

A history of ATM violence

From blowing up safes over jackpotting to all-round malware

Erik Van Buggenhout & Daan Raman

OWASP Chapter Meeting - May 2014



Who are we?



Penetration testers



Certification lovers



Instructor
SEC 560 & 542

NVISO ApkScan
Scan Android applications for malware

Drag & drop Android package here

Choose File No file chosen

Binary statistics

File name
MD5 checksum
Binary size

Scan package

By clicking "Scan package" you agree with the [terms and conditions](#) of using this service. Although the uploaded samples will not be made public, the [scan reports](#) are shared with the community.

NVISO ApkScan



Topics for tonight



- Introduction
- Attacking the ATM
- Common ATM system design
- Assessing a sample ATM
- Conclusion



Topics for tonight

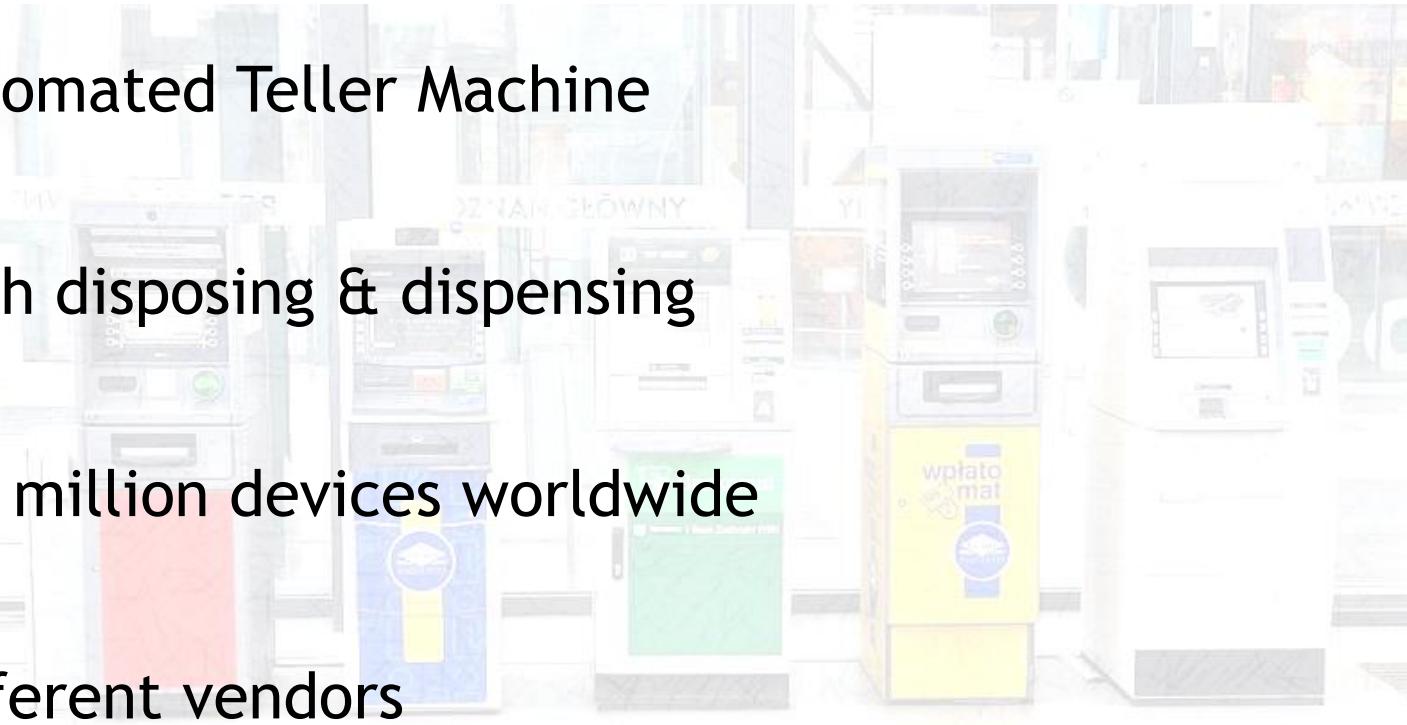


- Introduction
- Attacking the ATM
- Common ATM system design
- Assessing a sample ATM
- Conclusion



ATM?

