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.

#**threat**modeling

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.

#**attack**waiting**to**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..

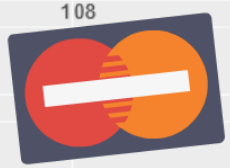
- Bypass restrictions
  - Get access in the internal network, send commands to the POI: Close Receipt, Open New Receipt with new Amount, Complete Payment
  - Pay as normal but instead of trying to clear the cache, remove the OS completely, with a quick key combination.

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?

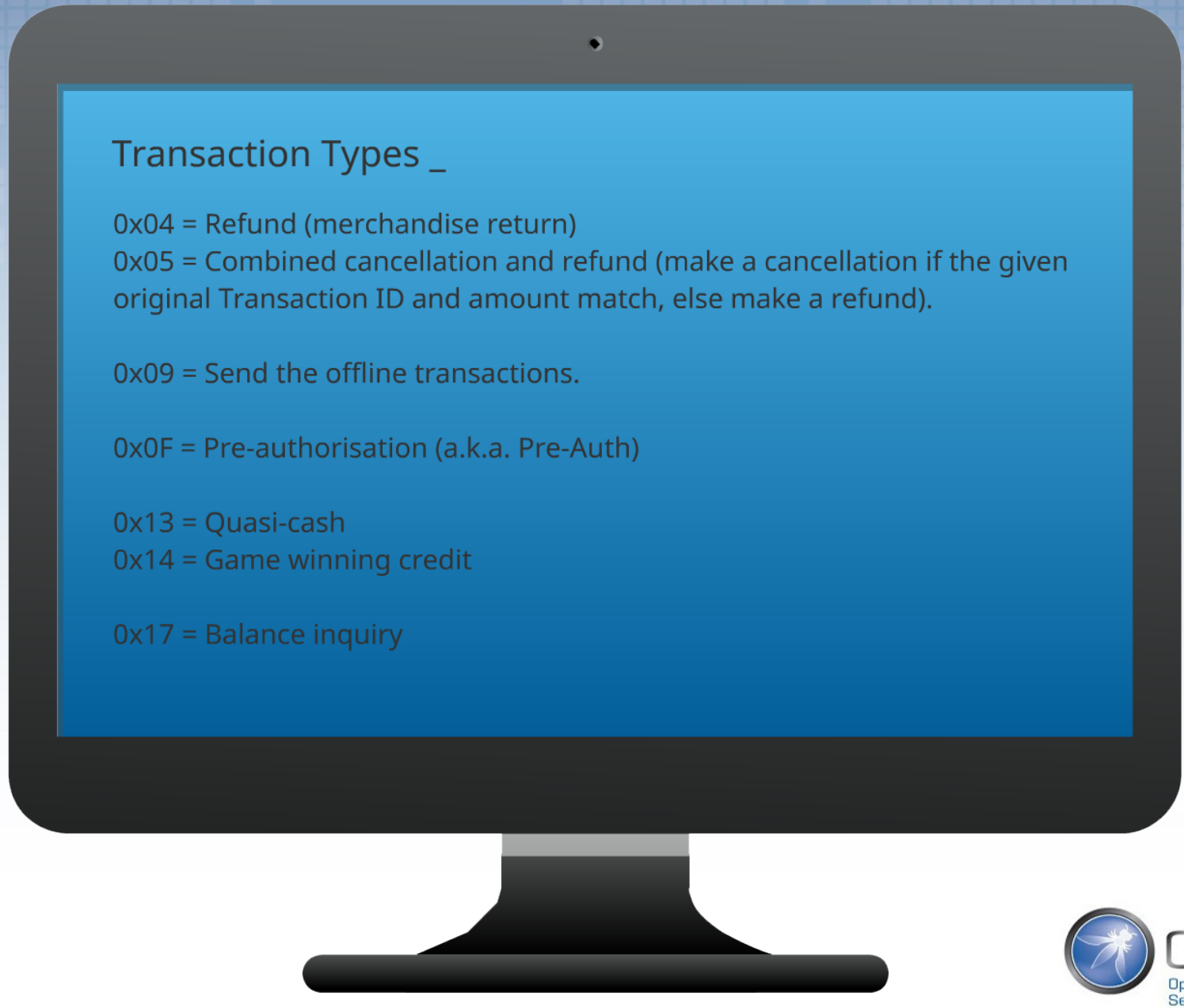
Name	Type	Lenght	Example value HEX	Info
Control	Byte	1	F1	Constant Control byte
Control	Byte	1	F1	Constant Control byte
Control	Byte	1	F1	Constant Control byte
PacketType	Byte	1	08	
Frame Content Length	Integer			
Application Type	Integer			
Connection	Integer			
Command	Integer	4	00000001	Depends on 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



