



OWASP

Open Web Application
Security Project

Threat Modeling against Payment systems

Dr. Grigorios Fragkos

Head of Offensive CyberSecurity at **invinsec** (@invinsec)

 @drgfragkos

Agenda

- Threat Modeling Highlights
- Point of Sale (#POS)
- Point of Interaction (#POI)
- Locked and Unlocked POI devices
- Tricks with POI
- Tricks with Virtual Terminals
- The outcome of a Threat Modeling exercise

Threat Modeling

- A process by which potential threats can be identified, enumerated, and prioritized – all from a hypothetical attacker’s point of view.
 - The purpose of threat modeling is to provide defenders with a systematic analysis of the probable attacker’s profile; meaning, the most likely attack vectors, and the assets most desired by an attacker.
 - Threat modeling answers the questions “Where are the high-value assets?” “Where am I most vulnerable to attack?” “What are the most relevant threats?” “Is there an attack vector that might go unnoticed?”

Multiple approaches to threat modeling

- **OWASP** : www.owasp.org/index.php/Threat_Risk_Modeling
- **SAFECODE** : www.safecode.org (non-profit)
 - Software Assurance Forum for Excellence in Code
- Software centric threat modeling
- Security centric threat modeling
- Asset or risk centric threat modeling

Approaching Threat Modeling

- STRIDE stands for:
 - **S**poofing
 - **T**ampering
 - **R**epudiation
 - **I**nformation disclosure
 - **D**enial of service
 - **E**levation of privilege

Approaching Threat Modeling

- DREAD stands for:
 - **D**amage
 - **R**eproducibility
 - **E**xploitability
 - **A**ffected users
 - **D**iscoverability

Keep in mind..

Performing threat modeling provides a far greater return than spending £££s for fraud control for a system that has negligible fraud risk. Make threat risk modeling an early priority in your application design process.

#threatmodeling

POI Devices

- You have likely used a Point of Interaction (Chip & PIN device)
 - Remember your PIN; you need it for transactions
 - Keep your PIN safe; so no one can use your card



Assumptions

- ..from your side:
 - I will **not** mention POI manufacturers
 - I will **not** tell you which OS vendor(s)

Assumptions

- ..from my side:
 - You will behave after the presentation!
 - If you decide to fly to **#LasVegas** (after having seen all these tricks), you promise to take me with you (and pay for my plane ticket).
 - Seriously! ;)

Keep in mind..

It is getting easier by the day for fraudsters and cyber criminals to get their hands on “live” payment systems.

#attackwaitingto happen

Locked and Unlocked POI devices

- There are 2 types of POI devices (terminals); the ones which are Locked and the ones that are Unlocked.
 - The Unlocked ones, have no open ports.
 - The Locked ones, have 1 open port
- The locked POI is controlled by an Electronic Cash Register (ECR or ePOS), which is responsible for unlocking the device, opening a new receipt and accepting a transaction.
 - Locked POI devices can be found unattended!
 - Locked POI devices, can be unlocked in 7 to 10 sec.

Getting to know the rules

- Until recently it was so much easier..
 - Successful transactions were sent every 24 hours.
 - Clearing the transactions cache used to be a few clicks away.
- Since last year onwards..
 - Successful transactions are sent back in “real-time”
 - Clearing the transactions cache is now protected by a “secure code” (like a PIN, that only few people know)

Ways to never actually pay for a transaction..

- Bypass restrictions
 - Get access in the internal network, send commands to the POI: Close Receipt, Open New Receipt with new Amount, Complete Payment
 - Pay as normal but instead of trying to clear the cache, remove the OS completely, with a quick key combination.

How to..

- Delete the OS
 - After Reset, when a specific string appears on the screen
 - [Key 1] > [Key 2] > [Key 3] > [Key 4]
 - Terminal resets and displays boot screen
 - Everything is deleted
 - Keeps BIOS, Hardware configuration file, Ethernet configuration file

Do you speak POS?

Name	Type	Length	Example value HEX	Info
Control	Byte	1	F1	Constant Control byte
Control	Byte	1	F1	Constant Control byte
Control	Byte	1	F1	Constant Control byte
PacketType	Byte	1	08	Packet type
Frame Content Length	Integer			Length of the frame content
Application Type	Integer			Application type
Connection	Integer			Connection ID
Command	Integer	4	00000001	Depends on the request to be sent.
DataLength	Integer	4	00000105	Length of the data container
...Data...	string	var	...	Message data.