- Automated Teller Machine
- Cash disposing & dispensing
- 2.2 million devices worldwide
- Different vendors



ATM - Did you know that?



The first ATM was installed in 1939 in New York City, known as “Bankograph”.

Removed after 6 months because it was not used ☺



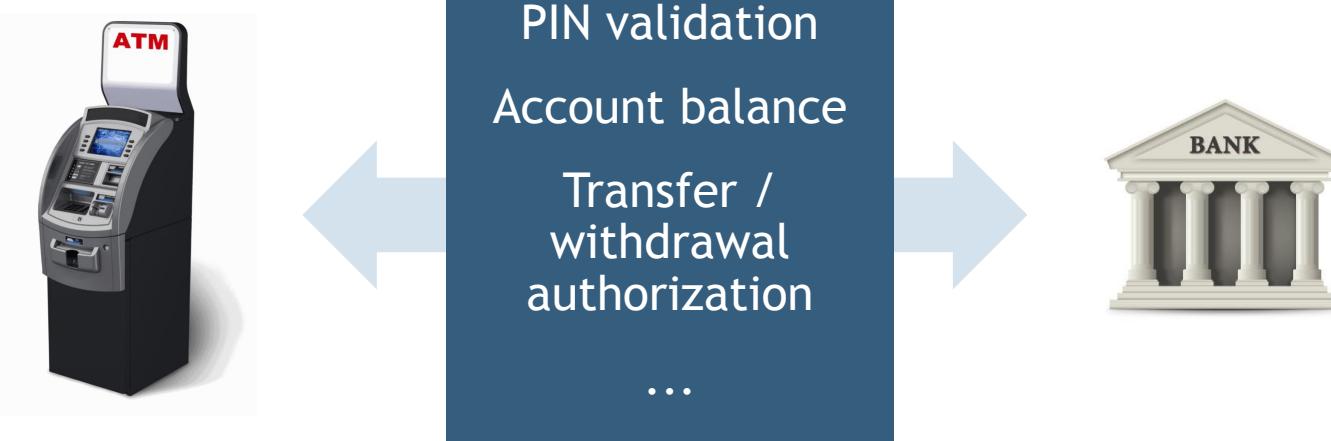
It was reintroduced in Ohio in 1959, with huge success.

There are currently more than 2.2 million ATM's worldwide.



ATM?

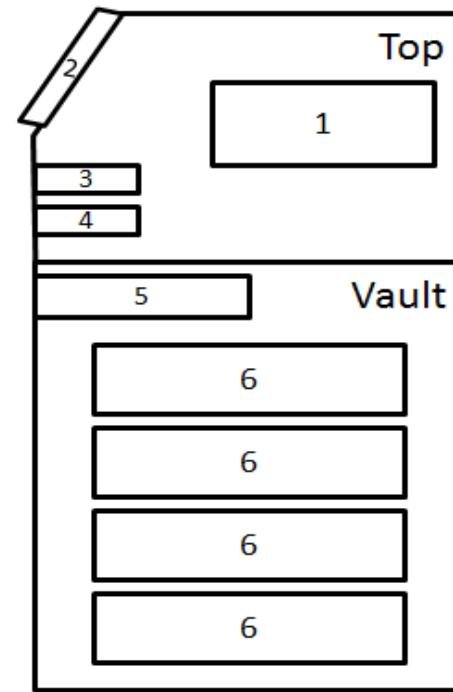
The ATM is a “stupid” device, part of the bank’s overall architecture



ATM?

