

New attack trend pushes POS encryption to the fore

Vendors offer new tools to try to help retailers stop data-in-transit thefts

By Jaikumar Vijayan

May 20, 2008 (Computerworld) The relatively scant attention that retailers have paid to securing their point-of-sale systems over the past few years is making the POS setups increasingly [attractive targets](#) for cybercrooks who are looking to steal payment card data.

Hoping to help merchants address that situation are a handful of vendors who have begun offering new products aimed at making POS environments a lot harder to crack.

The biggest of those vendors is VeriFone Holdings Inc., which last month [released](#) a security tool designed to let merchants encrypt credit and debit card data from the moment a card is swiped at a merchant's PIN entry device all the way to the systems of the company's external payment processor.

VeriFone's VeriShield Protect software is based on patented technology from Semtek Innovative Solutions Corp., which makes appliances for securely decrypting data. VeriFone said that Semtek's technology, called the Hidden Triple Data Encryption Standard, can be used to encrypt personal account numbers and the so-called Track 2 data stored on the magnetic stripe located on the back of payment cards. That information includes card numbers and their expiration dates.

A key feature in VeriShield Protect is that it encrypts payment card data in such a way that the information will still be recognizable as valid card data by other POS applications, said Jeff Wakefield, vice president of marketing at VeriFone. As a result, merchants won't need to tweak or modify their POS systems in any way to accommodate the encryption technology, he claimed. But at the same time, encrypting the card data will render it totally useless to anyone who steals the information, Wakefield said.

A separate device — which could be installed by either a retailer or its payment processor — then would be used to decrypt the data before transactions are processed.

Merchants using newer models of VeriFone's PIN entry devices can have the encryption function "injected" into them for less than \$50 per device in license and service fees, Wakefield said. He added that the vendor doesn't have a published list price for new PIN devices that support the technology, because per-device prices can vary depending on the individual installation.

Meanwhile, the decryption appliances, which are made by Semtek and sold by VeriFone, can cost from \$50,000 to upward of a million dollars for high-throughput, fully redundant systems. Larger retailers that want to exercise direct control over all aspects of their payment card transaction process might invest in such systems themselves, Wakefield said. But, he added, most small and midsize merchants will likely look to their payment processors to handle the decryption component.

Another company targeting the POS security market is [Merchant Warehouse](#), a credit card processing firm that provides services to about 50,000 retailers, most of them small or midsize. The company offers a product called [MerchantWare](#), which like VeriFone's technology is designed to enable merchants to encrypt card data from the beginning to the end of the sales and payment process.

Although VeriShield Protect is focused on the PIN pad devices that are used by customers themselves to swipe their cards, Merchant Warehouse CEO Henry Helgson said that MerchantWare is aimed more at POS systems in which cards need to be handed over to a cashier.

MerchantWare is based on technology from MagTek Inc., a rival of Semtek. Like VeriShield Protect, MagTek's product also encrypts data at the card reader. But integrating the technology into existing environments does require "minimal" updates to a company's POS software, Helgson said.

With MerchantWare, merchants never have to store any payment card data on their systems, according to Helgson. Instead, a retailer that needs to access payment transaction data to handle issues such as chargebacks or payment disputes would log into a MerchantWare payment gateway to get at the information.

Helgson said that the recent disclosures of several [data-in-transit thefts](#) are helping to generate interest in technologies such as MerchantWare. "This is our way of getting new customers," he said. "We expect huge demand for this.

Also offering capabilities similar to MerchantWare is payment processor Element Payment Service Inc., which is using MagTek's technology to provide bundled encryption services to retailers, said [Gartner Inc.](#) analyst [Avivah Litan](#). It's surprising, she added, that more vendors haven't already come out with similar products that can help retailers encrypt payment card data while it is inside their networks.

Currently, under the Payment Card Industry Data Security Standard mandated by the major credit card companies, merchants are required only to ensure that any payment card data being transmitted over a public network is encrypted. The lack of a rule requiring that data be encrypted while it is transmitted internally has been exploited in at least three major data breaches disclosed in the past few months.

The biggest of the breaches took place at [Hannaford Bros. Co.](#), a supermarket chain based in Scarborough, Maine. In March, Hannaford said that malware [planted on the POS servers](#) at nearly 300 grocery stores had been used to steal unencrypted payment card data on more than 4 million customers. Last month, Hannaford officials said that the grocer planned to spend ["millions" of dollars](#) on IT security upgrades in the wake of the breach.

Similar incidents have also been reported by Okemo Mountain Resort, a [ski area](#) in Ludlow, Vt., and by Dallas-based restaurant chain [Dave & Buster's Inc.](#), which said last week that credit and debit card numbers were stolen from 11 of its restaurants during 2007 by hackers who allegedly gained remote access to POS servers and then installed packet-sniffing software on them.

Such breaches highlight the need for companies to pay more attention to encrypting payment card data within their own network boundaries, Litan said. But thus far, she added, adoption of the available encryption technologies has been slow because many retailers appear unconvinced that encryption can be introduced at the POS level without requiring major changes. For instance, one concern is that encrypting data will make it harder for retailers to handle issues such as chargebacks.

"Most merchants are passive about this because their systems rely on card numbers for chargebacks," Litan said. "They need to be convinced that their systems need to change." In addition, many retailers have spent a lot of money, time and effort complying with the existing PCI requirements and are reluctant to implement even more security controls, she said.