Commands to send

253 - POS Open
254 - POS Close
251 - Receipt Open
252 - Receipt Close

250 - Cancel Transaction
370001 - Change Amount

Transaction Types _

0x04 = Refund (merchandise return)

0x05 = Combined cancellation and refund (make a cancellation if the given original Transaction ID and amount match, else make a refund).

0x09 = Send the offline transactions.

0x0F = Pre-authorisation (a.k.a. Pre-Auth)

0x13 = Quasi-cash

0x14 = Game winning credit

0x17 = Balance inquiry

How to pay with someone else's card..

- Because you don't know the PIN:
 - While in payment state, press [Key] > [Key]
 - It prints a receipt which you need to sign instead (PIN is not used)
 - The message on the screen says that the transaction is accepted and prompts the user with "Remember Signature". **#SignatureMode**
 - If you hit Green, the message will go away and the customer copy will start printing



How to pay with someone else's card..

- Because you don't know the PIN and you don't want to sign the retailer's copy either:
 - Enter the Card upside down.
 - POI thinks the Chip is not working and asks you to swipe the card instead.
 - Should raise a fallback alert to the card issuer.
 - Swipe the card and transaction is complete.

How to pay with someone else's card..

- By “blocking” the wireless communication:
- Wait for 2 tries and press [Key] for manual
- Tells you to contact the bank to give you the “proceed” code.
 - If == AMEX, enter any 2 digits.
 - If != AMEX enter a number that validates the Luhn algorithm.
- Maybe clear the OS after the payment is accepted? ;)



How to get paid instead of paying..

- Find an unattended locked POS:
- Unlock the POS using a key combination.
- Enter your card and request a **#refund** to be send to your account.
 - Enter your card but this time request a refund to be send to your account, “marked” as winnings from gambling!?!

How to get a significant discount..

- During a normal payment, when the POI is **unlocked**:
 - Pull your card out (just 2 mm).
 - Wait 6 seconds!
 - Press: MENU > [key] > Enter the amount you want to pay > OK > [Push Card In] > [key]
 - Give the POS back to the merchant
 - Smile! :D

The Cuckoo example..

- Assuming you are an existing merchant:
 - Instead of tampering with the POI and risk getting caught, **replace** the target POI with one of your own.
(#ConArtist skills highly recommended) #WhiteCollar
 - **No one** checks the serial numbers at the back of the POS before every single transaction. ;)

POS & Contactless

- All of the above apply, plus..
 - No need for PIN
 - If you are prompted for a PIN use any of the previous methods
 - You can charge a card more than once using different contactless POS devices only milliseconds after each transaction!
 - Do not have two POS devices trying to read the same card at the same time.
 - **#Contactless** have a £30 limit per transaction (not in all countries). There are considerations to remove the limit in the near future.
 - More work to be done...

Now that you know all that, we need Card Info

How many people take pictures and put their card information online?

#creditcard, #debitcard, #cvv

If you want to go shopping..



