AS SEEN ON TV

ATMs

We Kick Their Ass

“Leet is my name and ATMs is my game” ;)

Yaniv “Lament” Miron
Marcel “MC” Carlsson

security 1337s at BREAKPWN

CONFIDENCE 2014

About Marcel “MC” Carlsson

- Intercontinental man of mystery who has worked with business penetration testing for many years

- Co-Founder @ Breakpwn

- Speaker at POC, Shakacon, CONFidence, Hackmiami, Nordic Sec Conf etc

- Cert monkey (SEPP, CISSP, CISM, CISA, ISO27k etc) and former QSA and PA-QSA

BREAKPWN

About Yaniv Miron

- Security Researcher

- Co-Founder @ Breakpwn

- Speaker @ cons – BlackHat/PoC/IL.Hack/CONFidence/Hacktivity/Syscan/Hacker Halted/Hack Miami/Shakacon/NSC and more

- Found security vulns in Microsoft, IBM, Apache, Oracle products and more

- CISO certified & Certified locksmith

BREAKPWN

About Breakpwn

- Top Notch Breakazoids
- Founded by Marcel Carlsson & Yaniv Miron
- International and Independent
- Advanced hacking services
- We r0x0rz
- Labs v2

ALL CHARACTERS
AND EVENTS IN THIS TALK —
EVEN THOSE BASED ON REAL
PENTESTS — ARE ENTIRELY FICTIONAL.
ALL HACKING STEPS ARE
IMPERSONATED.....POORLY. THE
FOLLOWING TALK CONTAINS
COARSE LANGUAGE AND DUE TO
ITS CONTENT IT SHOULD NOT BE
VIEWED BY ANYONE.

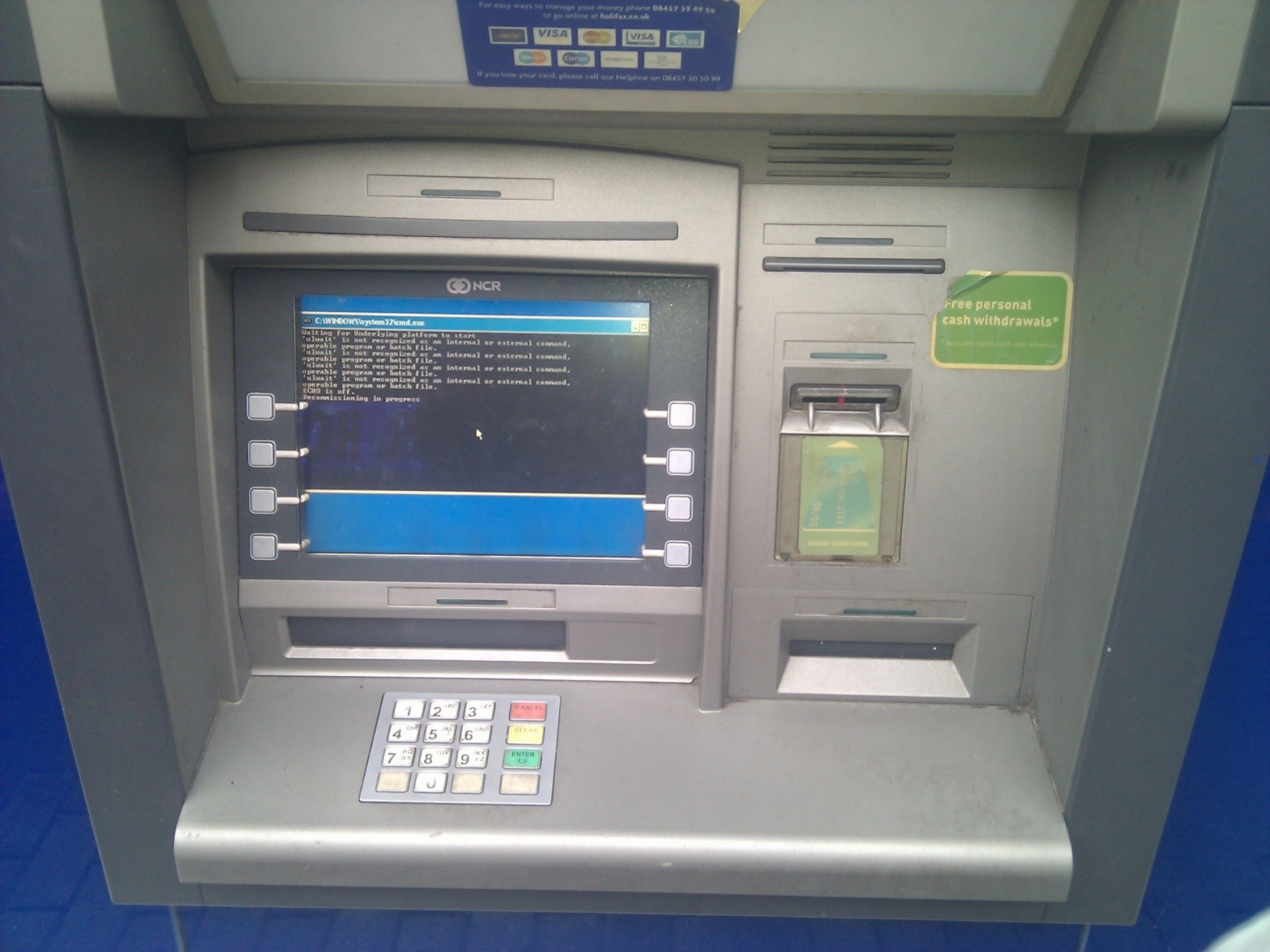
WE CAN NOT SHOW ACTUAL EVIDENCE

Agenda

- **General intel about ATMs**
- **Common weaknesses in ATMS**
- **How to pwn ATMs**
- **Specific attack execution**
- **Q&A**

ATMs in General

- **Automated Teller Machine (ATM)**
- **Take out or deposit cash and perform basic account transactions**
- **Pay your bills, buy tickets, top up etc**
- **ATMs are often old and expensive**
- **More common in certain countries**
- **Vendors >> NCR, Diebold, Wincore Nixdorf, Hyosung, Triton etc**



For easy ways to manage your money phone 08457 39 49 59
or go online at halifax.co.uk
VISA
VISA
Cirrus
If you lose your card, please call our Helpline on 08457 20 30 99
NCR
C:\WINDOWS\system32\cmd.exe
Free personal
cash withdrawals*
INSERT CARD HERE
CANCEL
CLEAR
ENTER

