How Secure are Contactless Payment Systems?

Matthew Ngu
Engineering Manager
RSA, The Security Division of EMC

Chris Scott
Senior Software Engineer
RSA, The Security Division of EMC
Some threat scenarios

◆ Can an attacker stand behind me and charge my card?
◆ Can an attacker read my EMV card?
◆ Can an attacker mount a high power reader in a van?
◆ Replay attacks?
◆ Can you think of anything else?
Global Adoption

Contact EMV Global Adoption*

*Figures reported as of Q4 2013 and represent the latest statistics from American Express, Discover, JCB, MasterCard, UnionPay, and Visa, as reported by their member financial institutions globally. Figures do not include data from the United States. Figures are reported by region and do not imply country-by-country statistics.
Some US Statistics

- 0.03% of transactions are EMV.
- 50,000 unique merchant terminal locations processed EMV transactions in 2014, compared to an estimated 12 million terminals that didn’t do a single EMV transaction.
- Apple Pay and Google Wallet are currently only available in the US.
- To the end of November 2014, Apple Pay accounted for 1.7% of mobile payments whilst Google Wallet had a 4% share.
- Apple: $2 of every $3 spent in contactless transactions in the US in the lead up to Christmas were made via Apple Pay.
How does it work?
How does it work?

- Contactless Cards
- VISA PayWave / MasterCard PayPass
- Google Wallet
- Apple Pay
How does it work? Contactless Cards

Contactless cards use Near Field Communications (NFC) to send and receive data from the terminal using inductive coupling.

Source: rfid-handbook.de
How does it work?
PayWave / PayPass
How does it work? PayWave / PayPass

Wait for merchant to enter amount.
How does it work? PayWave / PayPass

Reader uses NFC to send and receive information with your card.
How does it work? PayWave / PayPass

Dynamic data unique to every purchase protects your transaction data.
How does it work?

Google Wallet
How does it work? Google Wallet Prerequisites

[Image of NFC technology and Android 4.4 KitKat]

14
How does it work? Google Wallet – Setup

Login to your Google account.
How does it work? Google Wallet – Setup

Enter your credit card details on wallet.google.com.
How does it work? Google Wallet – Setup

Verify your identity by providing Personally Identifiable Information (PII) such as name, address, date of birth, last four digits of Social Security Number (SSN) or Individual Taxpayer Identification Number (ITIN).
How does it work? Google Wallet – Setup

Create your Wallet PIN (different to phone PIN).
How does it work? Google Wallet – Setup

A MasterCard®-branded virtual prepaid debit payment card product, the Google Wallet Virtual Card, issued by Bancorp Bank will be installed on your phone.
How does it work? Google Wallet - Payments

Add money to your Wallet (website or mobile app).
How does it work? Google Wallet - Payments

Bring the phone up to an NFC-enabled terminal.
How does it work? Google Wallet - Payments

Phone will ask you to authenticate the payment with Wallet PIN.
How does it work? Google Wallet - Payments

- Phone transmits the Google Wallet Virtual Card information to the merchant's terminal, not your real credit card information stored on Google's servers.
- Transaction completed as normal using credentials for current payment only.
How does it work?

Apple Pay
How does it work? Apple Pay Prerequisites

- iPhone 6
- iPhone 6 Plus
- iWatch
- iOS 8
How does it work? Apple Pay - Setup

Card Details
Enter your card information or use the camera.

Name: Required
Card Number: Required
Expiration Date: Required
Security Code: Required

RSA Conference 2015
How does it work? Apple Pay - Setup continued
How does it work? Apple Pay – Payments

- Bring the phone or watch up to an NFC-enabled terminal.
## How does it work? Comparison

<table>
<thead>
<tr>
<th>Contactless Implementation</th>
<th>Stores Primary Account Number (PAN)</th>
<th>Customer Authentication</th>
</tr>
</thead>
<tbody>
<tr>
<td>Pay Wave/ Pay Pass</td>
<td>Yes, in secure element on card</td>
<td>None below threshold amount, PIN or signature above threshold amount</td>
</tr>
<tr>
<td>Google Wallet</td>
<td>Yes, on Google servers in cloud</td>
<td>PIN (different from phone unlock PIN)</td>
</tr>
<tr>
<td>Apple Pay</td>
<td>No, PAN only required during registration</td>
<td>iTouch or Passcode</td>
</tr>
</tbody>
</table>
What are the Security Features?

- Secure Element, Trusted Execution Environments.
- EMV for preventing card fraud.
From EMVCo: PKI

Diagram showing the flow of keys and certificates between the Issuer, Certification Authority, and Acquirer, with the IC Card and IC Terminal as endpoints.
What is protected with EMV?

- Authenticity of the cards (protects against counterfeit cards).
- Payment transactions by adding dynamic data unique to each transaction.
- PINs and keys stored in secure part of card (TEE or SE). PIN encrypted between PIN pad and card.
- A standard is only as good as its implementation.
What are the Security Features?

- Payment tokens for protecting PAN.
What is protected with tokenisation?

- PAN and card expiry date are protected.
- Viability of stolen data is minimised by limiting the domain in which the token is valid.
- Merchant liability is limited by not processing or storing actual cardholder PAN.
What are the Security Features?

- Multi factor authentication during payment transaction (Wallet and Pay).
- Contactless card does not need to leave your hand for payment.
What are the weak points and threats?

- Stolen EMV contactless card can be used to make small payments (below PIN limit).
- Malware on the device or reader.
- Stolen card details can possibly be registered with electronic wallets and then used – depending on ID&V process of Issuer.
- Static authentication data.
The threat scenarios again...

- Can an attacker stand behind me and charge my card different amounts in quick succession?
- Can an attacker read my EMV card and encode PAN on a mag stripe card?
- Can an attacker mount a high power reader in a van?
- Replay attacks?
How can I APPLY what I have learned?
If I am a Merchant, Bank, Processor...

- Use a combination of EMV and (back-end) tokenisation.
- Realtime authorization, ie no offline transactions.
- Phase out mag stripe cards – data from chip card can be transferred onto mag stripe.
- Do not send activated cards by mail.
- Monitor usage patterns and implement other fraud detection measures.
- Secure issuer and card private keys; card MAC master keys. Isolate from corporate network and include physical interlocks for access.
- Biometric authentication on card or just simple button that has to be pressed to enable chip to be energized.
If I am a Consumer?

- Do metal card sleeves really work?
- Tell your bank when you travel.
- Check your statements regularly.
- Protect your PIN.
- Enable iPhone “locate my phone” feature.
- Set limits on transactions.
EMV Contactless, Google, Apple Pay

Contactless payments systems are not fraud-proof.

But more secure than mag stripe-based systems.

More/as convenient, more secure than cash.

Mostly simple measures can be taken to improve security.

Novel approaches are required to improve convenience and bring down cost of implementation.
Any Questions?

- Matthew Ngu: matthew.ngu@rsa.com
- Chris Scott: chris.scott@rsa.com