DIEBOLD NIXDORF PERSPECTIVE

Counter the $2 billion card-skimming threat

By Joerg Reuter, Diebold Nixdorf Business Development Lead, Security

Joerg Reuter
Diebold Nixdorf

Despite the ongoing move towards EMV-compliant chip cards, the skimming and misuse of card data has continued to rise. The European ATM Security Team (EAST) found international skimming losses increased by 15% from 2014 to 2015, and through the first half of 2016, that number had risen by another 8%.

The skimming evolution

Recent years have seen steadily increasing sophistication of skimming devices used to harvest consumer card data – some being so difficult to discover that it would take thorough examination of an ATM or POS by an expert. We've seen the evolution from M1 skimmers, bulky enough to be spotted by attentive consumers, to M2 skimmers mounted in the card-reader throat, and now M3 skimmers, also known as 'deep insert skimmers', that are placed inside the card reader itself. New 'periscope skimmers' tap directly into a card reader's electronics or the read head to steal information, a process known as 'eavesdropping'.

Fraudsters are attempting to attack EMV chip cards, through 'shimming' devices that capture the data exchanged between the chip card and reader

Each of these malicious methods targets data stored on a card's magnetic stripe, which can easily be duplicated. EMV chips were designed to circumvent this issue as it contains a microprocessor that takes an active role in self-service transactions, making it nearly impossible to copy the contents from a chip.

Of course, fraudsters are now attempting to attack EMV chip cards, through 'shimming' devices that capture the data exchanged between the chip card and reader. We have seen a few cases in which captured data has been used to create counterfeit magnetic stripe cards with supposedly defective chips. In such a 'fallback scenario' the reader will in certain cases revert back to the magnetic stripe.

These are outliers, however. Where best practices for handling EMV transactions are followed (e.g. creation and checks of card verification values and data authentication protocols), no practical EMV attacks have been successful 'in the field'.

Solutions for the hybrid era

However, until magnetic stripes have been rendered obsolete, skimming will remain a problem. But as skimming devices have become more sophisticated, so too have anti-skimming devices. One effective solution is jamming, in which an electromagnetic signal is generated around the card reader. This 'disturbance' overpowers the signal from the magnetic stripe that the skimming device is attempting to read.

Our engineers have come up with a solution that goes even further: It thwarts skimming devices from accessing the card reader in the first place. The ActivEdge card reader requires users to insert their card long-edge first. A sliding head reads the card internally, rendering stationary skimming devices useless. To prevent eavesdropping, card data is securely encrypted in the head as it is read. Consequently, the card reader only handles encrypted data. Combined, these innovations can prevent all known skimming attacks.

Skimming is a very expensive problem, but it does not have to affect your network. Here is an effective four-step roadmap for protecting your ATMs – and most importantly, your customer data:

1. In the short term, equip existing ATMs with anti-skimming devices. Diebold Nixdorf's ASKIM II Disturb is an example of an effective jamming solution for self-service terminals.
2. Limit fallback scenarios and implement measures such as geoblocking (disabling a customer's cards outside their home country) and fraud detection.
3. Know the most current options for thwarting skimmers and consider incorporating solutions such as ActivEdge onto new ATM purchases.
4. In the long term, play your part in driving the shift to a fully EMV-enabled ecosystem, so card issuers can finally begin to phase out magnetic stripes.

Self-service security is a layered, constantly evolving challenge that requires global action and 24/7 surveillance. Follow along with us on the latest trends and how they can apply to your security strategy at DieboldNixdorf.com/trends. ■

DIEBOLD NIXDORF