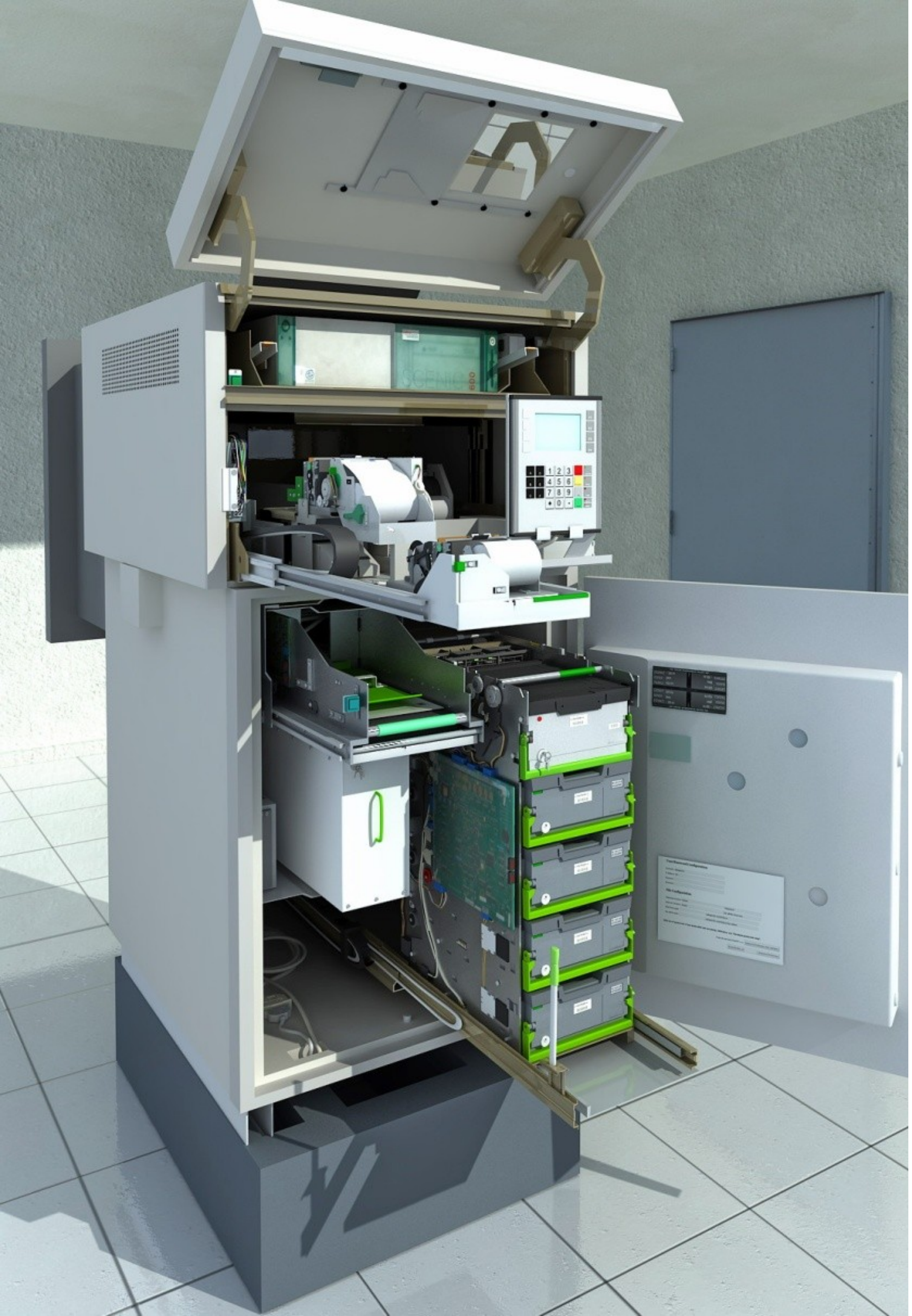
```
Waiting for Underlying platform to start
'ulwait' is not recognized as an internal or external command,
operable program or batch file.
'ulwait' is not recognized as an internal or external command,
operable program or batch file.
'ulwait' is not recognized as an internal or external command,
operable program or batch file.
'ulwait' is not recognized as an internal or external command,
operable program or batch file.
ECHO is off.
Decommissioning in progress
```

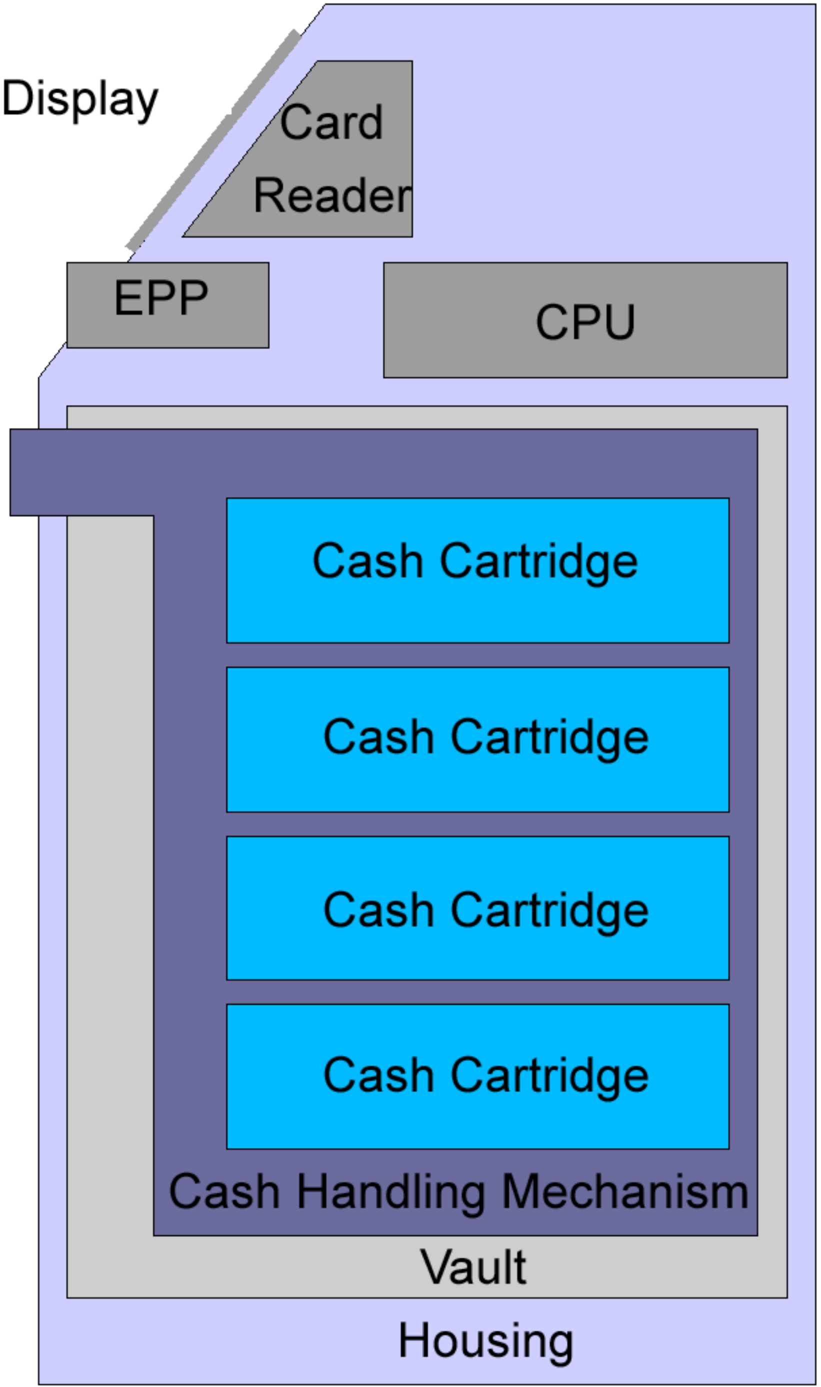
ATM Physical Locations

- Inside bank or bank lobby
- On the street “hole in a wall”
- Shopping malls, convenience stores, gas stations, hotels etc
- On-premise vs off-premise
- Pretty much everywhere

ATM Physical Components

- **PC inside a steel box with lock**
- **Cash cartridges in a locked safe**
- **Cash dispenser and receipt printer**
- **Display monitor and numeric pin pad**
- **Admin display and keyboard (back)**
- **Card reader, camera, sensors/alarm**
- **Network hardware, cables and locked cabinet**