Typical lay-out of a modern ATM

1. ATM computer
2. (Touch)screen
3. Card-reader
4. PIN pad
5. Cash dispenser
6. Cash cassettes



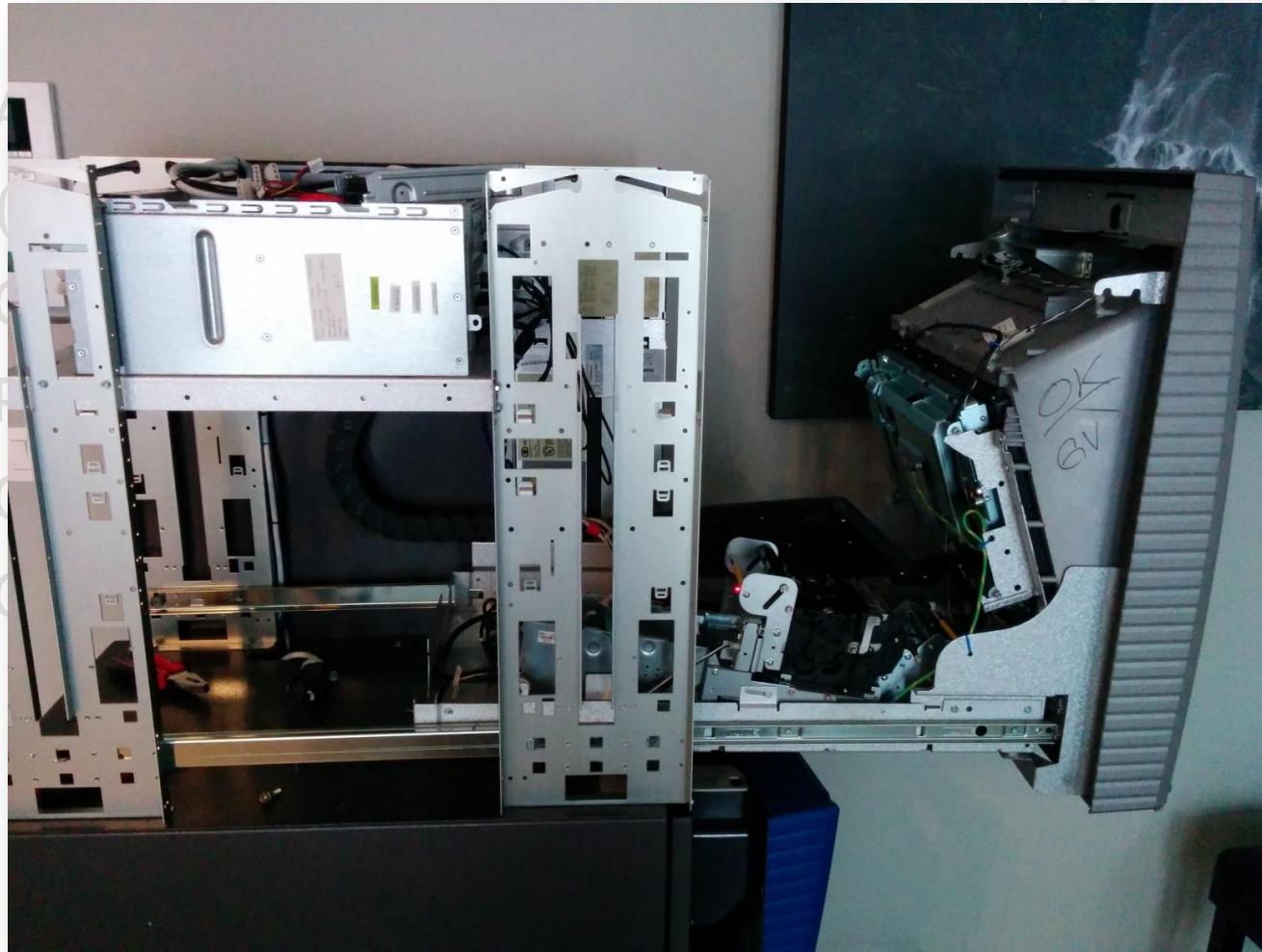
ATM?

1. ATM computer
2. (Touch)screen
3. Card-reader
4. PIN pad
5. Cash dispenser
6. Cash cassette



ATM?

1. A
2. C
3. E
4. R
5. O
6. C



Top

1

Vault



ATM?