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

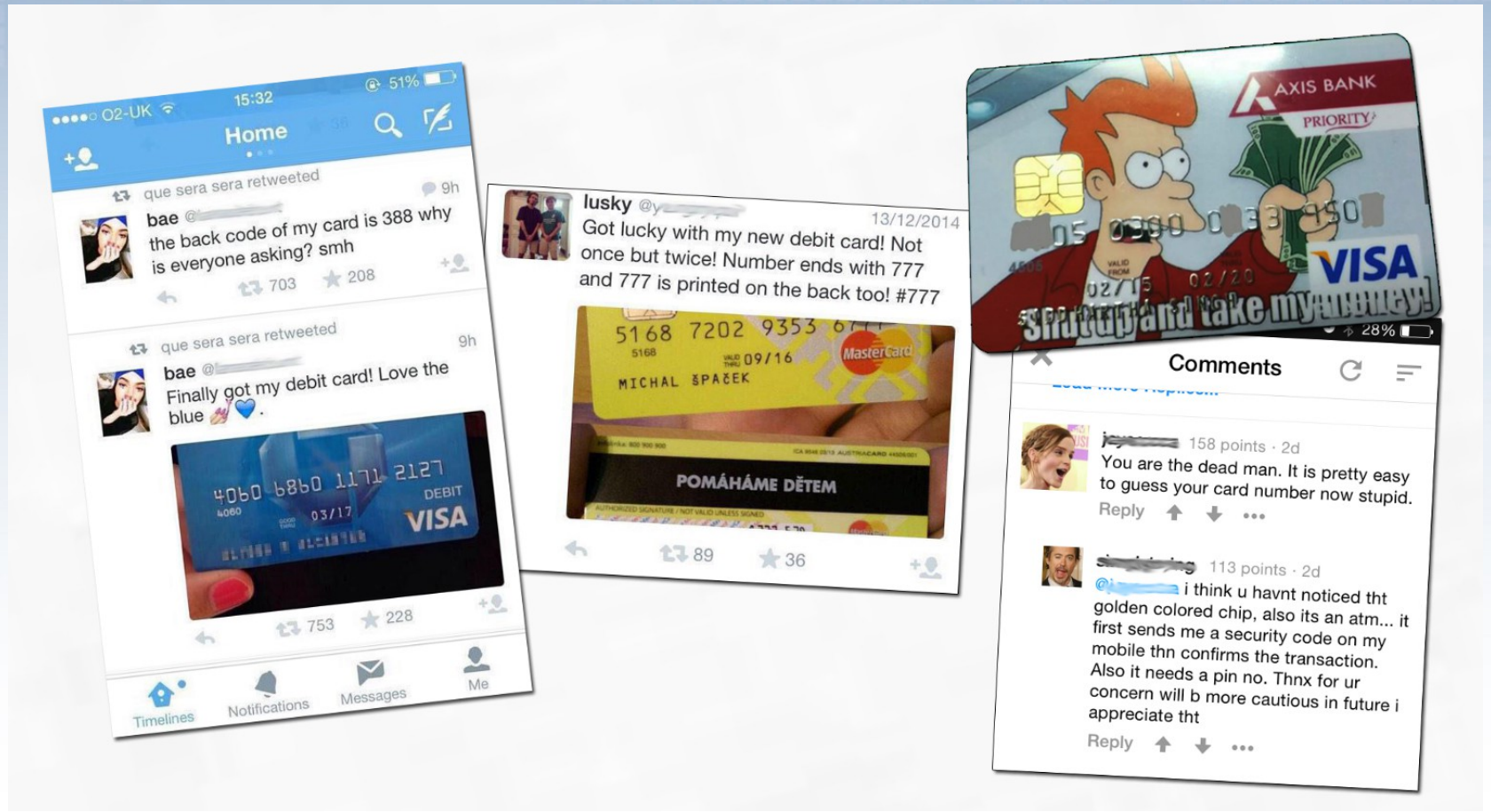
- All of the above apply, plus..
  - No need for PIN
  - If you are prompted for a PIN use any of the previous methods
  - You can charge a card more than once using different contactless POS devices only milliseconds after each transaction!
  - Do not have two POS devices trying to read the same card 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 may people take pictures and
put their card information online?