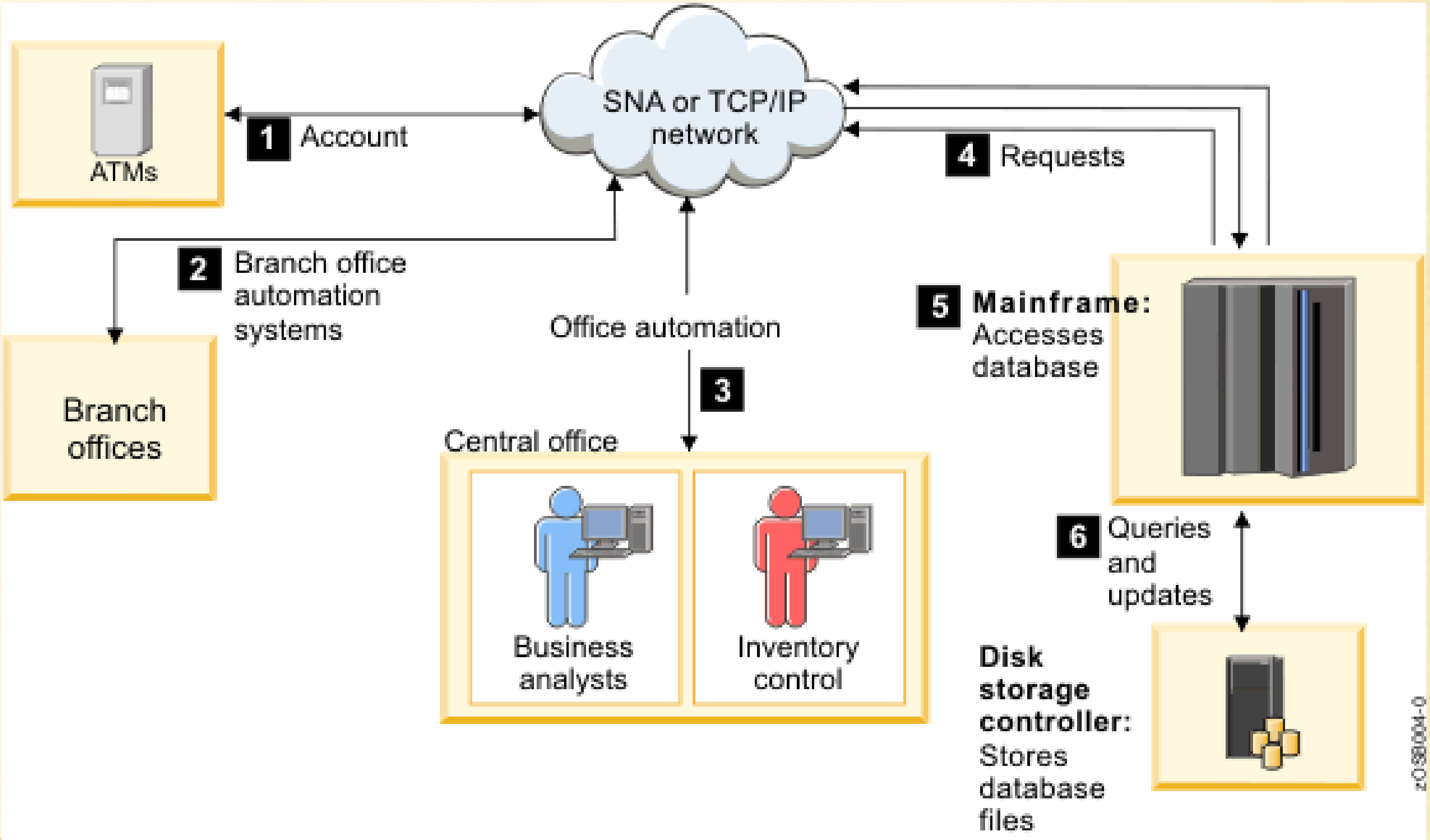


http://en.wikipedia.org/wiki/Automated_teller_machine

ATM Networks

- ATMs communicate over Electronic Fund Transfer (EFT) networks
- ATM Controllers (ATMC) route ATM traffic
- ATMCs are interconnected
- Mainframe host connect to ATMCs
- ATMs in development, testing, staging networks connect to host

ATM Networks



https://publib.boulder.ibm.com/infocenter/zos/basics/index.jsp

ATM OS

- Mostly Microsoft Windows OS
- Windows XP
- Windows XP embedded
- Migrations to Windows 7
- Old school >> Windows 2000, NT and CE(!)
- Some Linux variants also

ATM Applications

- **XFS (CEN XFS) platform common**
- **API for accessing ATM hardware components**
- **Middleware to integrate XFS variants**
- **Programmable application >> Windows OS + XFS**
- **Big difference with regards to ATM application complexity across world**

ATM Hardening - Physical

- Locks and thick steel attempt to slow down attackers
- Ink dye >> bank notes stained when attack is detected
- Gas explosion sensor (alleged) >> suppression chemical released to neutralize explosive gas

ATM Hardening - Physical

- Encrypting pin pad and secure key management protect transactions
- Alarms and sensors (temperature, tilting, vibration and open door)
- Various anti-skimming mechanisms
- Remote ATM monitoring for abnormal time-outs etc
- Often there are gaps in the hardening implementation – w00t!

ATM Hardening - Logical

- ATM OS often not stripped down or hardened according to business need
- Vulnerable applications not removed e.g. Movie Maker, Adobe Reader
- Broken and out of date anti-malware
- Weak hardening allows privilege escalation attacks

Let’s party like it’s 1999, you geeky b*st*rds.

But Wait...

THERE'S MORE!

ATM Hardening - Logical

- **Boot settings often not secure**
- **Possible to boot from USB, CD/DVD or PXE**
- **Run own attack Linux distro on ATM**
- **Possible to use ATM to attack other ATMs on same network**
- **Possible to use ATM to attack backend mainframe or other shared critical infrastructure components**

ATM Hardening - Logical

- **Lack of or weak file integrity checking mechanisms**
- **Possible to tamper with any file**
- **Possible to add malicious code and root kits and modify registry**
- **Possible to enable debug mode and write card holder data in log file**
- **Possible to downgrade applications to older vulnerable versions**

