WHITE PAPER

atm marketplace

Securing ATMs with Software: Five Strategies

Encryption protocols and remote key management are just two of the tools deployers can use to protect themselves from breaches.

By Emily Wheeler
Contributing editor,
ATMmarketplace.com

Sponsored by:

Triton
A DOVER COMPANY

In February 2009, it took a group of hackers only 30 minutes to steal $9 million from 130 ATMs in 49 cities around the world. The problem of ATM theft continues to grow, as fraudulent ATM activity cost consumers more than $50 million in 2010. Many operators are turning to EMV to increase security. The United States, however, remains primarily dependent on mag-stripe cards, leaving deployers vulnerable to criminal activity. Should a network be breached, IAD deployers could be liable for millions of dollars.

This white paper, sponsored by Triton, discusses five strategies for making sure ATMs are secure via software.

Stay up to date

Everyone who owns a PC knows that software grows obsolete quickly, and it can seem like new patches are available daily. For an ATM deployer who owns multiple machines, it is essential to keep the software running an ATM current.

"Hackers thrive on old software, because they can exploit its weaknesses," said Bob Douglas, vice president of product development and engineering for Long Beach, Miss.-based Triton, an ATM manufacturer.

The longer software has been available to ATM deployers, the more time thieves have had to determine any vulnerabilities. Software providers, however, also have been paying attention to potential weak spots, and most likely have developed patches or new versions of the software.

Hackers can more easily exploit weaknesses on old software. An ATM provider should provide free software upgrades and easy access to the software.

An ATM provider should offer free software upgrades and easy access to the software, making it convenient for deployers to install.

"Triton notifies me whenever a patch is available," said Gavin Reubenson, business development executive at Paycorp Holdings, an IAD based in South Africa. Paycorp has 4,500 ATMs throughout South Africa and Namibia. "Then, I just have to go to the website and download it to my machines. I stay up to date, without having to put in a lot of time and effort."

Make good use of passwords

ATMs come loaded with default passwords set by the factory. Although almost every deployer knows the password should be changed, it is a task that easily can be overlooked.

If the default password remains in place, however, anyone who knows that password can use the ATM as an administrator, with the ability to bypass all security.

New ATMs now are being shipped with software that will force the technician to change the ATM master password at installation, combating the problem of default passwords. Many IADs, however, are using older ATMs, and even new installations can contain refurbished ATMs. Updating older ATMs with the latest software will require the deployer to set new passwords.

Choose a software package that allows different passwords with different levels of authority. For example, the cash loader can have one password that only allows him to access the parts of the system needed to load money, while someone who works in the back office could have a password that allows her a greater level of access. Of course, the IAD deployer should have a master password that allows him access to all parts of the system.

Tips for setting an ATM password

- Make it unique.
- Have it contain a mix of numbers and letters. One good strategy is to substitute numbers for letters (i.e., use 8 for H) and vice versa.
- Do not use significant dates or names that easily can be guessed. Although it is tempting to pick a birthday or the name of a pet, if that information is easily available to thieves, they can guess the password.
- Don't use a word that can be found in the dictionary.

Enable Message Authentication Codes (MACs)

ATMs are networked, sending messages to and from the host. Such networking represents a point of vulnerability for IADs, because a criminal can intercept the messages and alter them, or impersonate an ATM or a host and send counterfeit messages.

Message Authentication Codes are "cryptographic checksums" which are appended to messages sent to and from the ATM to verify that the messages sent are identical to the messages received, and that the messages originate from a legitimate source. MACing ensures that the correct machines are speaking to one another and only authorized messages are being received and transmitted.

"Software with MACing enabled prevents 'man-in-the-middle' attacks," said Douglas. "A criminal can't perform unauthorized operations by modifying communications on the network, so long as message authentication is implemented."

Enable SSL on TCP/IP machines

When TCP/IP communications are used, for example over the Internet, an attacker may attempt to eavesdrop upon or modify a message, to impersonate a server or to interlope as a "man in the middle." Enabling secure socket layer (SSL) prevents such activities.

SSL should be enabled on both the server and the client (in this case, the ATM). It allows the ATM client to authenticate the host server, and ensures the integrity of the messages.

At the same time, enabling SSL prevents any snooping on the line by a criminal. If the information is transmitted only from an SSL-enabled client to an SSL-enabled server, a thief cannot capture the message and use the information for fraudulent activity.

Use remote key management

PCI DSS requirements mandate that deployers update keys at least annually. Traditional key loading involved manually inputting the keys into each ATM by service personnel, costing a deployer money and leaving the system vulnerable. Security keys may become compromised due to accidental disclosure or infiltration of the system by criminals, and manual inputting of long strings of numbers can lead to typing errors.

Remote key loading allows keys to be updated in a secure environment remotely over a network. Removing humans from the equation eliminates the possibility of human error or criminal activity from the update activity. And since uploading a new key remotely is both easier and more cost-effective than doing so manually, deployers can update keys more frequently, making them less prone to attack. In the case of a suspected breach, new keys can be uploaded quickly.

Message Authentication Codes are "cryptographic checksums" which are appended to messages sent to and from the ATM to verify that the messages sent are identical to the messages received, and that the messages originate from a legitimate source.

ATMs will always be vulnerable to attack, and thieves grow ever more sophisticated. Security is paramount to a deployer, but it doesn't have to be a burden. A few simple strategies can help keep a deployer safe, and a partnership with an ATM provider who provides a comprehensive security protocol can ease security headaches.

About the sponsor: *With more than 200,000 installations in more than 24 countries worldwide, Triton has been a trusted leader for affordability and service for 30 years. Triton's full line of ATMs for retail locations and financial institutions are designed and assembled in the United States at a state-of-the-art manufacturing facility in Long Beach, Miss. In addition, Triton offers world-class customer support, parts, service and training via partner ATMGurus.*