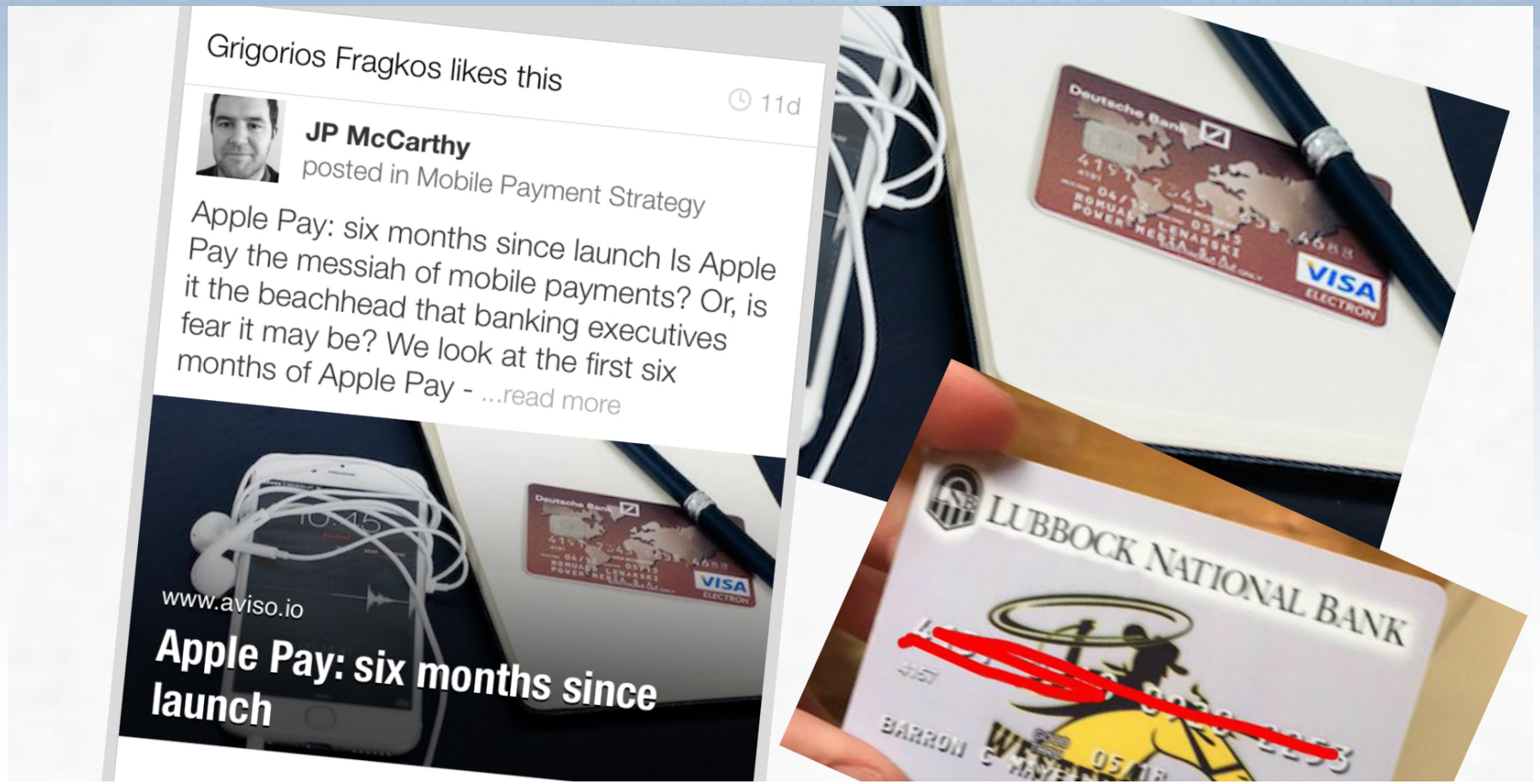
#creditcard, #debitcard, #cvv

If you want to go shopping..



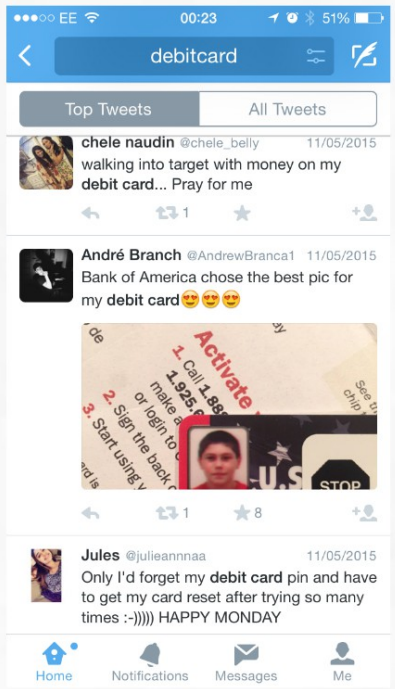
OWASP
Open Web Application Security Project

We need Cards..