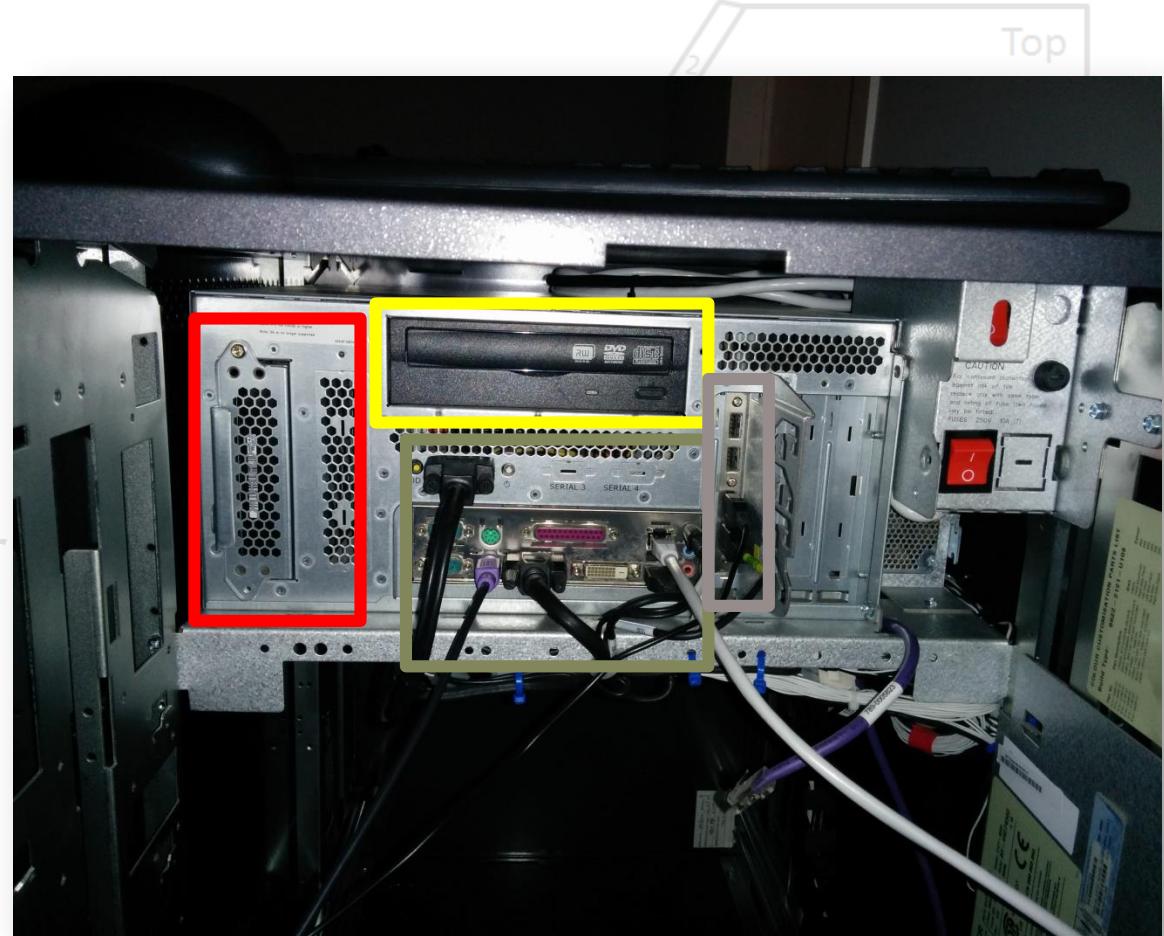
Disk bays

2. (Touch)screen

CD / DVD

Auxiliary ports

USB



Topics for tonight



- Introduction
- Attacking the ATM
- Common ATM system design
- Assessing a sample ATM
- Conclusion



Why attack the ATM?



Why attack the ATM?



It stores **MONEY**

Handles interesting customer data as well,
which could be abused to get **MORE MONEY**



How to attack the ATM?

Blow up the safe

Copy cards &
steal PIN codes

Steal the entire
thing

Attack back-end
communication

Attack the OS

Access
“operator” mode



...



How to attack the ATM?

Blow up the safe

Copy cards &
steal PIN codes

**Steal the entire
thing**



...

Attack back-end
communication

Attack the OS

Access
“operator” mode



How to attack the ATM?

Blow up the safe



ATM

Attack back-end
communication

Attack the OS

Access
“operator” mode



How to attack the ATM?

Blow up the safe



How to attack the ATM?

Blow up the safe



How to attack the ATM?

