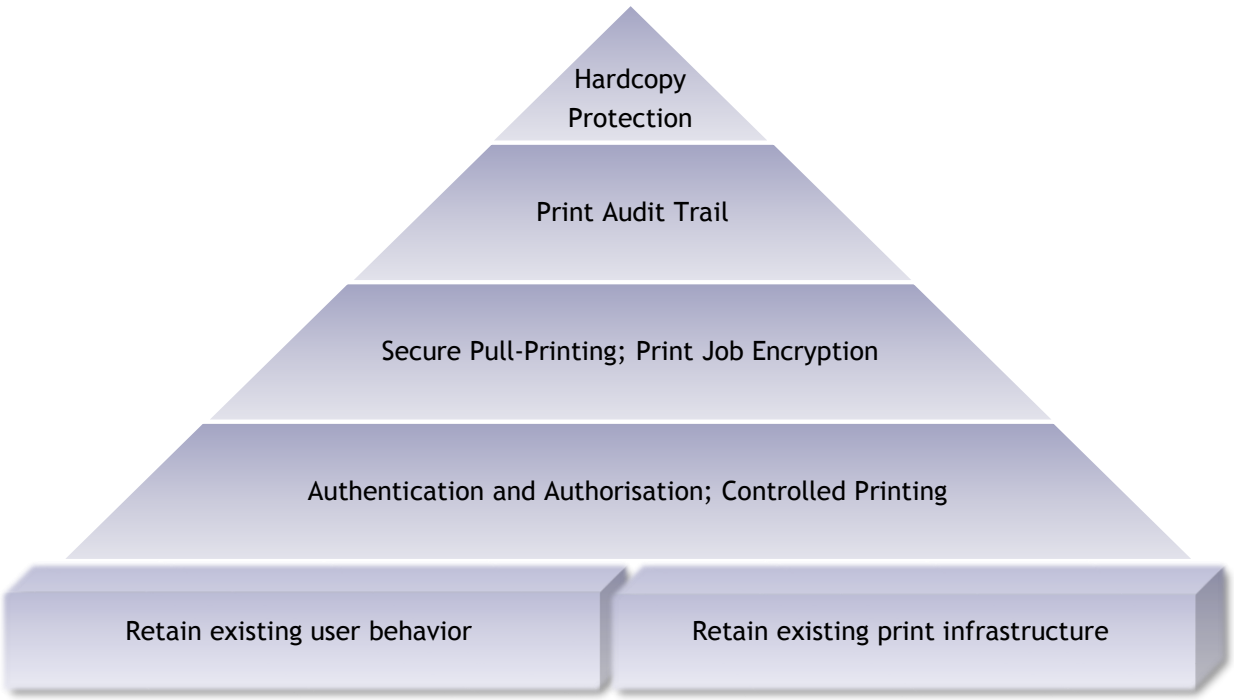

Figure 1: The Secure Printing Pyramid

Phidélity Product Suite

Integrating advanced security technologies with innovative ideas, CrimsonLogic's Phidélity product offers a powerful and flexible secure printing solution using only normal paper and a typical office printer with regular toner. Phidélity's functionality can be accessed using a virtual

printer driver that appears as a regular printer on the client machine. Alternatively, Phidélity can be integrated seamlessly into an existing document-generating web application, in which case it can also provide controlled client-side printing through the Print Control front-end and restrict the number of copies printed. Phidélity also integrates with a variety of print output management components to provide pull-printing capabilities.

Phidélity's Optical Watermark and Microprint can reveal unauthorized attempts to copy a document, since the watermark and microprint on a photocopied document differ from those on the original.

The CryptoMark, based on a form of visual cryptography, can be used to authenticate a document through a customized lens. Phidélity's SecureCODE is a 2-dimensional barcode that holds digitally-signed document data to authenticate the document and protect against tampering. The SecureCODE can be verified using a mobile app or web interface, and alterations to the document can be detected by comparing the printed information with the contents of the SecureCODE.

Phidélity also provides a variety of customizable anti-forgery structures including intentional artifacts, discontinuous lines, and deliberate errors. These non-obvious features are easily overlooked by a forger and are difficult to reproduce using conventional methods.

ID-Trace inserts a covert but traceable identifier into the printed document. The identifier can carry dynamically-captured information such as the identity of the print issuer, the date and time of printing, or the IP address of the issuing machine, or alternatively act as an index to a database that holds such information. If a leaked page is obtained, the identity of the original document holder can be traced via the identifier, allowing for the necessary follow-up action.

Phidélity Secure Printing Solution: Solving real business needs

Print Secure Documents Conveniently - Protect against counterfeit, forgery and leakage with no change required in end-user behavior.

Achieve Cost Savings - Ensure responsible printing by reducing print wastage and unclaimed printouts, minimizing operational expenditure.

Enhance Credibility - Ensure the authenticity of documents, building trust among partners, customers and other relevant stakeholders.

Comply with Standards - Help companies to comply with regulatory requirements, such as the Sarbanes-Oxley Act (SOX) of 2002.

Industry Focus

Government - Agencies that issue licenses, certificates and stamp duty documents.

Financial Services, Banking and Insurance - Firms that issue or use trusted policies, letters of credit, statements and/or contracts.

Legal - Judicial bodies and legal firms that issue or use notarized documents, legal contracts and agreements of all types.

Trade and Logistics - Secure cross-border documentation including bills of lading, air waybills, clearance permits and certificates of origin, and commercial trade documents such as invoices, purchase orders and delivery orders.

Education – Universities and private educational institutes issuing degree or diploma certificates, marksheets, transcripts, and examination papers.

References

[1] Closing the Print Security Gap: The Market Landscape for Print Security, Quocirca, 2011

[2] 2012 ITRC Breach Report, Identity Theft Resource Center, http://www.idtheftcenter.org/ITRC%20Breach%20Report%202012.pdf

[3] Glossary of Security Documents, Security Features and other related technical terms, The Council of The EU

[4] M Mowbray, "The Fog over the Grimpen Mire: Cloud Computing and the Law", (2009) 6:1 SCRIPTed129, http://www.law.ed.ac.uk/ahrc/script-ed/vol6-1/mowbray.asp

[5] David Talbot, Security in the Ether, MIT Technology Review (2009) http://www.technologyreview.com/featuredstory/416804/security-in-the-ether/

[6] Security Architecture for Open Systems Interconnection for CCITT Applications, CCITT Recommendation X.800

[7] Cryptography and Network Security Principles and Practices, Fourth Edition, William Stallings

[8] "Uncover Security Design Flaws Using The STRIDE Approach", Shawn Hernan, Scott Lambert, Tomasz Ostwald, Adam Shostack http://msdn.microsoft.com/en-us/magazine/cc163519.aspx

[9] Governing for Enterprise Security, Julia Allen, June '05. Carnegie Mellon Univ. Tech. Note CMU/SEI-2005-TN-023

[10] 'Security Fix', Brian Krebs on Computer Security, Washington Post http://voices.washingtonpost.com/securityfix/2009/12/paper_data_breaches.html