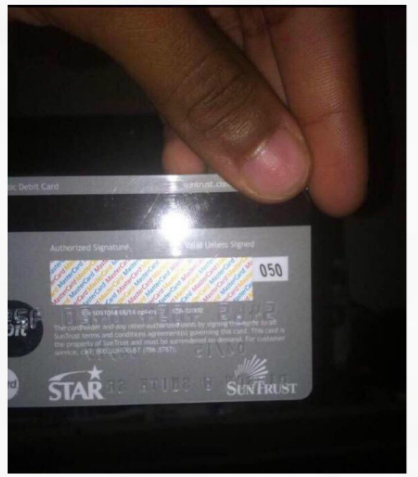
OWASP
Open Web Application Security Project

We need Cards..



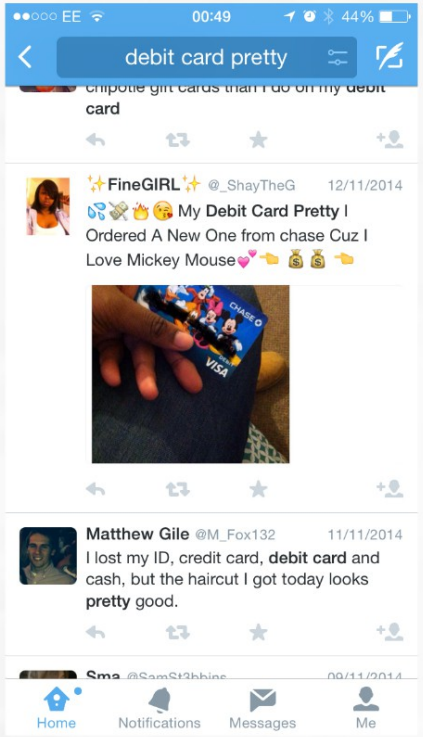
OWASP
Open Web Application Security Project