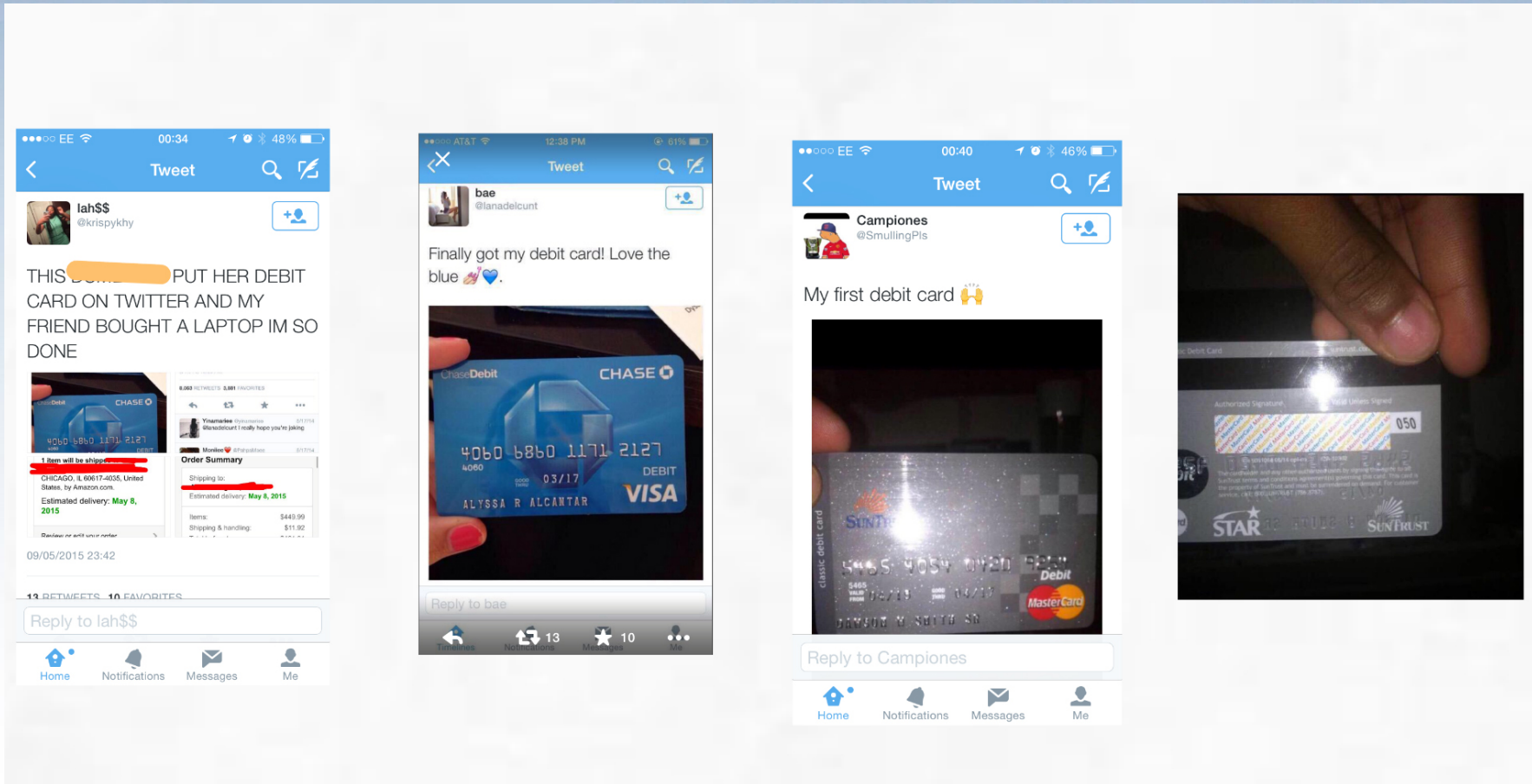
We need Cards..



We need Cards..

The collage consists of four screenshots from a mobile device, likely an iPhone, showing tweets related to debit cards. The first screenshot shows a tweet from user 'keeps' (@kinomatika) dated 11/05/2015 at 23:14. The tweet text is 'look at my new debit card tho. look how far i have fallen' and includes a photo of a hand holding a Visa debit card with a colorful, abstract design. The second screenshot shows a search for 'debitcard' with 'Top Tweets' selected. It features a tweet from 'chele naudin' (@chele_bely) dated 11/05/2015, which says 'walking into target with money on my debit card... Pray for me' and includes a photo of a card activation card with instructions: '1. Call 1.888.1.925.6 or login to make a card 2. Sign the back 3. Start using y'. The third screenshot shows the same search results with 'All Tweets' selected, displaying a tweet from 'ash' (@ashleeromanx3) dated 10/05/2015, which says 'my asu id/debit card lololol' and includes a photo of an ASU student debit card. The fourth screenshot is a close-up of the ASU student debit card, showing the 'SUN DEVILS ASU' logo, 'MIDFIRST BANK' branding, and the cardholder's name 'ASHLEE N ROMAN' and ID number '120-230811'. The card is set against a background of a colorful, patterned fabric.

We need more Cards..



We need more Cards..

