WHITE PAPER

An Introduction to Dynamic Authentication

While magnetic stripe cards are perceived as more vulnerable than EMV-enabled cards, using the mag-stripe's unique biometrics can ensure security.

By Suzanne Cluckey
Contributing writer,
ATMmarketplace.com

Everyone pays for card fraud. According to a 2011 study by LexisNexis, credit card fraud costs the U.S. card payments industry more than $100 billion annually, with the bulk of the losses falling on merchants, who absorb ten times more in identity fraud costs than financial institutions.

The majority of credit and debit cards in the United States rely on magnetic stripe technology for security, but the mag-stripe has proven vulnerable to theft. Many card issuers now are looking seriously at the EMV chip, which is already widely used in Europe and Asia. This solution, however, would be extraordinarily expensive to implement in the United States, whose population of cardholders is by far the world's largest. The Mercator Advisory Group estimates the cost of a switch to EMV at $3 billion for banks and nearly the same amount for merchants who would have to replace or modify their POS systems. What is more, chip-and-pin technology also has been shown to be at risk for fraud.

There is another alternative to card-present fraud prevention, however, one that works not by dispensing with the magnetic stripe, but by capitalizing on its unique biometrics, thereby offering dynamic authentication.

The chance that particles would be distributed in precisely the same way twice is approximately one in 900 million.

What is dynamic authentication?

Every magnetic stripe has embedded biometric-like information; the organic process of creating the magnetic stripe results in the distribution of particles on the stripe that are more distinctive than fingerprints. The chance that particles would be distributed in precisely the same way twice is approximately one in 900 million.

A team of researchers from Washington University in St. Louis discovered that unique magnetic particle patterns could be captured and identified with an extraordinary degree of accuracy during the card swipe process. This magnetic fingerprinting process has been patented and licensed for use by Seal Beach, Cali.-based MagTek, a provider of secure transaction technology to the payment card industry.

How it works

Card fingerprinting works by identifying the unique particulate pattern on a card's magnetic stripe as it is swiped through a Secure Card Reader Authenticator (SCRA). The reader, which is easily retrofitted to an existing POS system, takes into account variations in each physical card swipe, as well as changes that would naturally occur with card wear.

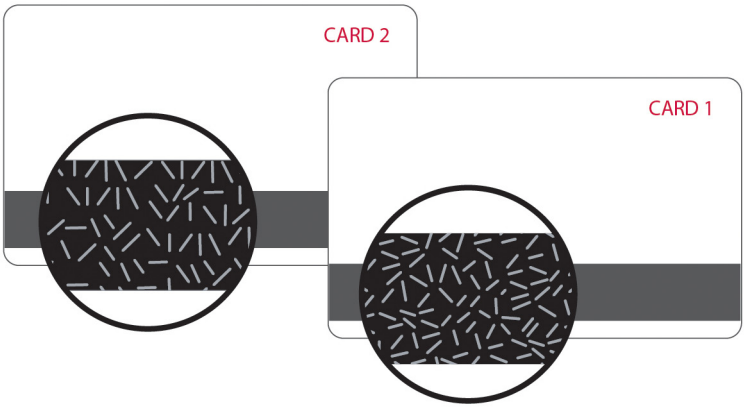
The swipe data is translated into a 54-byte print value, which is sent to a globally accessible database during the transaction approval process. Here, the swiped print is compared to the reference print on file for that card number and the transaction can be accepted or rejected based on that comparison.

Importantly, the matching process can be carried out without causing a significant delay in the transaction approval process. Just as importantly, the swipe and comparison data render highly accurate authorization results. A test run of one million bankcards by system developers resulted in zero false acceptances and a false reject rate of just .027. The reject threshold may be manually set by the authorizing party to the sensitivity with which they are most comfortable.

Benefits

Biometric stripe recognition can effectively immunize the magnetic stripe card against three types of card-present fraud by making stolen data useless to criminals in these applications:

Dummy cards. Cards created using stolen magnetic stripe information on counterfeit charge plates will be identified when the particulate distribution of the dummy card does not match the print on file. Even if the data and card appear to be authentic, the system will reject the transaction because the magnetic "fingerprints" do not match.



Card fingerprinting works by identifying the unique particulate pattern on a card's magnetic stripe as it is swiped through a Secure Card Reader Authenticator (SCRA).

Altered magnetic stripes. As with dummy cards, restriped cards would be rejected because the data on the magnetic stripe does not match up with the reference print of the magnetic stripe itself.

Multiple transaction submissions. Just as no two stripes are alike, no two swipes are identical either. If a transaction is accidentally (or criminally) submitted more than once, the system will recognize the perfectly identical card reads and will reject the additional transaction.

Challenges

The success of a card fingerprinting system hinges on the development of a comprehensive and robust database. And the development of this database depends

on both banks and merchants. Sizeable groups of each must adopt the system in order for it ultimately to reach the tipping point of ubiquity.

In a best-case scenario, card-issuing banks would register a card fingerprint prior to issuance of the card. A workable alternative (or supplement) would be to collect a provisional card print during a merchant or ATM transaction. Should a card later be identified as a counterfeit, it would be removed from the database.

Retailers also would have to purchase an SCRA in order to access the print database. However, barriers here are relatively low: the reader is easily retrofitted to an existing system and it costs less than the chip reader alternative. Implementation at retail would likely have a snowball effect — as more retailers begin to add readers, fraud risk gets pushed down the chain, increasing the pressure on other merchants to get into the system.

Assuming widespread adoption, MagTek estimates that dynamic authentication might help reduce credit card fraud by as much as $1 billion. Combined with data encryption measures mandated by PCI DSS, this figure could become larger still as criminals find that the data they must work harder to obtain offers much less value than it used to.

Additional benefits of card fingerprint technology

Card fingerprint technology offers a number of other benefits including:

1. With magnetic stripe fingerprinting technology, banks need not reissue magnetic strip cards nor resort to issuing chip-and-pin cards at up to ten times the cost of a magnetic stripe card.

2. The card reader technology is relatively inexpensive to implement. SCRA card print readers can be retrofitted to most existing card authorization systems at a cost lower than that of chip-and-pin readers.

3. It is impossible to duplicate the particulate distribution on a magnetic stripe. Because this information becomes part of the data scanned by the SCRA reader, fake cards can be detected. By contrast, digital data stored in a chip card can be cloned simply by duplicating a series of zeroes and ones. A chip card reader cannot tell the difference between the numerical series on the originally issued card and the duplicated series on the fake card.

4. Card fingerprinting protects all parties in a transaction. Chip-and-pin systems primarily protect issuing banks, but leave merchants and consumers subject to continued risk from counterfeit cards. With card fingerprinting, protection extends all the way to the consumer, whose card information is useless to criminal operations that produce dummy cards or altered cards.

About the sponsor: *Since 1972, MagTek has been a leading manufacturer of electronic devices and systems for the reliable issuance, reading, transmission and security of cards, checks, PINs and other identification documents. Its products include secure card readers, check scanners, PIN pads and distributed credential issuing systems. These products are used worldwide by financial institutions, retailers, hotels, law enforcement agencies and other organizations to provide secure and efficient electronic payment and identification transactions.*