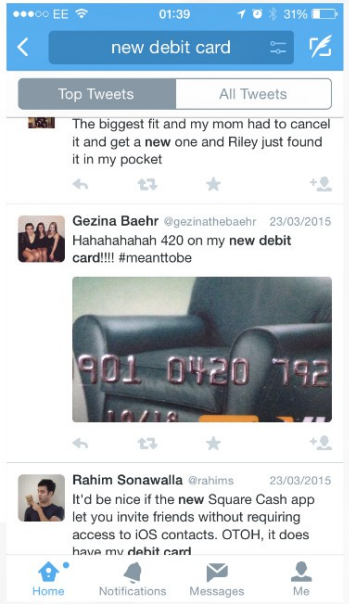
We need more Cards..



OWASP
Open Web Application Security Project

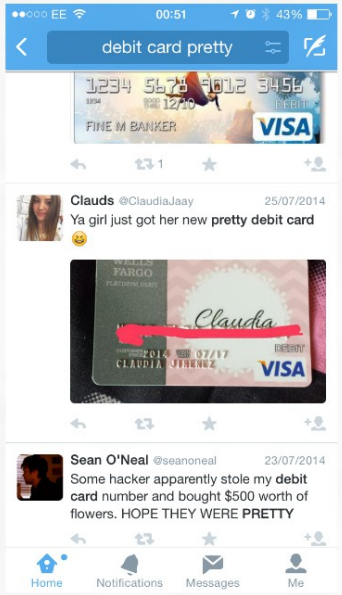
We need more Cards..





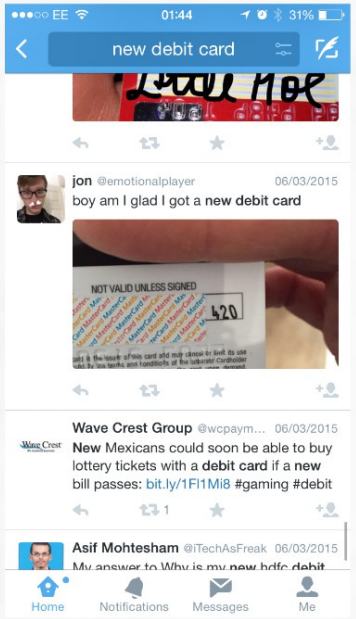
OWASP
Open Web Application Security Project

We need a few more Cards..



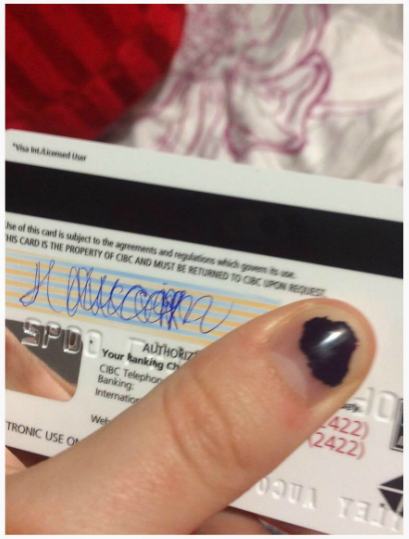
OWASP
Open Web Application Security Project

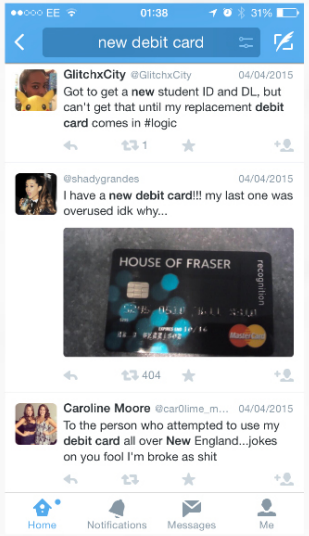
We need a few more Cards..