Blow up the safe

ATM

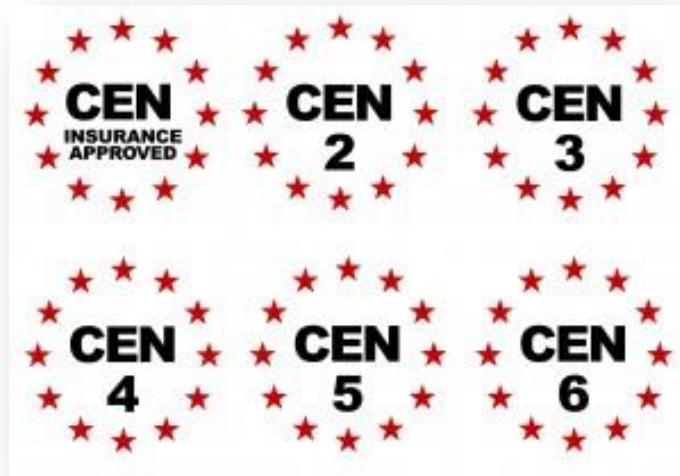
Attack back-end
communication



How to attack the ATM?



How to defend?



Safe certification standards, bolts, video surveillance...



How to defend?



Ink cartridges that stain money upon breach



How to attack the ATM?

Blow up the safe

**Copy cards &
steal PIN codes**

Steal the entire
thing

Attack back-end
communication

Attack the OS

Access
“operator” mode

...



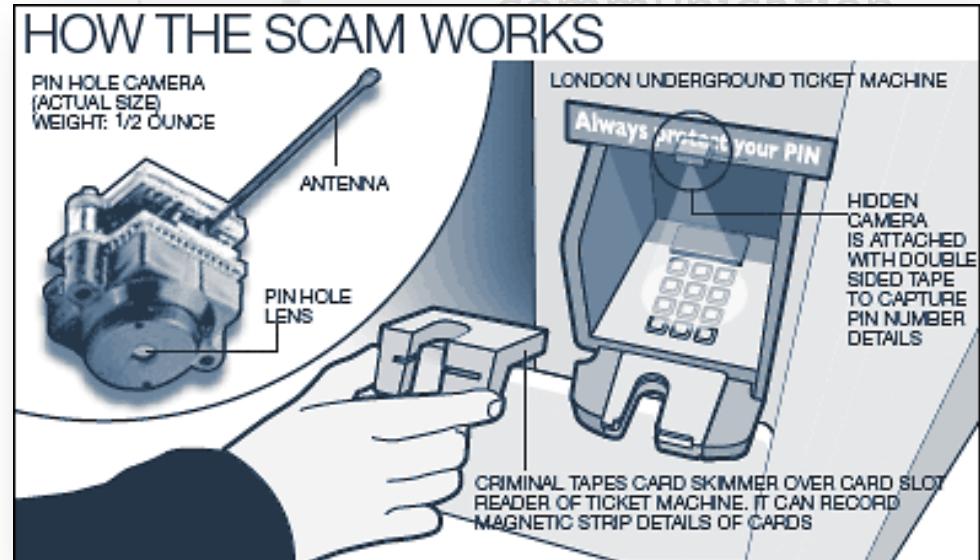
How to attack the ATM?

Blow up the safe

Copy cards &
steal PIN codes

Steal the entire
thing

Attack back-end
communications



...



How to attack the ATM?

Blow up the safe

**Copy cards &
steal PIN codes**

Steal the entire
thing

...



Attack back-end
database.



How to attack the ATM?

Blow up the safe

Copy cards &
steal PIN codes

Steal the entire
thing



...



How to attack the ATM?

Posted: 7:35 p.m. Thursday, Jan. 2, 2014

4 plead guilty to skimming 4,700 ATM cards

**Copy cards &
steal PIN codes**

Credit cards

Skimming off the top

Why America has such a high rate of payment-card fraud

Feb 15th 2014 | ATLANTA | From the print edition



Attack back-end

Police on the Hunt for Suspect Scamming ATMs

Have you seen this person? Police allege the suspect has stolen \$47,000 from area bank machines.

Posted by Penny Arévalo (Editor) , February 19, 2014 at 03:50 PM



More



How to attack the ATM?



How to defend?



Anti-skimming devices



How to defend?



Security awareness campaigns



How to attack the ATM?

Blow up the safe

Copy cards &
steal PIN codes

Steal the entire
thing

Attack back-end
communication

Attack the OS

**Access
“operator” mode**

...



How to attack the ATM?

Googling for ATM Master Passwords

By Ryan Naraine | Posted 2006-09-21 | [Email](#) | [Print](#)



Using clues obtained from a YouTube video and a simple four-word search engine query, a criminal can find step-by-step instructions on how to hack into and take control of thousands of cash-dispensing ATMs.