The collage features several elements related to debit cards:

- Twitter Search:** A screenshot of a Twitter search for "debit card pretty" showing tweets from users like FineGIRL and Matthew Gile.
- Chase Disney Visa Debit Card:** A close-up image of a hand holding a blue Chase Disney Visa Debit Card featuring Mickey Mouse and other Disney characters.
- 420 Debit Card:** A tweet from Gezina Baehr (@gezinathebaehr) dated 23/03/2015, showing a close-up of a Visa Interac card with the number 901 0420 792 and the date 10/18. The tweet includes the text "Hahahahahah 420 on my new debit card!!!! #meanttobe".
- Lost Debit Card:** A tweet from Matthew Gile (@M_Fox132) dated 11/11/2014, stating "I lost my ID, credit card, debit card and cash, but the haircut I got today looks pretty good."
- Square Cash App:** A tweet from Rahim Sonawalla (@rahims) dated 23/03/2015, discussing the Square Cash app and its features.
- Close-up of Card:** A close-up image of a Visa Interac card with the number 901 0420 792 and the date 10/18.

We need a few more Cards..

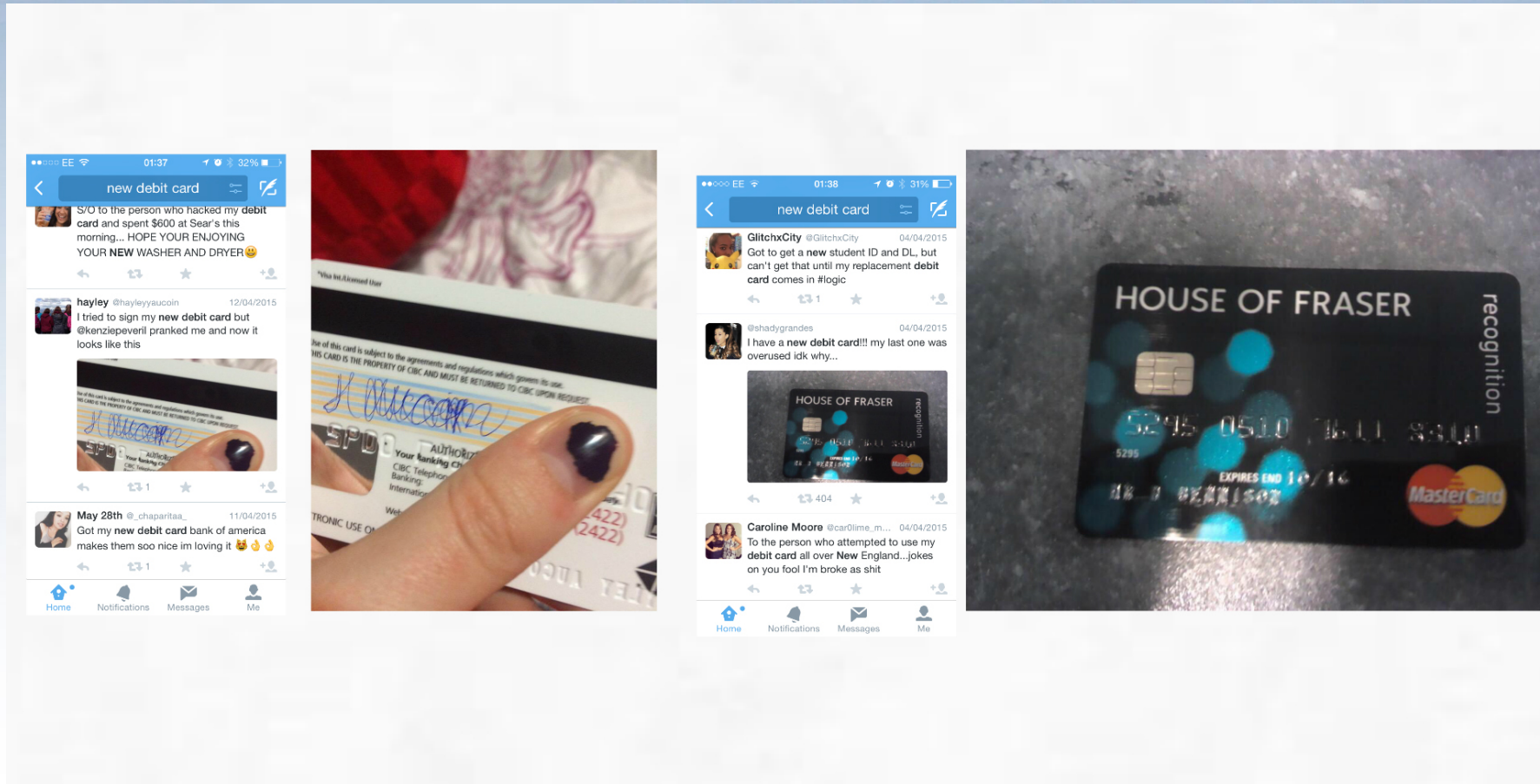


We need a few more Cards..

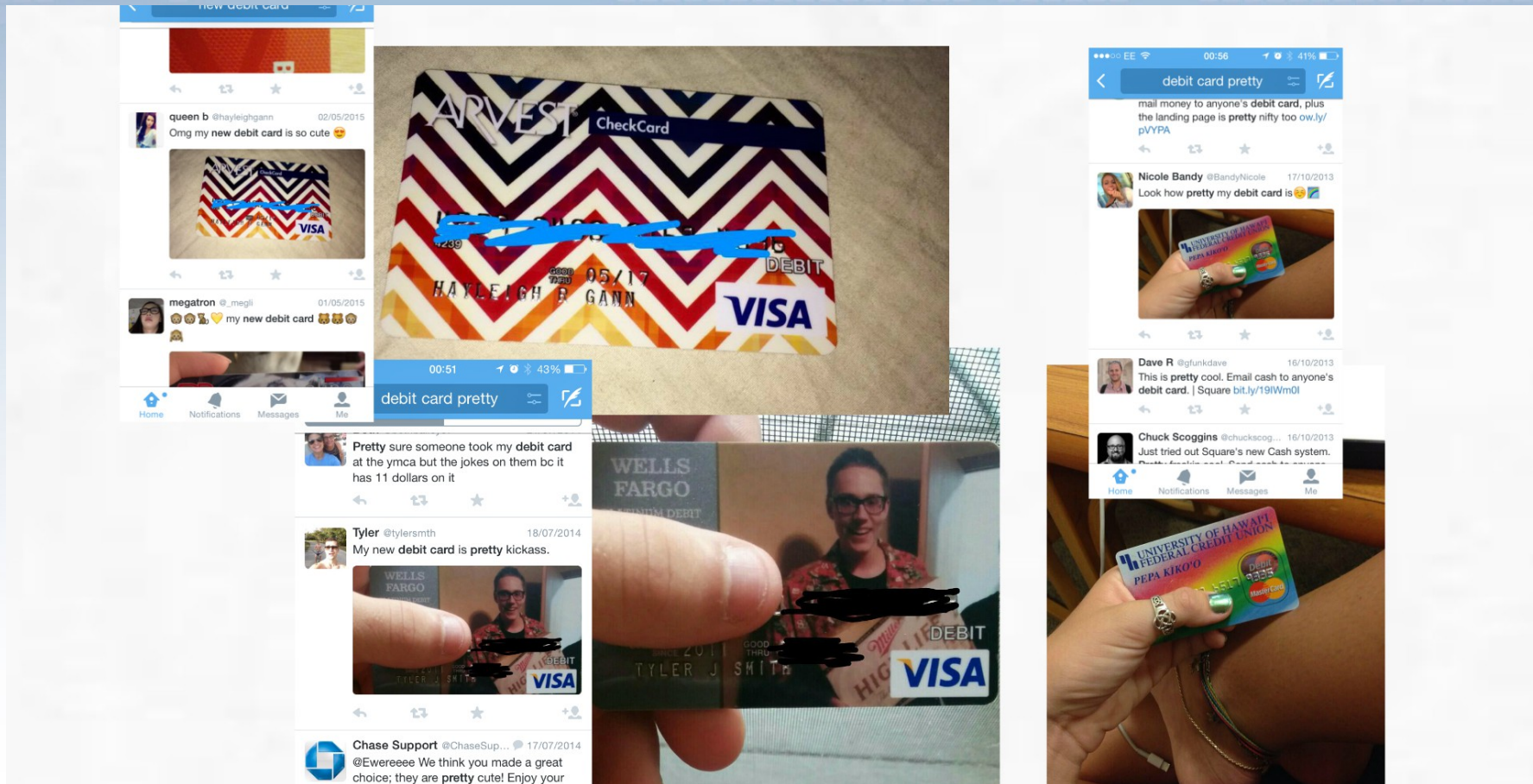
The collage features several elements:

