

AMERICAN BANKER

THE FINANCIAL SERVICES DAILY

Tuesday, August 29, 2006

Vulnerability Seen in ATM Links to Data Networks

■ BY TOM WRIGHT

ATM & Debit News

Just when banks thought that they were getting a handle on upgrading their automated teller machines to support the Triple Data Encryption Standard, a security firm is warning of potential insecurities with new operating systems that hook ATMs into banks' computer networks.

Redspin Inc. of Carpinteria, Calif., says that linking ATMs to banks' data networks offers numerous advantages and is becoming more popular, but can also make transaction data more vulnerable unless additional controls are put into place.

Historically, ATMs were connected through dial-up telephone lines directly to an electronic funds transfer network, and then linked to a financial institution's core data system through a leased or virtual leased line.

John Abraham, Redspin's president, said that "these machines used obscure protocols and there were significantly fewer opportunities for any 'sniffing' of the transaction data on these proprietary networks."

Today, institutions are increasingly moving toward ATMs that use Microsoft Corp.'s Windows operating system running over TCP/IP (transmission control protocol/Internet protocol) networks.

There are numerous advantages to banks that use this architecture, including lower monthly telecommunications fees, higher bandwidth, and easier management of ATM menu changes.

Yet, with these advances come new security issues surrounding broader access to sensitive ATM data.

According to Mr. Abraham, "in the course of doing bank security audits and observing their network traffic, we noticed card numbers, expiration dates, account balances, and

withdrawal amounts traversing the networks in clear text."

Rick Ewart, a CPA who specializes in credit union information systems, network security, and ATM PIN and encryption key reviews, wonders whether more information captured at ATMs should be encrypted at the machine.



Abraham: Audits showed withdrawal amounts "traversing the networks."

"Only the PIN is encrypted because in the past the computing power and bandwidth weren't there to allow added encryptions," he said. "Before the advent of [offline] debit cards, not having the PIN essentially rendered the rest of the information much less useful. However, I always thought that all card data should be encrypted."

Mr. Ewart is quick to point out that the ATM industry is not alone in passing unencrypted, sensitive data over networks. He notes that "many data processing vendor systems use terminal sessions that pass data in clear text, which means that there is often a lot of other unencrypted traffic on the network that might be of even higher value than basic card information."

Configuring ATMs to use a virtual local area network would significantly reduce the chances of a rogue employee, visiting vendor, or an outside hacker gaining access to the data, Mr. Ewart said. "I always recommend segregating ATM connectivity" from open parts of a network, he said.

Mr. Abraham said that firewalls, routers, and intrusion-detection and intrusion-prevention systems should be subject to regular security audits. Protecting unencrypted card data is important, he said, because even without the PIN, criminals can use the remaining card data to create a duplicate card to be used for signature-based transactions in merchant locations or on the Internet.

Since most financial institutions now use a "hub-and-spoke" communications architecture between their main office and branches, where they often deploy lobby, through-the-wall, or drive-up ATMs, security experts insist that these wide-area network connections also be secured.

Mr. Ewart noted that telecommunication carriers do not guarantee the security of information transmitted across their lines.

And Mr. Abraham suggested that financial institutions are pretty much on their own to secure ATM transaction data traveling over internal networks.

"ATM deployers need to be aware of vulnerabilities," Mr. Abraham said, "and do their best to minimize fraud as much as possible."

Mr. Wright is a freelance writer in St. Louis. This article originally appeared in ATM & Debit News, a sister publication to American Banker.