ATM Hardening - Data

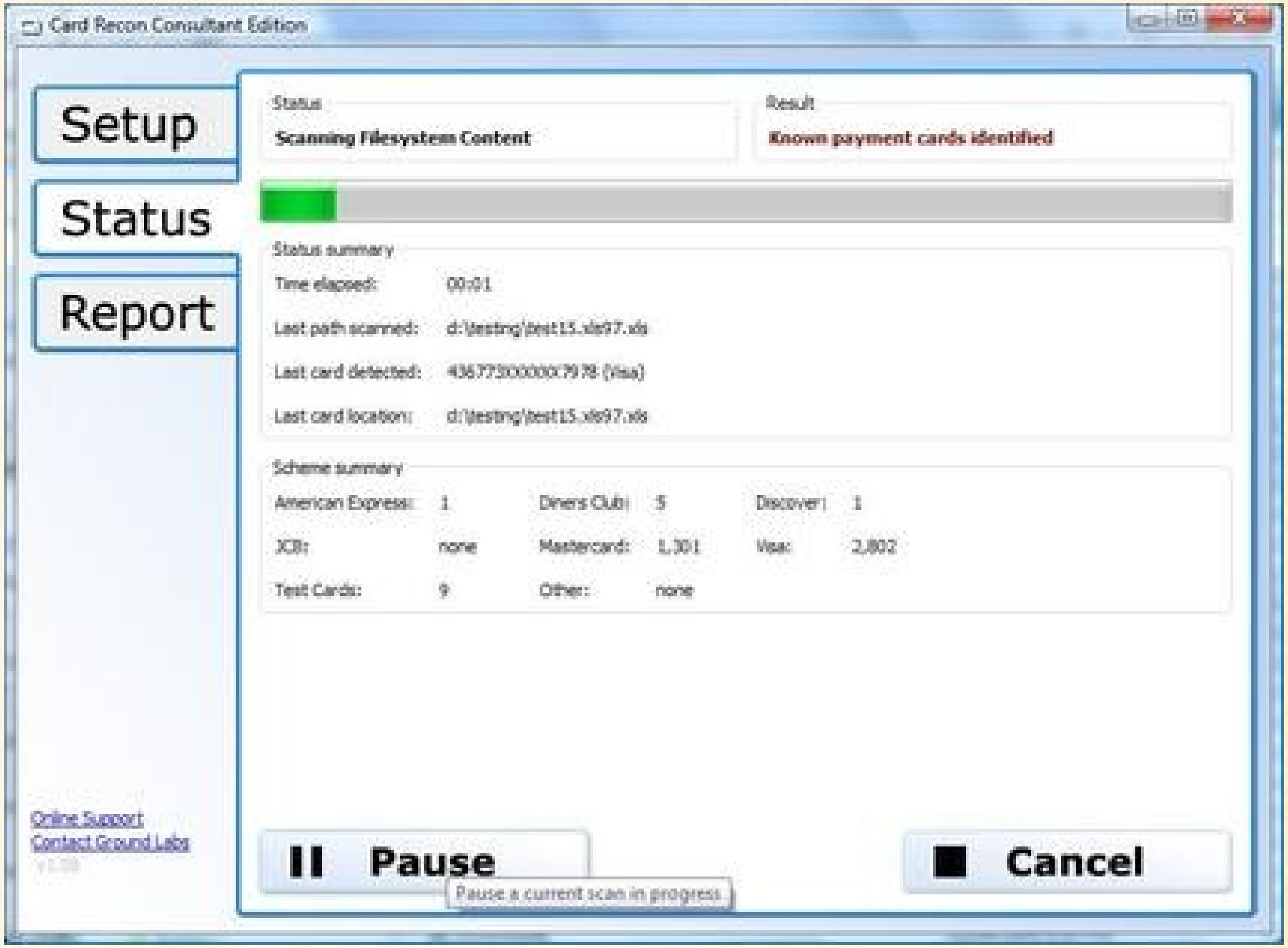
- Legacy data is often not removed from file system e.g. full PAN (credit card number)

- Debug mode was enabled but forgot to disable >> juicy data in log files e.g. full PAN and even full track data etc

- Legacy machines may have PAN etc printed on paper due to old configuration

- ATM hard drive usually not encrypted

ATM Hardening - Data


Card Recon Consultant Edition
Setup
Status
Report
Online Support
Contact Ground Labs
Pause
Cancel
Pause a current scan in progress

Status
Scanning Filesystem Content

Result
Known payment cards identified

Status summary

Time elapsed: 00:01
Last path scanned: d:\testing\test15.xls97.xls
Last card detected: 436773XXXXXX7978 (Visa)
Last card location: d:\testing\test15.xls97.xls

Scheme summary

American Express:	1	Diners Club:	5	Discover:	1
JCB:	none	Mastercard:	1,301	Visa:	2,802
Test Cards:	9	Other:	none		

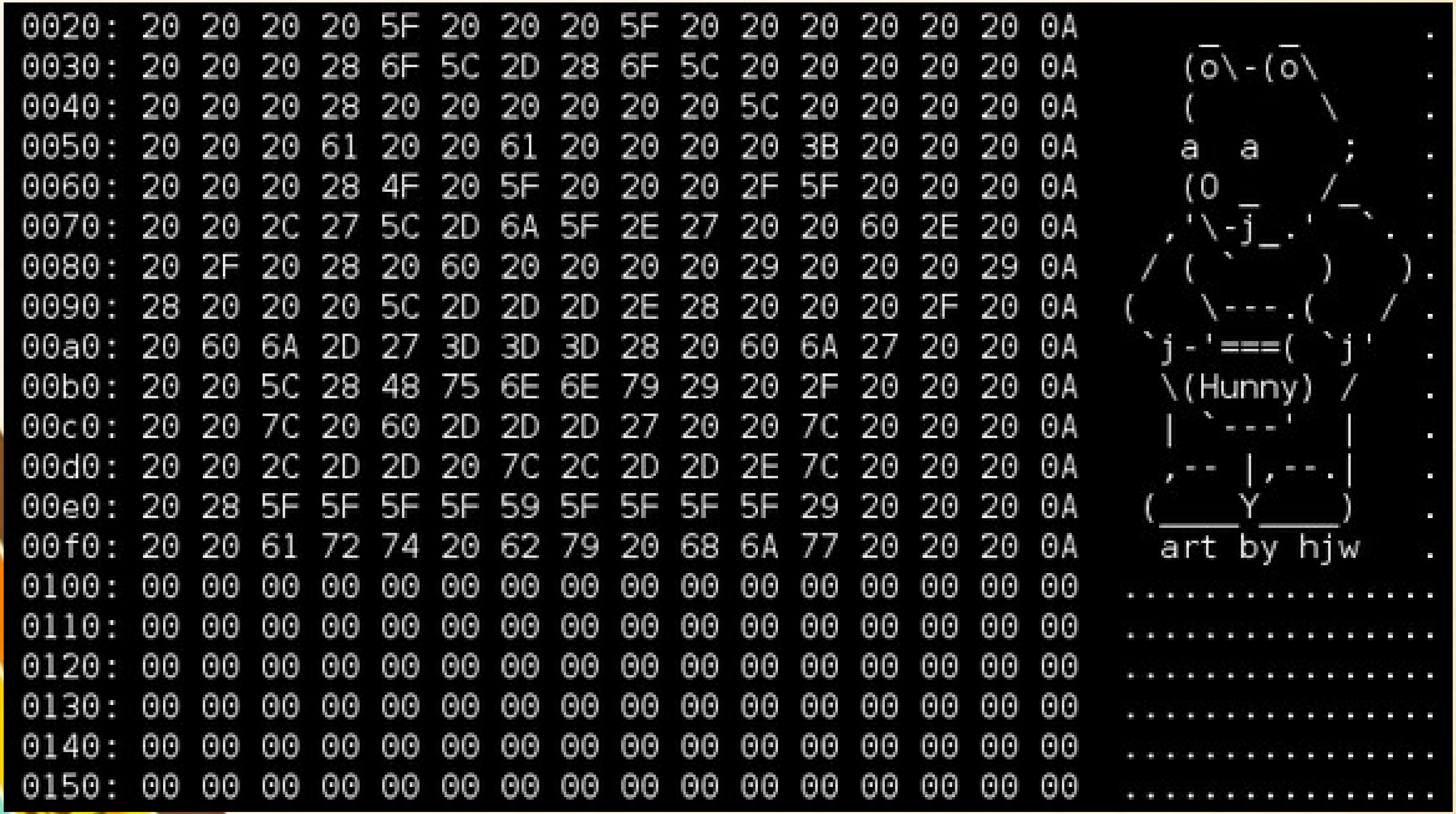
http://www.freebsdnews.net/2011/03/14/ground-labs-announces-support-freebsd/