Steal the entire
thing



...

Access
“operator” mode



How to attack the ATM?

Googling for ATM Master Passwords

By Ryan Naraine | Posted 2006-09-21 | [Email](#) | [Print](#)



Using clues obtained from a YouTube video and a simple four-word search engine query, a criminal can find step-by-step instructions on how to hack into and take control of thousands of cash-dispensing ATMs.

Two Arrested For Reprogramming ATMs To Provide Extra Cash

from the *this-is-still-doable?* dept

Almost exactly two years ago, a story made the rounds of how easy it was to [reprogram ATMs](#) to believe it had a different denomination. Thus, if it actually had \$20 bills, you could convince it that it really had \$1 or \$5 bills. Then when you took out money from the machine, you would get the \$20 bills, making a tidy profit. The reason this hack was so easy was that many ATM owners simply left the default passwords on the machines -- and those passwords were easily found online. Last year, we noted that, despite the publicity around this easy hack, many ATM owners [still had not](#) changed the default password. Apparently, that's still the case, as [two men have been arrested for using the hack to steal thousands of dollars](#). Still, it's worth noting that the only reason they seem to have been caught was they hit the same store multiple times (and, apparently, the owner of that store *still* hadn't changed the default password).

Access
“operator” mode



How to defend?

Changing Default Passwords

With the release of newer software, you may experience a new error code. Error Code **(246)** has been created for when the terminal's **Master** and/or **Administration** password(s) are in the default state. The terminal will detect this condition and go out of service. On the "Out of Service" screen, no error information will be displayed. The following are screen captures of this state. This error code will not clear until the Master and/or the Administration passwords are changed from their default state.

The default MASTER password is '123456' and the default ADMINISTRATION password is '987654'.

Awareness + force change of default passwords



How to attack the ATM?

Blow up the safe

Copy cards &
steal PIN codes

Steal the entire
thing

Attack back-end
communication

Attack the OS

Access
“operator” mode

...



How to attack the ATM?



Adam Greenberg, Reporter

October 28, 2013

ATM malware Ploutus updated with English-language version

Copy cards & steal PIN codes

Attack the OS

Texting ATMs for Cash Shows Cybercriminals' Increasing Sophistication

Created: 24 Mar 2014 12:57:46 GMT • Updated: 24 Mar 2014 17:45:39 GMT • Translations available: [日本語](#), [Español](#)

