by Hengbin Liao
Chao Duan
Yun Sheng

News Headlines

Apple Pay: a new frontier for scammers

— The Guardian

Fraud Comes to Apply Pay

— The Wall Street Journal

Morning Agenda: Blame Game in Apple Pay Fraud

— The New York Times

Does Apply Pay really have a fraud problem?

— The Verge

Who's at fault in Apple Pay fraud, Apple or banks?

— CNBC

Nope, there’s no ‘Apple Pay fraud’

— Business Insider

Voices on the Internet

"If they have the card number and a few other details they can enroll it in Apple Pay and their iPhone, in effect, becomes a credit card."

— Patrick Nielsen
senior security expert at Kaspersky Lab

“Criminals will always follow the money, and payment-card fraud will always be an issue.”

— Darren Hayes
assistant professor at Pace University

“Apple Pay is designed to be extremely secure and protect a user’s personal information.”

— Apple spokesperson

“It’s to the benefit of consumers to have a consistent process.”

— Jason Malo
CEB Tower Group’s cybersecurity specialist

More secure payments

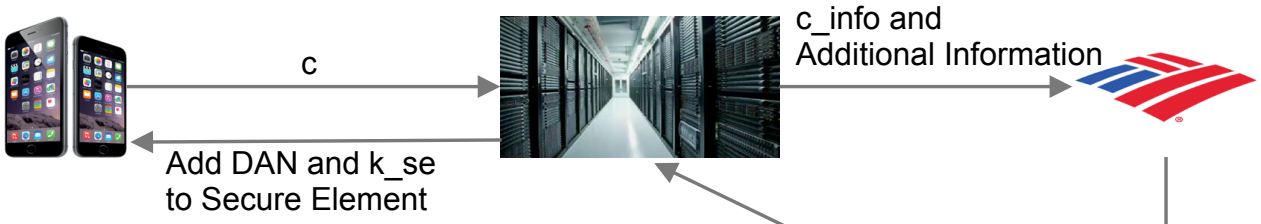
Apple Pay protects your personal information, transaction data and credit and debit card information with industry-leading security.

— Apple

Sort Things Out

- How Apple Pay works?
- Something goes wrong...
- Social Engineering!

Add card to Apple Pay



info = Credit Card Number
Expiration Date
CVV

c = Enc_applepk(info)

Additional Information contains:

- Last four digits of phone number
- Device name
- Rounded latitude and longitude
- iTunes Account Activity information

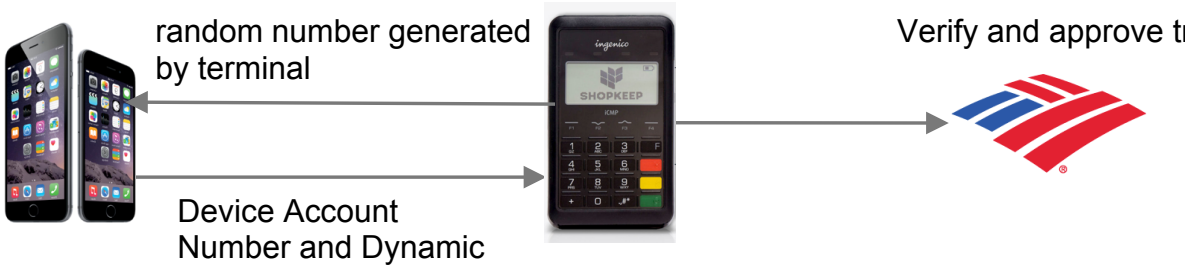
info = Dec_applesk(c)

1. Determine payment network
2. c_info = Enc_bankpk(info)
3. Sends c_info to bank using SSL with additional information

Once Approved send back the following via SSL

- Encrypted Device Account Number
- Other info such as the key k_se used to generate Dynamic Security Codes

Use Apple Pay In Store



Authenticate with passcode or TouchID

The Dynamic Security Code is calculated via

- A counter that is incremented for each new transaction
- A random number generated by the payment applet (which is in SE)
- Another random value generated by the terminal

Secure Element provides:

- Device Account Number
- Dynamic Security Code

In Short:

Dynamic Security Code = PRG_k_se(counter, r_se, r_terminal)

Use Apple Pay in Applications

cryptographic nonce generated by Apple Server

c

verify received data if true then send back data encrypted with merchant's public key

Application initiates an Apple Pay transaction

billing address, shipping address, zip code etc.