- Twitter Post 1:** A tweet from @emotionalplayer dated 06/03/2015 with the text "boy am I glad I got a new debit card". It includes a photo of a card with the number 420 and a "NOT VALID UNLESS SIGNED" warning.
- Twitter Post 2:** A tweet from Wave Crest Group (@wcpaym...) dated 06/03/2015 with the text "New Mexicans could soon be able to buy lottery tickets with a debit card if a new bill passes: bit.ly/1Fi1Mi8 #gaming #debit".
- Twitter Post 3:** A tweet from Asif Mohtesham (@ITechAsFreak) dated 06/03/2015 with the text "My answer to Why is my new hfc debit".
- Twitter Post 4:** A tweet from King OJ (@Official_RyRy) dated 18/03/2015 with the text "fabrics from the market" she almost forgot to order me a new debit card." It includes a photo of a red Boone County National Bank debit card with the number 5112 7101 0060 8544 and the name ALEXANDER M RITTER.
- Twitter Post 5:** A tweet from Priestess Moonfire (@julle_ma...) dated 18/03/2015 with the text "Can't get a new debit card til tomorrow, someone send me a pizza."
- Card Photos:** Two photos of a "pulse Jeanie PLUS" card, one showing the front with the number 420 and the other showing the back with the name Jeanie PLUS.

My precious..



My precious..



Regenerating the hidden digits..

The collage consists of several elements:

- Top Left:** A tweet from Commerce ISD (@CommerceISD) dated 10/03/2015, titled "new debit card". The text says: "Check out the new Tiger Visa Debit Card from Alliance Bank. 5 cents of every transaction goes to CISD. #cisdtigers". It includes a small image of the Tiger Visa card.
- Top Center:** A close-up photograph of a Tiger Visa debit card. The card is black with orange tiger stripes. It features the "TIGERS" logo, "Alliance Bank", and "COMMERCE ISD". The card number is 4924 4600 0000 1793, and the name is BLAKE COOPER. The expiration date is 04/18.
- Top Right:** A tweet from StormKiller (@TheStormKiller) dated 2012/2013, titled "debit card pretty". The text says: "Good job @NBCNews pretty sure Ryan Evans wanted her debit card number shown to millions For your target fraud story." It includes a small video thumbnail.
- Top Far Right:** A screenshot of a news broadcast from NBC 4. The text at the bottom reads: "TUTTLE PUBLIC SCHOOLS: ATHLETIC EVENTS CANCELED TODAY".
- Bottom Left:** A tweet from #Danyele@* (@iamdanyele) dated 06/03/2015, titled "New customized debit card". It includes a small image of a Wells Fargo debit card.
- Bottom Center:** A close-up photograph of a Wells Fargo Platinum Debit card. The card is silver and features a photo of a woman. The name is WELLS FARGO PLATINUM DEBIT. The card number is 9 9056 4170, and the name is WELLS FARGO DEBIT. The expiration date is 04/18.
- Bottom Right:** A terminal window titled "Bitvise xterm - root@10.0.0.118:22". The output shows a Python script running:

```
root@kali:~/Documents/gLuhn# ./gLuhn.py 442518?990561770
Attempting to generate 10 PAN combinations for: 442518?990561770
[+] Valid PAN 4425180990561770
Total valid PAN generated: 1
root@kali:~/Documents/gLuhn#
```

McDumpals

News FAQ Terms of service Settings Logout

Account

Orders Payments Wallet Cart

Bins All countries Expires from Expires to Any type Card brand Card category Code

* Checks price: \$0.2
* Dumps from packs are not refundable
* Citibank is currently not refundable
* Maestro is currently not refundable

10 records per page Search all columns

Track 2	Country	Brand	Type	Category	Exp. date	Code	Name	Checker
No data available in table								

Showing 0 to 0 of 0 entries

← Previous Next →

© McDumpals - 01:23:18 News · FAQ · Terms of service · Support

Moving to Virtual Terminals..