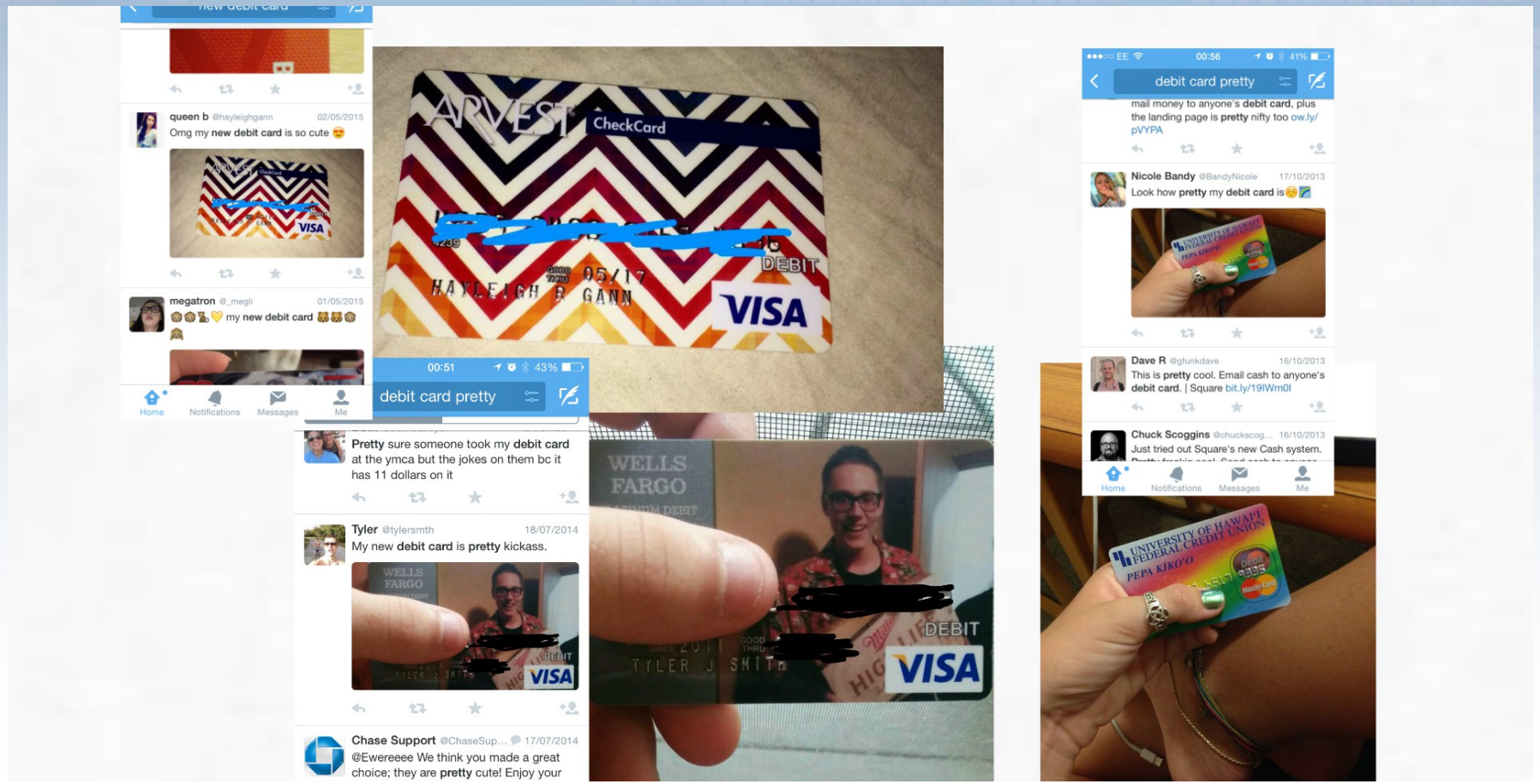
OWASP
Open Web Application Security Project

My precious..