TouchID or passcode Authentication

c = Enc_applepk(nonce and transaction data passed to SE to generate payment credential)

amazon

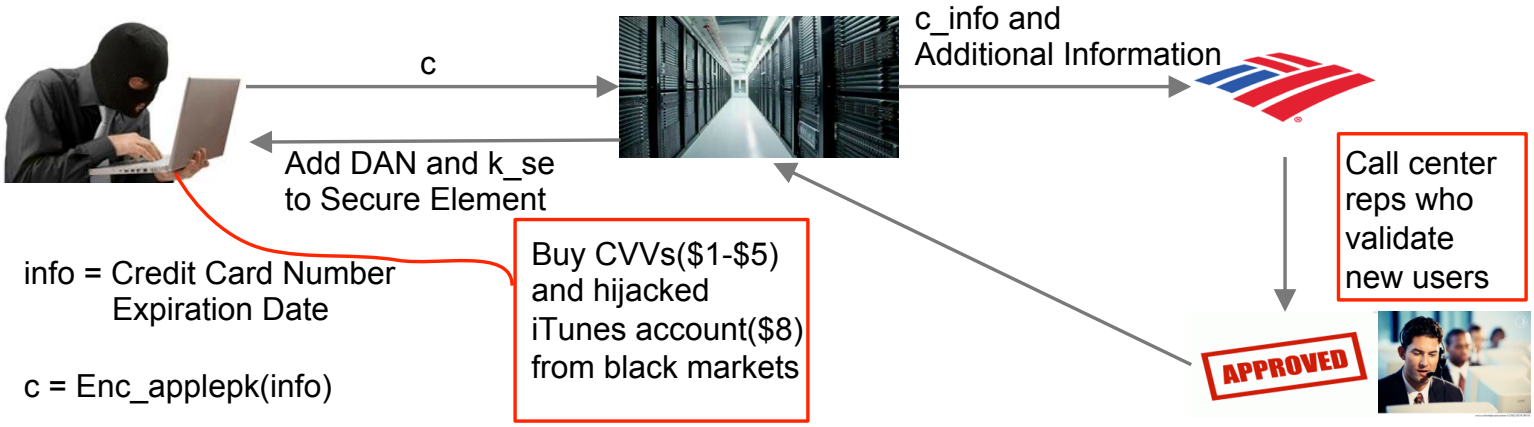
Decrypt with merchant's private key and send to payment network

Stolen Credit Card Data

Dumps is fraudster language for the **raw information** on the card's magnetic strip, and can be obtained by capturing the data through a point-of-sale device that has been infected with malware. Dumps are mainly used at **main street** merchants.

CVVs is fraudster language for credit card records that may include the cardholder name and address, card number, expiration date, and CVV2 (the three digits on the back of a card). CVVs can only be used with **online** retailers.