BREAKPWN

ATM Hardening - Data

- **Weak or no hardware integrity checks**
- **Possible to remove hard disk**
- **Possible to inject malicious code or any content into hard disk**
- **Possible to copy and steal data from hard disk**
- **Scrape memory and grab goodies**

ATM Hardening - Data



```
0020: 20 20 20 20 5F 20 20 20 5F 20 20 20 20 20 20 0A      _   _      .
0030: 20 20 20 28 6F 5C 2D 28 6F 5C 20 20 20 20 20 0A     (o\-(o\     .
0040: 20 20 20 28 20 20 20 20 20 20 5C 20 20 20 20 0A     (      \    .
0050: 20 20 20 61 20 20 61 20 20 20 20 3B 20 20 20 0A     a  a    ;   .
0060: 20 20 20 28 4F 20 5F 20 20 20 2F 5F 20 20 20 0A     (O _   /_   .
0070: 20 20 2C 27 5C 2D 6A 5F 2E 27 20 20 60 2E 20 0A    ,'\-j_.'  `. .
0080: 20 2F 20 28 20 60 20 20 20 20 29 20 20 20 29 0A   / ( `    )   ).
0090: 28 20 20 20 5C 2D 2D 2D 2E 28 20 20 20 2F 20 0A  (   \---.(   / .
00a0: 20 60 6A 2D 27 3D 3D 3D 28 20 60 6A 27 20 20 0A   `j-'===( `j'  .
00b0: 20 20 5C 28 48 75 6E 6E 79 29 20 2F 20 20 20 0A    \(Hunny) /   .
00c0: 20 20 7C 20 60 2D 2D 2D 27 20 20 7C 20 20 20 0A    | `---'  |   .
00d0: 20 20 2C 2D 2D 20 7C 2C 2D 2D 2E 7C 20 20 20 0A    ,-- |,--.|   .
00e0: 20 28 5F 5F 5F 5F 59 5F 5F 5F 5F 29 20 20 20 0A   (____Y____)   .
00f0: 20 20 61 72 74 20 62 79 20 68 6A 77 20 20 20 0A    art by hjw   .
0100: 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00  ................
0110: 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00  ................
0120: 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00  ................
0130: 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00  ................
0140: 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00  ................
0150: 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00  ................
```

http://remember.gtisc.gatech.edu/~brendan/honeybleed.patch

ATM Hardening - Credentials

- Default passwords never changed

- Passwords shared between different accounts

- Same passwords are used in production, development, staging and test environments for same account

- Similar passwords in use – easy to guess and move laterally into new systems or domains

ATM Patch Process

- Often no or slow process
- Vendor dependencies
- Often outsourced to third party
- Lack of integrity checking
- Sometimes old school >> CDs
- Possible to inject malicious patches or attack central patch server

ATM Operations

- Often too wide local/remote access
- Often weak authentication
- Often weak authorization
- Often weak compartmentation
- Often weak security monitoring
- Often weak security logging
- Possible to exfiltrate data unnoticed

ATM Eco System

Cash Replenisher

Software Developer

Hardware Vendor

Bank Employee

Service Technician

Customer

and often even more than above …

ATM Eco System

- **Threats from all involved entities**
- **Multiple targets**
- **Different attacker motives and goals**
- **Complex system**
- **Heavy reliance of physical security and network isolation**

ATM Complex Trust Relationships

Hardware vendor

OS vendor

Application Vendor

Cash Handling Vendor

Developer

Outsourcing Vendor

Bank Employee

Networking Vendor

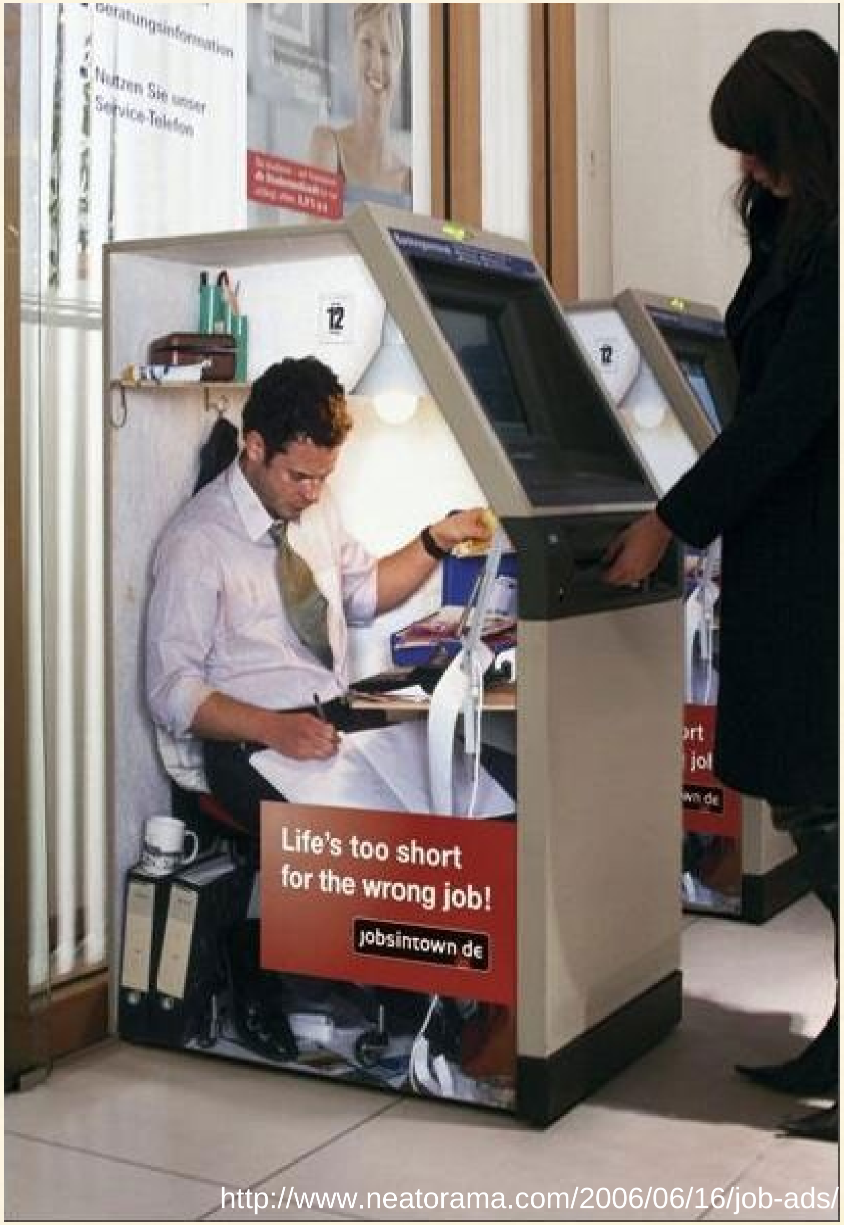
Telco Vendor

Sys Admin

ATM Complex Trust Relationships

- **Trust relationships span all layers**
- **Physical, logical, processes, meatware and data**
- **Complex due to number of entities having access**
- **Large attack surface (also for trusted insiders)**
- **Weaknesses in trusted entity can lead to compromise of ATM #opsec**

ATM Complex Trust Relationships


Beratungsinformation
Nutzen Sie unser Service-Telefon
Life's too short for the wrong job!
jobsintown.de

http://www.neatorama.com/2006/06/16/job-ads/

How to pwn ATMs

- Intelligence gathering
- Weakness identification
- Plan attack
- Execute attack
- Steal data
- Rinse and repeat
- Clean up and profit

