Lexmark PrintCryption™ Card Assures Security of Confidential Print Jobs

Hardware option encrypts data at computer, decrypts at printer for privacy

White Paper
October 2002

Executive Summary

Safeguarding information is a fact of life. Whether it's the password to your e-mail account, the key to your home's front door or the personal identification number for your ATM card, you use these mechanisms to keep sensitive information private and secure.

Printing documents is no different. In today's networked environments, where computer and printer may be hundreds of feet or even hundreds of miles from each other, assuring the security of print jobs along every foot of wire, or from one end of the Internet to the other, is a fundamental—and growing—concern.

The challenge

Imagine financial reports, salary reviews, budgets, bank statements, contracts, or corporate restructuring plans falling into the wrong hands. The results could be disastrous, both financially and legally. Keeping confidential materials out of the wrong hands is a concern faced by all organizations, public-sector and private, regardless of size, line of business or number of employees.

As internal corporate networks and the Internet have grown, they have evolved simultaneously into a fertile ground for legions of hackers, crackers, disgruntled employees, and others who are, at best, merely gaining access to unauthorized data purely for sport, or, at worst, bent on criminal action. Indeed, it is with almost mind-numbing regularity that we read news accounts reporting the outright theft or malicious alteration of financial or medical network-based data.

Given that cyber-intrusion occurs and that the pilfering of data streams can never be prevented completely, the logical course of action is to make these data streams useless to prying eyes. The technique is a model of simplicity: scramble the data at its point of origin and descramble it at its destination. Banks long ago adopted this approach, ensuring that customers' account numbers, balances and PINs are never exposed "in the clear" as their ATM transactions travel between a remote teller machine and the faraway mainframe computer on which the card holder's account resides.

Elegant solution

Responding to the growing concerns expressed by customers, Lexmark's engineers developed the Lexmark PrintCryption Card, a device that addresses these issues by safeguarding the security of print jobs. The card is a firmware option that installs inside Lexmark's T52x and T62x series network printers and MFPs and works over any wired or wireless network running TCP/IP: LANs, WANs, intranets, extranets, and the Internet.

Each time a mainframe or UNIX workstation creates a print job, an encryption program running on it initiates a communications session with the destination printer's Lexmark PrintCryption card. Both computer and printer agree on a randomly generated encryption key, essentially a complex password of 128, 192 or 256 bits in length. Keys are generated in accordance with the Advanced Encryption Standard, a federal standard that became effective on May 26, 2002. The computer uses this key to encrypt the print job and then route it over the TCP/IP network to the printer.

As the print job traverses the network or Internet, it is no less vulnerable to pilferage than before, but now it cannot be interpreted by any other device—or person. Only a Lexmark printer equipped with a PrintCryption Card that is programmed with the identical key can decrypt the data, transforming it back into a useable print job. When the print job arrives at the printer, the PrintCryption card analyzes it. If the electronic key "fits," the file is decrypted and printed. If the key is not a match, the print job is discarded.

As for that mutually agreed-to encryption key, it expires upon completion of the print job. To ensure security, Lexmark's PrintCryption card generates a new session key for each print job. Unencrypted print jobs will print normally.

Lexmark offers secure printing capabilities for UNIX, Solaris (7, 8, 9), and Linux (Red Hat 7 and 8, Caldera 3.1, and SuSE 8). Secure printing from Microsoft Windows, Apple Macintosh, IBM AIX and HP-UX, will be made available from Lexmark in early 2003.

Note: Classified by BEA as a retail encryption commodity. Subject to export restrictions.