Apple Pay Frauds

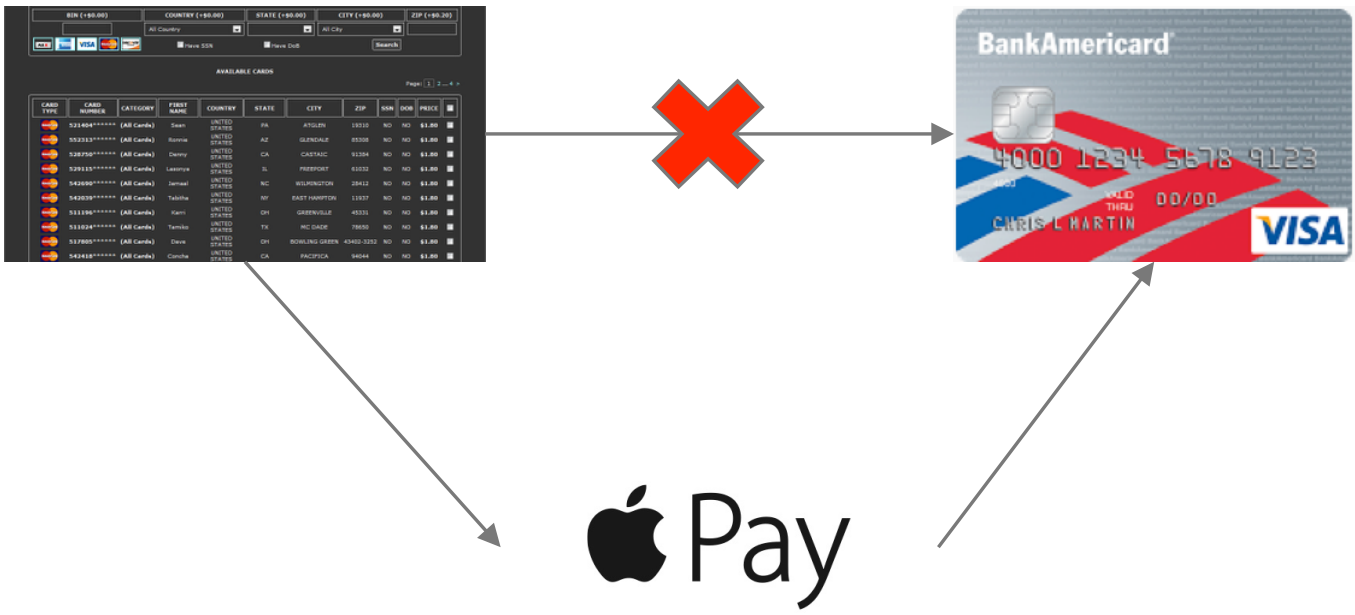


Additional Information contains:

- Last four digits of phone number
- Device name
- Rounded latitude and longitude
- iTunes Account Activity information

Fraudsters are calling the call center themselves to **alert the bank about a trip out of town** so that fraud rules looking for abnormal transactions do not trip them up.

Apple Pay -- Your Personal Credit Card Forge Factory



Whose Fault?

Apple

- Required banks to do additional verification (calls, login to banks) just one month before Apple Pay launch
- Simplified the sign-up process (collect and provide less information)
- Erased the limitations of CVVs

Banks

- Call center based validation process

Solution?

— Upload pictures of credit cards or photo IDs in card verification process. (Driver's License...)

— Compare the mobile service's billing address with the card account holder's billing address.

— Periodic identity checking. (email verifying)

References

- Apple Pay security and privacy overview: https://support.apple.com/en-us/HT203027
- Apple Pay Programming Guide: https://developer.apple.com/library/ios/ApplePay_Guide/
- iOS Security Guide 2014: https://www.apple.com/br/privacy/docs/iOS_Security_Guide_Oct_2014.pdf
- RAMPANT: EXPLAINING THE CURRENT STATE OF APPLE PAY FRAUD: http://www.droplabs.co/?p=1231
- Apple Pay: Bridging Online and Big Box Fraud: http://krebsonsecurity.com/2015/03/apple-pay-bridging-online-and-big-box-fraud/
- Social Engineering: https://www.owasp.org/index.php/Social_Engineering
- Apple Pay: An in-depth look at what's behind the secure payment system: http://www.engadget.com/2014/10/02/apple-pay-an-in-depth-look-at-whats-behind-the-secure-payment/
- How to Buy Stolen Credit Cards from the 'Amazon of Cybercrime': http://www.tomsguide.com/us/how-to-buy-stolen-credit-cards,news-18387.html
- Smart Mouse Traps and Lazy Mice: http://www.droplabs.co/?p=1204
- Apple Pay: a new frontier for scammers: http://www.theguardian.com/technology/2015/mar/02/apple-pay-mobile-payment-system-scammers
- Pointing Fingers in Apple Pay Fraud: http://www.nytimes.com/2015/03/17/business/banks-find-fraud-abounds-in-apple-pay.html