Breach physical perimeter

- Gain physical access
- Buy ATM keys online or pick lock
- Use a crow bar :P
- Social engineer job role that has or can provide physical access
- Work for entity that has physical access to ATM (bank, vendor etc)

Hardware pwnage

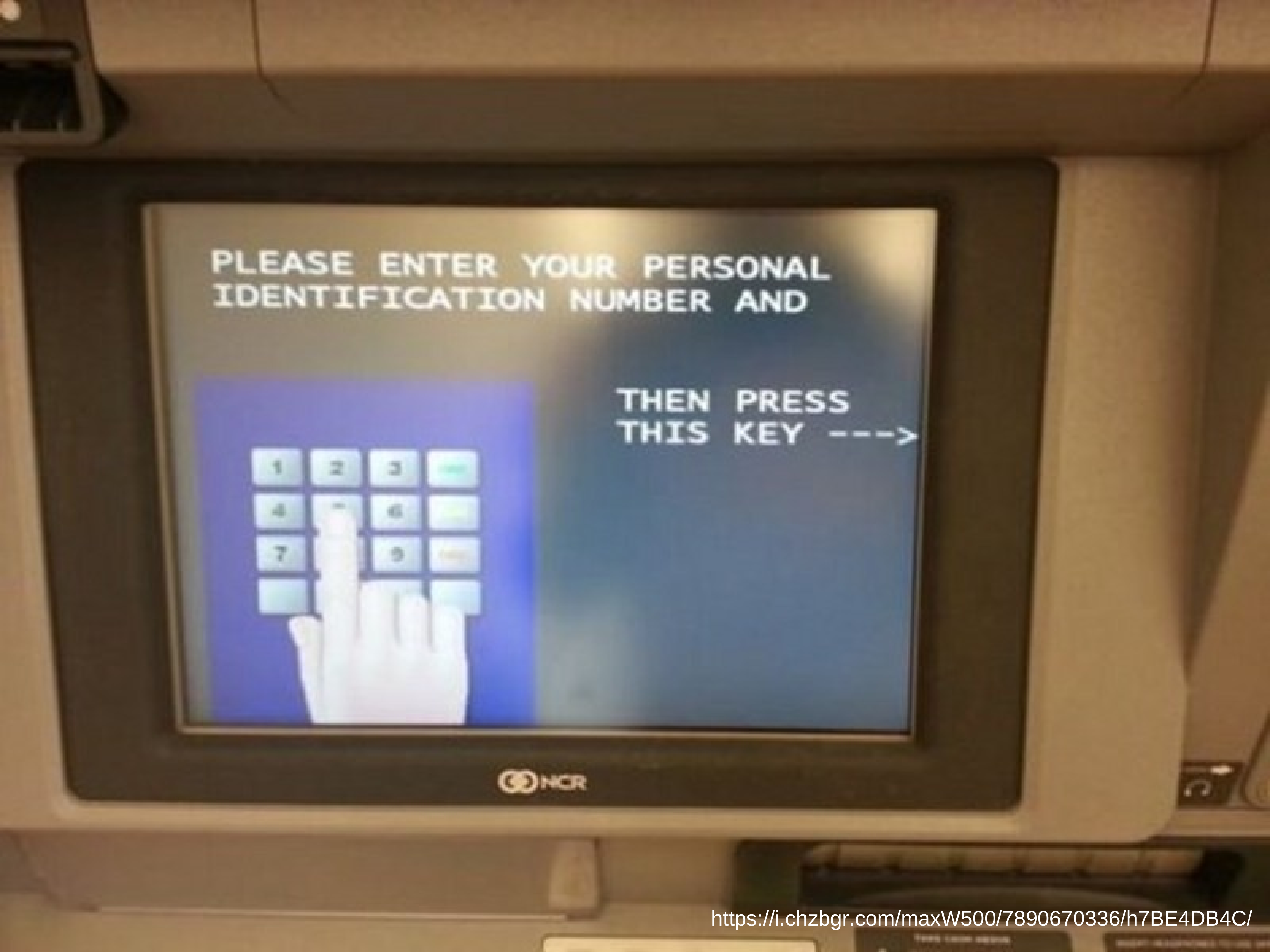
- **Attach hardware keylogger to steal credentials**

- **Install hardware with 3G modem for remote access**

- **Use credentials to attack other ATMs or move laterally into other networks and systems**

- **Use FireWire attack to dump memory or escalate privilege**

BREAKPWN



PLEASE ENTER YOUR PERSONAL
IDENTIFICATION NUMBER AND

THEN PRESS
THIS KEY --->

https://i.chzbgr.com/maxW500/7890670336/h7BE4DB4C/

Busting authentication

- **Smart Cards? Yeah right…**
- **Default passwords**
- **Google search**
- **Hardware Keylogger**
- **Social Engineering**

Privilege escalation

- Exploits
- PStools
- DLL code injection
- FireWire
- Pick your pentest poison

Data Pilfering

- **Steal disk**
- **Copy disk**
- **Scan for PANs**
- **Install malware**

Detection bypass

- Alarm is not working/weak – Mess with the packets

- No/weak monitoring – disable local monitoring software/delete logs before being sent

- AV is weak - Packer/Edit file

- IDS/IPS - works?

- Tripwire etc - works?

Response bypass

- No response mechanism or process
- Weak response mechanism
- Weak response process
- Often not verified to be working

Network attacks

- Attack from remote management desktop
- Use ATM to attack backend
- Use ATM to attack trusted networks
- Use ATM to attack shared critical technology infrastructure

Meatware attacks

- **Social engineering works**
- **Vendor technicians**
- **ATM operators /application developers**
- **ATM system admins**
- **ATM business managers**
- **Auditors / Whitehats**
- **Security guards**

Pwning ATMs

Pwning ATMs – Steps

- **Obtain intel ! (this is what we did so far in this presentation)**

- **Best to be stealthy – if you are quiet you can stay longer**

- **Practice good opsec and minimize leaving any trails of any kind, no finger prints and no visible damage etc**

