

[Email](#)[ShareThis](#)

Benefits and Security Vulnerabilities of Contactless Card Payment Systems

Close-Up Look at RFID, EMV and NFC

By Marv Chen and Kevin Tsuei, AuditOne LLC

Contactless payment systems have experienced tremendous growth in the last decade. According to the Smart Card Alliance, a non-profit industry association, 35 million contactless chip cards are already in circulation in the U.S. In addition, over 35,000 merchant locations now accept contactless payment cards and devices.

There are numerous benefits to contactless payment. For consumers, contactless payment is convenient; they simply wave a payment card or mobile phone in front of the terminal to process a payment. In fact, the time saved has been quantified: according to an article in PC World, wait times were reduced 14 to 20% in stores and 40% at drive-throughs. Average transaction times also decreased 10 to 40%.

The merchant also wins with contactless payment. MasterCard Canada has seen 25% more spending by users of its PayPass-brand contactless credit card. Chase states that merchants have experienced 40% greater average ticket sales with its contactless Blink card than with cash purchases. In addition, Chase states that the frequency of everyday purchases increased by 35% when compared to traditional magnetic stripe credit cards.

In terms of security, contactless payment can also help fight fraud. For example, no longer does a consumer need to hand a credit card to a fast food operator or gas station attendant, where the card number, printed CVV or expiration date could be misappropriated. A contactless payment card cannot be easily cloned, unlike its magnetic stripe counterpart. Finally, magnetic stripe credit cards present a further security risk because they store additional personal and account information, such as customer name, account numbers, expiration date and CVV.

There are several contactless payment systems in use, notably the EMV, RFID and NFC.

RFID is primarily used in the U.S. and Japan. It has received a lot of attention lately, e.g., the "RFID Blocking Wallet" which prevents hackers from scanning your wallet. It is true that RFID has certain vulnerabilities, especially the first generation RFID card. Known vulnerabilities include skimming and eavesdropping attacks. Skimming attacks are possible because there is no security mechanism in place for the card to distinguish between an authorized or unauthorized RFID reader. Therefore, an off-the-shelf RFID scanner can obtain information from the card such as cardholder name, card number and expiration date. Eavesdropping involves placing an eavesdropper near the payment terminal. When the payment information is sent between the RFID contactless credit card and the terminal, payment information such as cardholder name, credit card numbers and expiration date can be obtained as this process is not encrypted.

However, there are some security controls in place for RFID. For example, an RFID contactless card is only designed to be read from one to four inches away from a terminal. Some cards even require the RFID payment unit (Visa) to be oriented a certain

way before it can be read by the terminal. In addition, each time a transaction is processed, the RFID contactless card generates a unique one-time transaction number. Since only the card number, expiration date, and the unique transaction numbers are passed through the terminal, it would be difficult for a hacker to make unauthorized purchases. American Express even goes a step further by preventing its RFID from passing on the account number during a transaction. Because the unique transaction is good for only for a single purchase, even if the transaction is skimmed or eavesdropped, it would be not be possible to make further unauthorized purchases. In addition, this unique transaction number cannot be used for online or phone purchases.

UK and Europe use what is known as EMV, Chip or PIN systems. EMV not only requires a payment card (contact or contactless), but a PIN to authorize the transactions. Since the implementation of the EMV payment system, the UK's Cards Association has reported, "Fraud on lost and stolen cards is now at its lowest level for two decades, and counterfeit card fraud losses have also fallen and are at their lowest level since 1999."

However, the EMV contact and contactless payment systems also have vulnerabilities. For example, PIN input can be observed by security cameras or via "shoulder surfing." In addition, the technical security protocols that EMV uses are vulnerable as well. For example, according to *la Repubblica* in Italy, both card and PIN numbers were compromised when the payment terminal was modified. Using a microchip, hackers were able to capture credit/ATM card numbers and PINs wirelessly using Bluetooth. In addition, there have also been a few research papers from Cambridge University in England that found vulnerabilities with EMV, such as the ability to fool an EMV terminal into making purchases without a valid PIN and flaws within the EMV system that allow bank insiders to extract PINs.