Writing a memory scraping POS malware?
Do they have to? ..once they get to know the system(s)?

#POSmalware

Virtual Terminals

- Software applications.
 - Provided by the Payment eco system, such as the Acquirer, Payment Service providers, and more.
 - VT can work without a POI connected to it.
 - Difference between ECR (ePOS) and VT; The ECR doesn't work without a POI.
 - You can key-in the card details on a VT
 - VT software needs to be PA-DSS compliant (according to PCI), while the ECR is only being checked if it stores CHD (!)

Penetration Testing for PA-DSS

- The main objective is to identify if it is possible to get your hands on the CHD.
 - SQLi or any other types of injections
 - Buffer Overflows
 - Cryptographic storage
 - Insecure Communications
 - Improper Error Handling

Threat Modeling

- Assessing the logic of the VT and look into the payment process from a malicious “merchant's” perspective.
 - A repeatable process to find and address all threats to your product.
 - The earlier you can start the better, with more time to plan and fix.
 - Must identify the problems when there is still time to fix them (before the ship day).
 - Third-Party Components & S/W Development Life Cycle (SDLC).
 - End Goal: Deliver more secure products.

At a first glance..

- Possible to modify the configuration files
 - One of the easiest tricks to demonstrate this was to change appears on the POI screen.



At a first glance..

- Possible to modify the configuration files
 - By the way, these new types of POI devices are interesting. They can communicate with the VT via Bluetooth if needed, while being powered over USB.



At a first glance..

- Possible to modify the configuration files
 - Each device comes with a different pairing key.



VT identifiers

- How do they distinguish between merchants?
- Each VT has “identifiers”.
- Based on the “identifiers”, payments are settled against the correct merchant.
- Editing however the “identifiers” in the configuration files messes with the encryption key, thus the encrypted header is not valid when a payment needs to be sent, and the transaction cannot be completed.

Anticipating shifts in fraudulent activity..

An alternative scenario to POS malware..

#POSmalware

Thinking outside-of-the-box

- Internet shoppers are expected to spend £748m on Boxing Day (£519,000 a minute)
- So, what you will need:
 - A valid Merchant ID
 - First year programming skills
 - Know how to cover your tracks
 - Think outside-the-box, focus on the money, not the card numbers!
 - Have attended this presentation!

Thinking outside-of-the-box



Thinking outside-of-the-box

- Last but not least:
 - Have attended this presentation!

Getting the job done

- You could create & spread malware that can:
 - Change the “identifiers” on every VT
 - Delete the encrypted header file
 - Reboot the VT application
- Covering your tracks by:
 - Change the “identifiers” to what it was.
 - Delete the encrypted header file
 - Clean the LOG file & Reboot the VT application

Delivery method

- Spread undetectable malware:
 - Much easier than one might think.
 - Activate it on.. Boxing Day / Black Friday?
 - Simply wait for the money to be settled to your bank account.

Bonus Round

- If the VT is written in JAVA
- Get the POS into asking you to Key-in the card:
 - Enter Card Number as normal
 - Add 70 years to your expiration date
- Alter the VT date by adding 70 years:
 - Perform any transaction you like

Conclusions

- Security is an ongoing process and the **Payment Card Industry** enforces compliance for a good reason.
- Cybercriminals are not better than **YOU**.
- It is easier to break things than fix stuff; it needs a **security mindset to keep things secure**.
- Cybercrime pays until you get caught.
- If you break the law, **you are going to get caught!**
- Technology is changing fast & won't be long before **you get caught**.

One last set of tips..

- Educate merchants **not to leave the POI unattended** at any time.
- To stay ahead of cybercriminals **consider such scenarios** & ensure you anticipate / can recognize, such **fraudulent activity in real-time**.
- Consider **threat modeling exercises**.
- If you **demagnetize your mag-stripe**, you cannot withdraw cash.
- You may **remove the CVV** from your card, if you memorize it.
- **Don't put a photo of your card online!**
- Use **RFID block: sleeves, wallets, cards**.

Time for Questions!

Thank you for your attention

#LetsGoShopping

 **@drgfragkos**