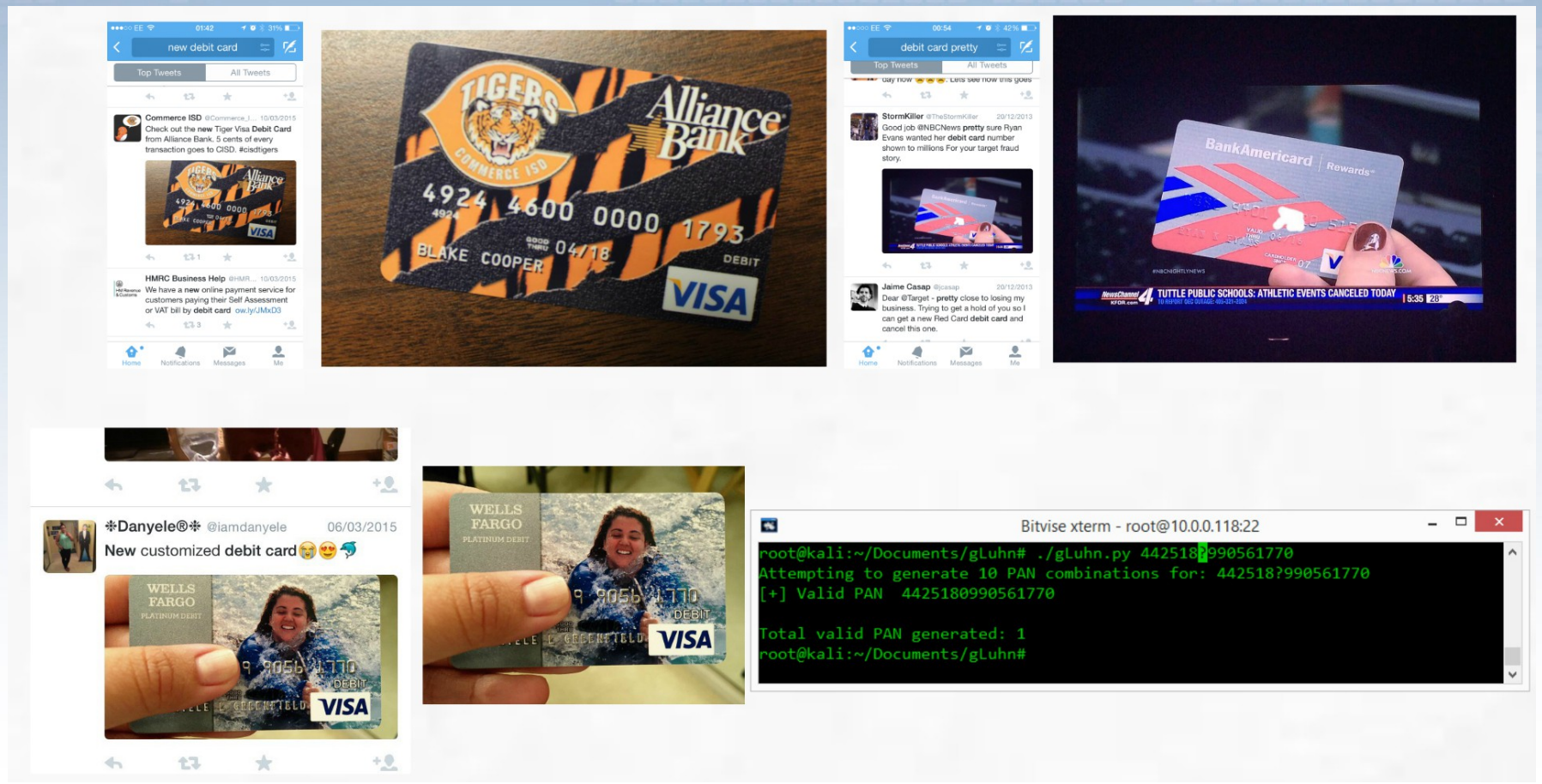


My precious..