Another up-and-coming contactless payment system is NFC or Near-Field Communicator. NFC has a variety of uses including Bluetooth, Wi-Fi, and social networking, and from a commercial perspective, NFC can be used as a mobile payment method in place of a credit card. The Android mobile operating system already supports NFC (i.e., Google Wallet). A number of handset makers (HTC, LG, Motorola, RIM, Samsung, Sony) have already agreed to support the new "Isis" NFC Payment Platform (created by Verizon, AT&T, T-Mobile). Similar to other contactless payment systems, NFC has many convenience-related and security-related benefits. One of the most distinct features of NFC is that you no longer need to carry credit cards; you only need your phone with the NFC chip to conduct the transaction. Since this technology is fairly new, not many mobile devices support this feature, but credit card companies are going out of their way to implement this system. For example, Visa payWave can be installed as an app on an iPhone with a Visa payWave micro-SD card.

Like all technologies, NFC has its share of vulnerabilities. Similar to EMV and RFID, it is also vulnerable to skimming attacks. For example, hackers can set up one smartphone acting as a rogue merchant terminal and another smartphone acting as a card merchant. When a payment is processed, the rogue merchant terminal captures the information, records it, and then forwards the information to the card merchant. In addition, since the payment chip is installed over the phone, it can be subject to attack by malicious smartphone applications.

There are, however, security controls in place to protect the NFC payment system. For example, with Visa payWave, the distance between the NFC and terminal must be two to four centimeters for the payment to be processed. Similar to RFID, a dynamically generated and unique transaction code is generated by NFC software for each transaction. In addition, the digital key (used in the authentication process) is encrypted on the smart chip. Finally, most mobile phones can enact password-protected screensavers, so payment cannot be processed if a hacker cannot unlock the phone.

Besides Visa payWave, Google is also making efforts to implement the NFC payment program. Security features of the Google Wallet-based phone include the following: the NFC antenna is turned on only if the screen is on (Google Wallet); a PIN is required, much like EMV's security feature; Android enforces strict access policies so malicious applications cannot have access to Google Wallet; the application itself has limited access to the payment smart chip; the smart chip is isolated from the Android OS and hardware; and only an authorized program or Google Wallet can initiate a transaction. Google has already partnered up with major point-of-sale terminals; see <http://www.google.com/wallet/current-partners.html>.

Sources:

- <http://www.rfidjournal.com/article/view/2875>
 - http://www.idtheftcenter.org/artman2/publish/m_press/RFID_and_Credit_Cards.shtml
 - http://www.computerworld.com/s/article/9156158/Researchers_find_huge_weakness_in_European_payment_cards
 - <http://www.cbc.ca/news/story/2010/05/31/f-rfid-credit-cards-security-concerns.html>
 - <http://www.contactlessnews.com/2006/08/02/chase-reaches-milestones-with-blink-continues-to-roll-out-contactless-payment-cards>
 - <http://www.repubblica.it/2006/09/sezioni/cronaca/truffa-blue/truffa-blue/truffa-blue.html>
 - <http://www.lightbluetouchpaper.org/2010/02/11/chip-and-pin-is-broken/>
 - <http://www.nytimes.com/external/qigaom/2011/09/27/27qigaom-handset-makers-line-up-behind-isis-nfc-payment-pl-40916.html?partner=rss&emc=rss>
 - <http://www.infosecurity-magazine.com/view/16393/rfid-credit-cards-are-more-secure-than-magnetic-strip-cards-says-itrc/>
 - <http://www.investmentu.com/2011/June/near-field-communication-smartphone-technology.html>
 - <http://www.google.com/wallet/fag.html>
 - <http://www.theverge.com/2011/11/9/2548440/paypal-android-app-update-nfc-mobile-payment>
 - <http://www.cl.cam.ac.uk/~rja14/rfid-fc07.pdf>
-

[<back to December 2011 Technology & Security Digest>](#)

Marv Chen is technology practice director for [AuditOne LLC](#). He can be reached at Marv.Chen@audit-one.com. Kevin Tsuei is an IT auditor at AuditOne. He can be reached at Kevin.Tsuei@audit-one.com.