SafeCom™ Security

Enables any private or public organization to use cost-effective network printers without putting document security at risk

Passwords and firewall appliances are today the primary ways of protecting confidential data within an organization. Protecting the corporate network often means limiting access to file servers and PCs. But when it comes to document confidentiality, it is not enough to control the network. What happens to document security after users press the print button?

> ″ Industry analysts estimate that in-house security breaches account for 70% to 90% of the attacks on corporate computer networks. And the percentage is probably even higher than that because most insider attacks go undetected. People are ignoring their biggest threat. The attention given to hackers by the press is what gets the attention of upper management, and that's what they base their security purchases on. People need to be worried about the insiders because they know how to hurt the organization specifically, drastically and quickly ″

John O'Leary
Director of Education at the Computer Security Institute in San Francisco

> ″ When you look at buying trends, it's mostly geared for maintaining a secure perimeter. Almost everybody has antivirus software, firewalls and VPNs. But people would do well by their money if they thought about policy access management software, and tracking and monitoring devices . . . They've got to think about a different kind of security ″

Network World, 05/08/00.

> ″ Networked printers are known to be especially vulnerable to hacking attacks. They have their own IP addresses, and they run various standard protocols that can be exploited. To make matters worse, printer vendors haven't added any strong security features to their products that would protect them against break-ins ″

Data Communications 06/17/99.

″Top Secret - Confidential″
A document with this heading on a departmental printer is certain to catch the interest of colleagues using the same printer. One of the best sources of confidential information is the output tray of network printers. There is also the risk that when you reach the printer to fetch your document, someone else has mistakenly picked it up and your confidential work could be circulating for everyone to see.

SafeCom™

SafeCom™

Confidentiality of printed documents is a prime concern of many organizations today, private as well as public. There is an increasing pressure on organizations to protect the privacy of clients, customers, citizens or patients, as well as a growing demand to restrict insider trading by limiting staff access to confidential information. On the other hand, there will always be a need to print confidential documents and distribute them to decision makers within the organization without compromising convenience.

So as printer networks become more extensive with more users and open standards, a growing challenge is faced by organizations: guaranteeing the overall confidentiality of the printed document.

Different print security solutions are available on the market. However, they are only available on selective printer models. There is a need for security solutions that are printer independent and ease administration. The lack of sufficient security facilities often prevents a printer from being placed where there is easy access to it. Who has not come across awkward solutions like a locked output tray, a locked printer room or simply personal printers for everyone? When it is not possible to have a secure printing area, it is quite simply every man for himself. The ”Print & Run” concept is well known to anyone who has printed a confidential document on a network printer!

SafeCom™ ensures document and print security at more than one level

With the unique pull printing system and personalized identity cards, SafeCom™ enables any private or public organization to use cost-effective network printers as personal printers - without putting document security at risk.

Encryption

Strong encryption methods ensure secure passage from PC to paper. Data is encrypted using TwoFish 128-bit encoding (cipher, symmetrical key) and the key exchange system is RSA 512-bit (asymmetrical key). As soon as the print button is pressed on the workstation, all data is encrypted before being transmitted from the individual workstation, via the server, to the printer itself. The secure SafeCom™ Client submits print data and transfers it between devices using encryption and key exchange mechanisms. Decryption is carried out at the printer interface which is installed on the parallel port connection of the printer, or in the built-in I/O card. As a result, it is impossible for unauthorized users to access information anywhere in the system.

Personal cards and PIN code

With SafeCom™, printing has become a pull rather than a push process, providing guaranteed confidentiality of the printed document until retrieval by the user. Print jobs are stored as encrypted data in a server until the user releases them with a personal identity card and PIN code, from any SafeCom™ equipped network printer. When the personal card is swiped through the SafeCom™ reader, the user has access to his/her print jobs and the SafeCom™ management options. These options provide extended command of the print jobs, e.g. delete, retain or additional copies.

The PIN code is an optional feature and can be used as an extra level of security. It enables the administrator to decide if the PIN code is necessary for some or all SafeCom™ users.

SafeCom™ - The Only Way to Safe and Convenient Print

idl-data
14, Chemin de Tramerolles
FR - 91720 Gironville-sur-Essonne
France
Téléphone: + 33 (0)1 64.99.52.29
Fax: + 33 (0)1 64.99.30.59
e-mail: sales@idl-data.com