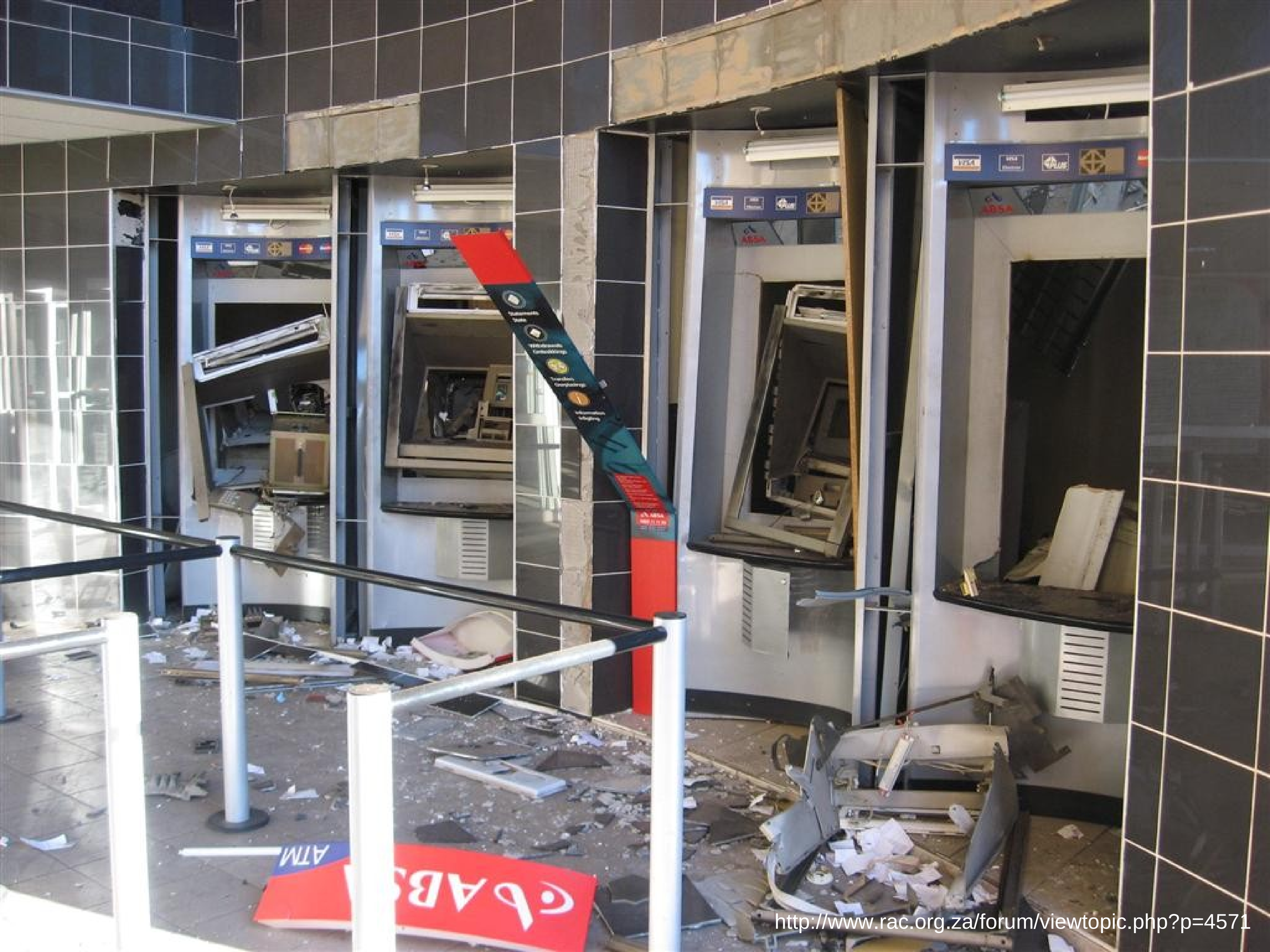
- **Work smart with the SE, not too many calls or many questions etc << “it’s all about them” – Robin Dreeke**

Pwning ATMs – General TIPs

- A single reboot takes long time (could take 20 minutes and more)
- Lack of proper testing means many controls are non-existent or broken
- Gaps all over the place (like broken alarms)
- Target areas between ”silos” in big corps where weaknesses are common
- Good threat modeling >> proper test scope

Physical Brute Force

- Pick/break the lock
- Alarm? Mostly off
- Cameras? Could be none/fake one/real one that does not recorded
- Seal all cracks with silicon and blow up safe with gasoline bomb
- Pull out ATM or ram raid with big truck
- Guards? Not really but GTFO quickly



http://www.rac.org.za/forum/viewtopic.php?p=4571

Pwn remote mgt desktop

- Identify job role using remote access
- Look for weak opsec / vulns in OS and remote access / application
- Timing / exploit selection / physical location / network location / SE
- Execute attack – gain access / change files / get PANs / exfiltrate data

Pwn developer and code

- Who are the developers, where is the code repos and what technology and language is in use?

- Look for tech or repo security issue/weak opsec / email use

- Timing/Physical Location/Exploit selection/Third Parties/SE

- Pwn devs/break into repo/steal or modify source code

Pwn central update server

- **Same same, intel comes first**
- **Job roles with access**
- **Technology vulns / weak opsec**
- **Gain access directly or using stolen creds**
- **Pwn server / replace updates**

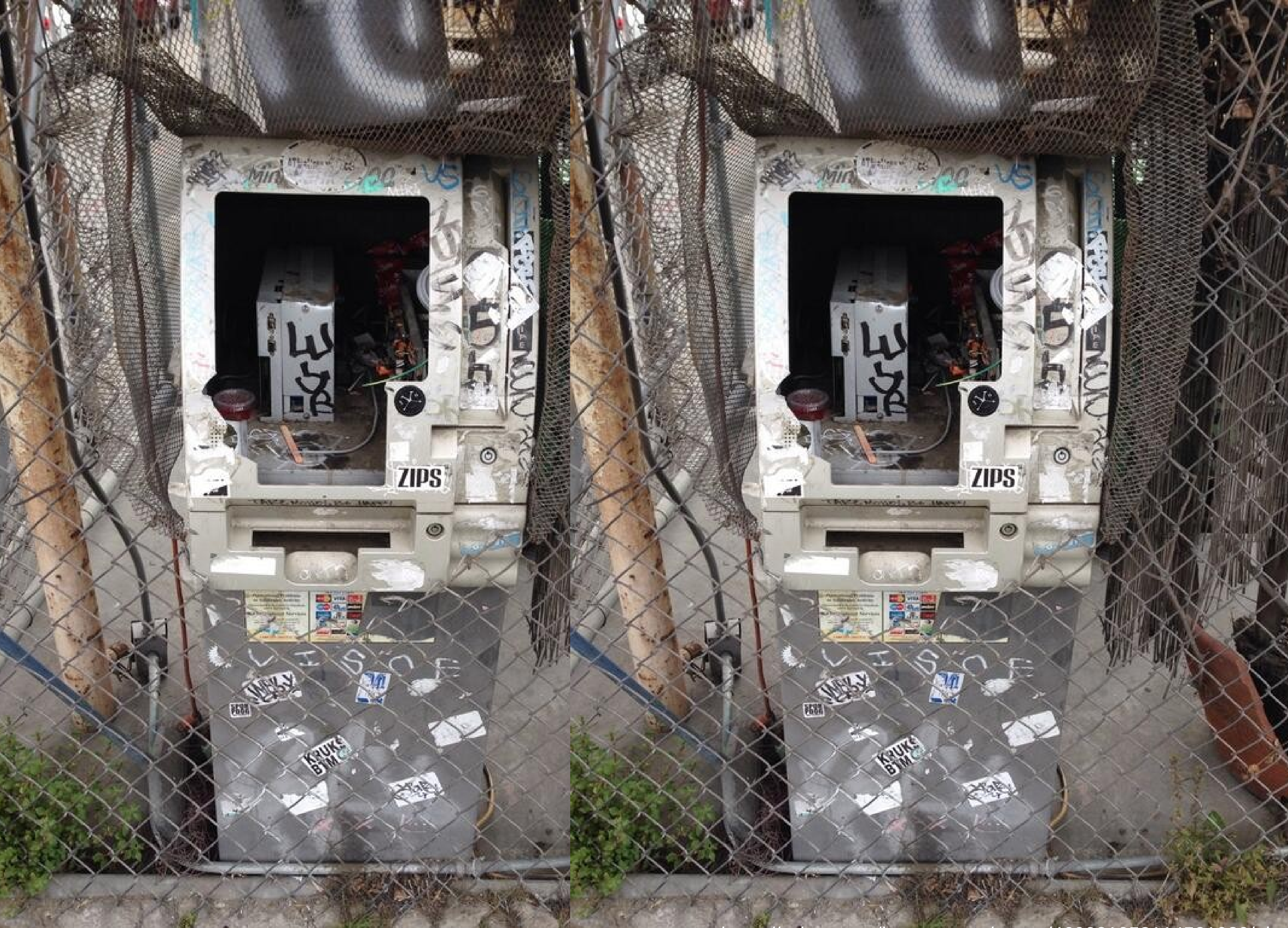
Pwn sysadmins

- **Intel gathering critical as usual**

- **Target meatware / email / creds**

- **Same weak passwords as being used on the ATM / shared pwds**

- **Had nothing to do with ATM hacking? Could be…**



https://twitter.com/haroonmeer/status/469981958114521089/pho
o/1

Our ATM Story – Phase [1]

- First thing first, gloves…
- Now as it's a standalone (not a hole in the wall ATM) we can get to the back part
- We can see & pick the lock easily with basic picks. Lock it after we are done.
- Now we got physical access to the machine

Our ATM Story – Phase [2]

- But wait… What about the Alarm?

