SecurityInfoWatch.com

Payment Card Industry meetings address future of card security

PCI Security Standards Council meetings review issues such as card fraud and encryption but overlook solutions

BY LARRY MEYERS, MAGTEK
For SecurityInfoWatch.com
October 6, 2009

MagTek's Larry Meyers says technology exists today which would allow the continued use of traditional (non smart-card) credit cards while solving the current PCI security issues.

Larry Meyers is vice president of business development for MagTek.

I recently attended the Payment Card Industry (PCI) Community meetings in Las Vegas, Nevada (Sept. 22-24, 2009), and came away with several observations that could have a significant impact on how banks, merchants and consumers handle credit and debit card fraud. For those of you not familiar with PCI Security Standards Council, the open global forum focuses on developing and implementing security standards for account data protection. The council provides guidelines on how business owners and financial institutions should protect personal information, and these guidelines serve as a mandatory requirement for organizations that process, store or transmit payment cardholder data.

Doing More than the Minimum

During the meeting, PCI Council addressed the need for the PCI community to think about overall security as opposed to just meeting the "check list" of PCI-Data Security Standard (DSS) requirements. This is an intriguing concept, as this wider view encourages people to consider security technologies and methods that go beyond just simply "protecting cardholder data." While some in the financial community may use PIN numbers and encryption as first and second layers of protection, we must remember that there is a third layer - which I feel is a critically important layer - that provides the missing piece for comprehensive data protection and transaction security. This powerful layer includes the important concept of dynamic card data authentication, but I am getting ahead of myself.

The next important take-away from the meeting was that the threat, sophistication, and frequency of cybercrimes on card payment data have soared to an all-time high. Even more concerning is that no end to such threats is in sight. According to new statistics

presented by Christopher Novak, the managing principal of investigative response for Verizon, the breadth and depth of the problem is worsening. Novak reviewed data and information collected as part of an independent study commissioned by Verizon which analyzed businesses that suffered payment data breaches. The results of the study were sobering, as they clearly underscored the reasons why the payment community needs to remain vigilant and proactive in protecting cardholder data and securing payment transactions.

But not all the news stemming from the PCI Council meeting was bad. A subsequent presentation titled "Emerging Technologies Research" shed light on five technologies that may improve the ability for the PCI community to obtain compliance to PCI-DSS requirements, reduce fraud, or even negate the need for PCI requirements altogether.

The highlighted technologies included:

- End-to-End Encryption;
- Dynamic Payment Card Data;
- Magnetic Stripe Imaging;
- Tokenization; and
- Virtual Terminals.

Granted, the Emerging Technology research presentation was cautiously (and appropriately) framed as being preliminary with the clear caveat that information may not be 100 percent accurate or complete. However, with that understanding, I found the following points from that presentation to be enlightening:

- There is no singular "silver bullet" technology that will assist in reducing existing PCI compliance requirements or reduce fraud. A layered security approach is best. Each of the aforementioned technologies provide either compliance and/or enhanced security merits depending upon how they are implemented.
- End-to-end encryption appears to show the most immediate promise to assist with compliance to the existing PCI requirements for "protection of cardholder data." The research suggests that this technology has the ability to completely remove card data out of the merchant environment, effectively maintaining security of cardholder data during storage, transmission, and processing. However, End-to-End Encryption has the significant inability to reduce fraud from counterfeit cards.
- Dynamic payment card data technology appears to show the best long-term promise to improve overall security and to "make stolen card holder data useless" to criminals. Most importantly, the presentation suggested that this technology "has the potential to eventually eliminate the need for PCI-DSS."
- Magnetic stripe imaging shows promise as a real-time fraud reduction technology that can detect and prevent the use of counterfeit magnetic stripe cards.

The Missing Piece

As previously mentioned, some inaccuracies do exist within the Emerging Technology review. Most notable was the failure to recognize that there are embodiments of magnetic stripe imaging that also provide dynamic payment card data features. This lack of recognition was an unfortunate omission of information because it would have allowed the audience to understand that it is possible to completely secure payment transactions using the magnetic stripe cards that exist today. Also missing from the presentation was the ability to discuss technology platforms that combine multiple elements of the aforementioned security capabilities into a single platform.

While some experts are proposing to phase out magnetic strip cards in favor of more expensive contactless payment systems or chip technology, there are alternative technologies that offer a cost-neutral solution that won't require the reissuance of the three billion cards in use today. One example is our own technology from MagTek called "MagneSafe."

Dynamic Card Data Authentication Via Digital Fingerprints

Much like our DNA, no two pieces of magnetic tape are the same. Each stripe on the back of a credit card contains billions of ferrous oxide particles of various shapes and sizes that mix in random patterns when the magnetic slurry is prepared. Those patterns are sealed in place when the slurry dries during the tape manufacturing process and give the stripe a unique identity or fingerprint. The distinct magnetic signal, like a human fingerprint, remains largely unchanged for the life of the card, yet provides dynamic data characteristics each time it is used.

During a card transaction, the technology reads the unique and dynamic magnetic noise or 'magnetic fingerprint' that is imbedded in each magnetic stripe card, and compares it with a 'reference print' on file. By reading this information, the system can determine in real-time whether a card has been copied, cloned or tampered with, and in doing so, can help the financial community render every counterfeit card worthless. Most importantly, this technology also provides a dynamic card data value that is unique for each transaction. In doing so, it provides the ever important "dynamic payment card data" capability that is referenced in the PCI Emerging Technology report. In short, MagneSafe provides the benefits of both card authentication and dynamic card data for each transaction.

Such a method of dynamic card data authentication would allow for complete end to end security of cardholder data and would provide a means to detect and eliminate the use of counterfeit payment cards. Importantly, these security capabilities would lessen the value of stolen cardholder data to the criminal community because it would eliminate their ability to redeem value from the stolen data via counterfeit cards. Additionally, the technology can provide these capabilities while utilizing the existing magnetic stripe cards that consumers already carry in their wallets today. In other words, banks and financial institutions will not need to reissue or change existing magnetic stripe cards, and consumers don't need to change existing behavior. Not to mention that this technology costs a fraction of a penny per card, which is less than many alternative solutions on the market today.

As the card payment community considers the information presented at the recent PCI Community Meetings, we should embrace the idea that overall card payment security needs to go beyond protection of data to include authentication and dynamic data elements as well. As this thought process continues, it is increasingly important to recognize that there are existing authentication technologies that are proven alternatives which would allow the United States to secure its card payment infrastructure with existing magnetic stripe technology.

About the author: *Larry Meyers is vice president of business development at MagTek, a provider of secure transaction technology to the payment card industry. Meyers currently oversees the strategic business and technical development of MagTek's next-generation products and technologies. Learn more about what Larry is working on at security.magtek.com.*