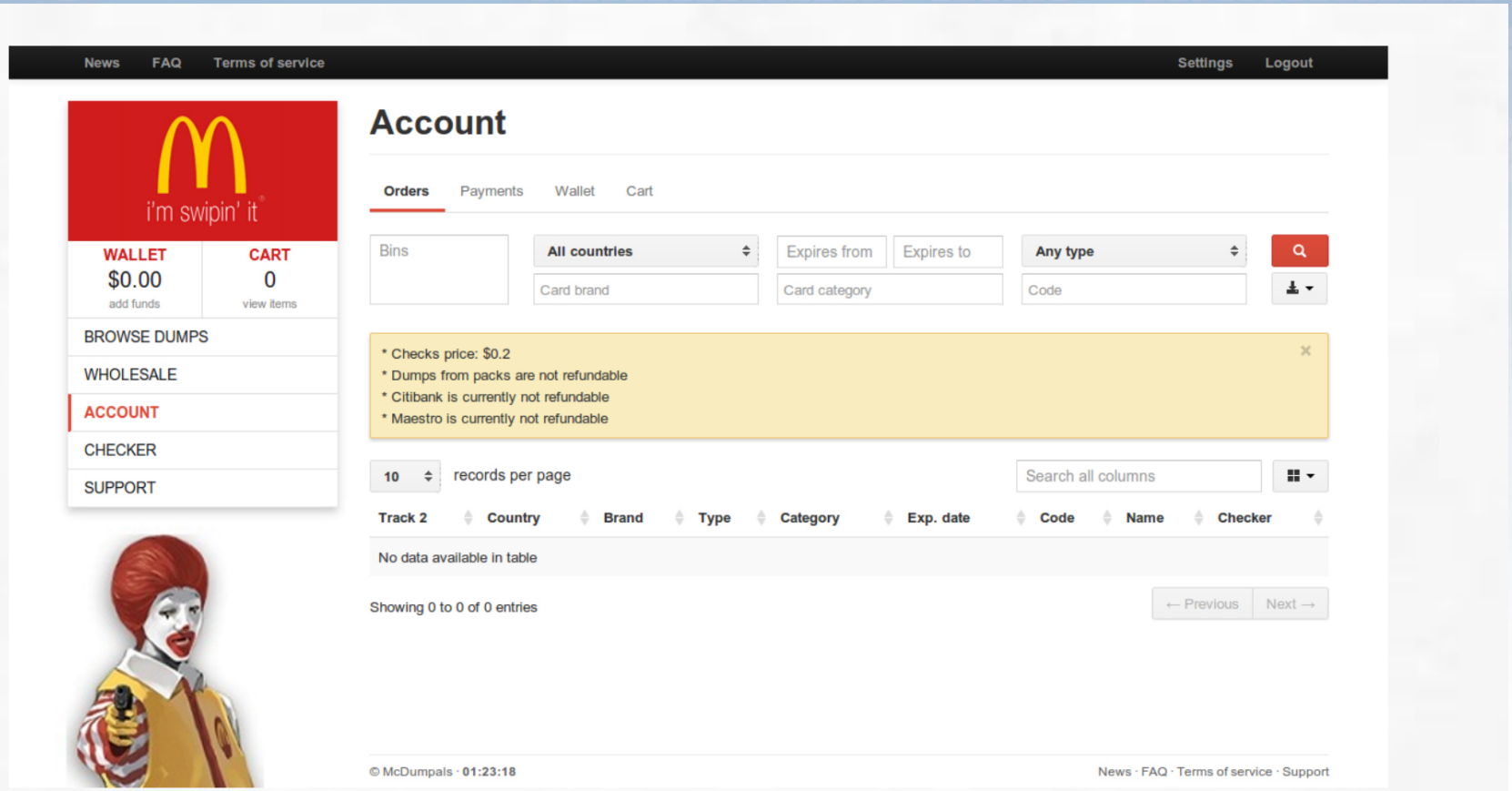
OWASP
Open Web Application Security Project

Regenerating the hidden digits..



OWASP
Open Web Application Security Project

McDumpals



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 compliant 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**