- It could be off, but if not it’s usually sending unencrypted packets. So the next step would be to /del/null them or fake them

- What about cameras?

- Could be off, could be empty (just a camera case – due to privacy legislation) and if not? Cover up or wear a mask.

Our ATM Story – Phase [3]

- Now to the logical part

- At first we could dd the hard drive and duplicate it for a later use

- Once we have a duplicated HD we can inject a malware, test it offline and do the switch

- Once we have a malware installed it's game over

- Add dropbox with 3G modem for remote access

Our ATM Story – Phase [4]

- Now to the logical part – 2nd option

- If we don’t want to make the ATM unavailable, even for a short period of time we will have to do things on-the-fly

- First, we will have to bypass the Anti-Malware/AV/etc

- Then we will have to collect information on the OS, Installed software, Patch level and more.

Our ATM Story – Phase [5]

- Logical part – 2nd option (cont.)
- We’ll use a known exploit and/or
- We’ll edit the registry and/or
- We’ll edit some local files and/or
- We’ll boot to a different OS and or…

Our ATM Story – Phase [6]

- Now that we have both physical and logical control we need to:

- Either penetrate deeper into the organization leveraging that the ATM is trusted on the network

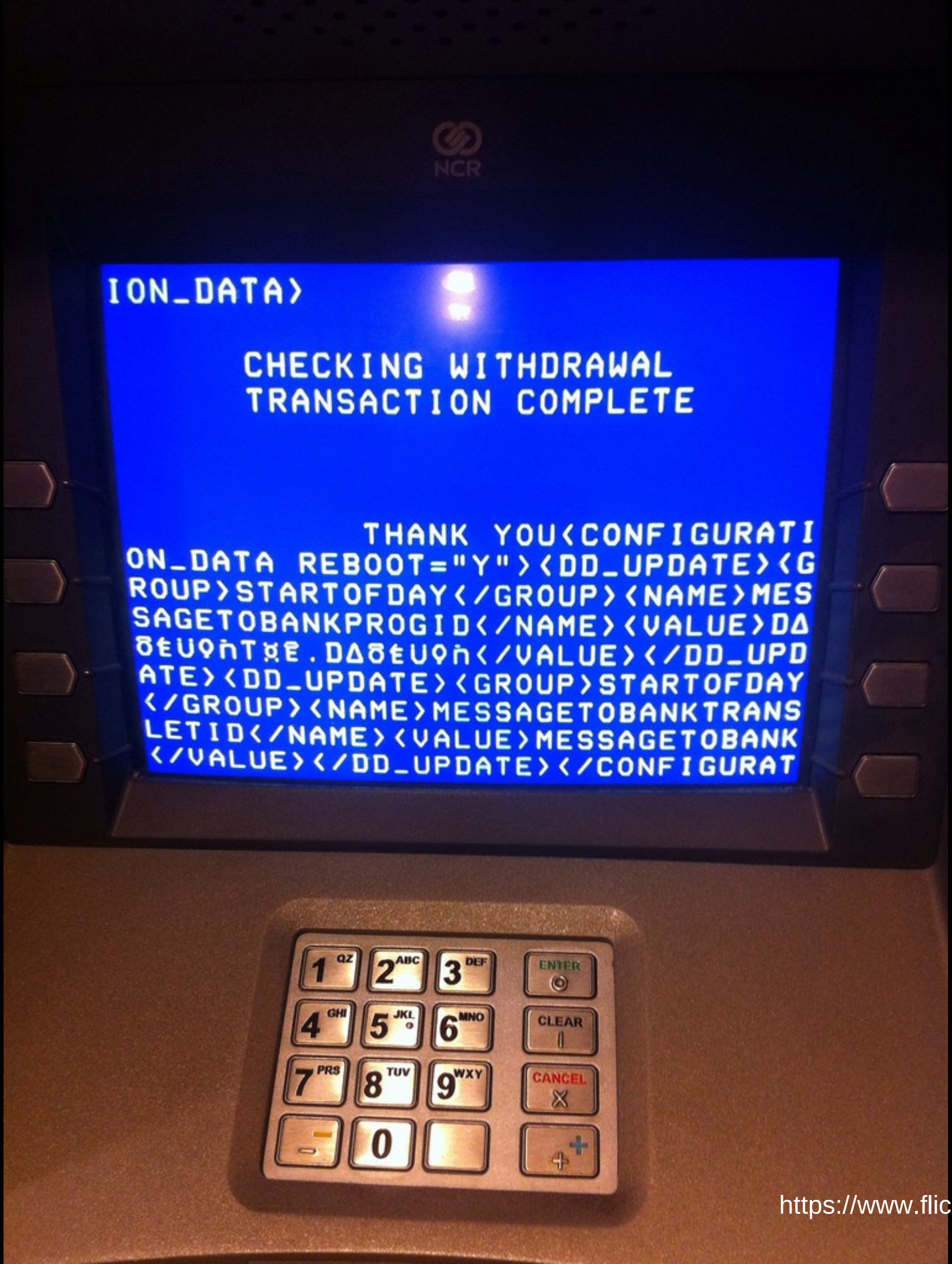
- Keep calm and maintain full control of the ATM

- Leech PANs from files on the ATM

- Command the ATM to dispense cash

How to fix

- Follow basic security principles and put in hard work
- Prevent – restrict access based on business need
- Detect – define attack patterns and monitor
- Respond – define process, implement and assign ownership
- Verify that the above works periodically and fix if broken



```
ION_DATA>

        CHECKING WITHDRAWAL
        TRANSACTION COMPLETE



               THANK YOU<CONFIGURATI
ON_DATA REBOOT="Y"><DD_UPDATE><G
ROUP>STARTOFDAY</GROUP><NAME>MES
SAGETOBANKPROGID</NAME><VALUE>DΔ
ŏ€UϘñT¤ĕ.DΔŏ€UϘñ</VALUE></DD_UPD
ATE><DD_UPDATE><GROUP>STARTOFDAY
</GROUP><NAME>MESSAGETOBANKTRANS
LETID</NAME><VALUE>MESSAGETOBANK
</VALUE></DD_UPDATE></CONFIGURAT
```

https://www.flickr.com/photos/jonkeegan/

Wrap-up

- ATMs are old and complex to manage
- Security by obscurity is eroding
- It’s not just about the money, it’s also about data and control
- Test that ATMs and associated mechanisms and processes are working as intended
- Evaluate and fix broken controls and processes according to business need
- “Silos” are bad in security and an attacker’s wet dream

# E [0] F

Any ?

Yaniv Miron
lament [at] ilhack.org

MC
@fahcu
mc [at] lootcore.com