Steal the entire

Access

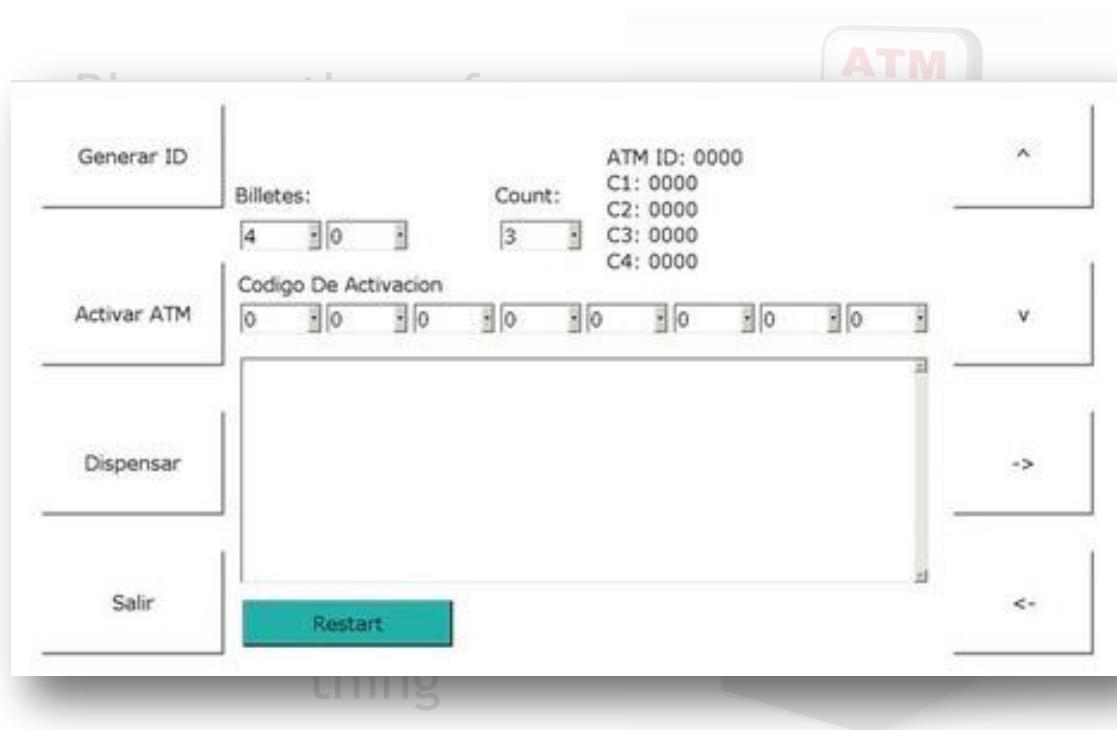
"operator" mode

Cash machines raided with infected USB sticks

By Chris Vallance
BBC Radio 4



How to attack the ATM?



Attack back-end
communication

Attack the OS

Access
“operator” mode

...



How to attack the ATM?



Barnaby Jack
“Jackpotting ATMs” - 2010

Attack the OS



How to attack the ATM?

Network access?

www.shodanhq.com/search?q=NCR+Self-Service

Shodan Exploits Scanhub Research Anniversary Promotion Register Login

SHODAN NCR Self-Service Search

Results 1 - 10 of about 613 for NCR Self-Service

IP Address	Location	Hardware	Software
119.154.147.211	Pakistan, Islamabad	NCR Self-Service Terminal Hardware: x86 Family 15 Model 2 Stepping 9 AT/AT COMPATIBLE	Software: Windows 2000 Version 5.1 (Build 2600 Uniprocessor Free)
37.195.119.5	Ukraine, Kyiv	NCR Self-Service Terminal Hardware: x86 Family 6 Model 22 Stepping 1 AT/AT COMPATIBLE	Software: Windows 2000 Version 5.1 (Build 2600 Uniprocessor Free)
217.8.33.214	Ukraine, Kyiv	NCR Self-Service Terminal Hardware: x86 Family 6 Model 22 Stepping 1 AT/AT COMPATIBLE	Software: Windows 2000 Version 5.1 (Build 2600 Uniprocessor Free)
91.190.85.138	Russia, Start	NCR Self-Service Terminal Hardware: x86 Family 6 Model 8 Stepping 10 AT/AT COMPATIBLE	Software: Windows 2000 Version 5.1 (Build 2600 Uniprocessor Free)
95.140.194.173	Armenia, Yerevan	NCR Self-Service Terminal Hardware: x86 Family 6 Model 23 Stepping 10 AT/AT COMPATIBLE	Software: Windows 2000 Version 5.1 (Build 2600 Multiprocessor Free)

HackerTarget.com
Everyone is a target
BUILT ON OPEN SOURCE NO BS
SCAN YOUR STUFF NOW

scan your website with netsparker

Hurricane LABS

How to attack the ATM?

Network access?

The screenshot shows a Shodan search results page for "NCR Self-Service". The search bar at the top contains the text "DOWNTONABY THEYELLOWSUB". The results list several IP addresses and their details:

- 119.154.147.211 PTCL Added on 23.01.2014 Islamabad
- 37.195.119.5 Novotelcom Ltd Added on 23.01.2014
- I37-195-119-5.novotelcom.ru
- 217.8.33.214 Somoncom IP Networks Added on 23.01.2014
- 91.190.85.138

The right side of the page features a sidebar with advertisements for "HackerTarget.com" and "netsparker".

Shodan HQ (Internet search engine) lists 800+ ATMs on the Internet



How to attack the ATM?



CCC 2013
“Electronic bank robberies”
Boot ATMs from USB

Attack back-end
communication

Attack the OS

Access
“operator” mode



Topics for tonight



- Introduction
- Attacking the ATM
- Common ATM system design
- Assessing a sample ATM
- Conclusion



ATM system design



CEN/XFS (eXtensions for Financial Services) provides a standard set of APIs that can be used by Windows applications to operate the ATM peripherals

CEN/XFS Device Classes

The following device classes are defined by the CEN/XFS specification:

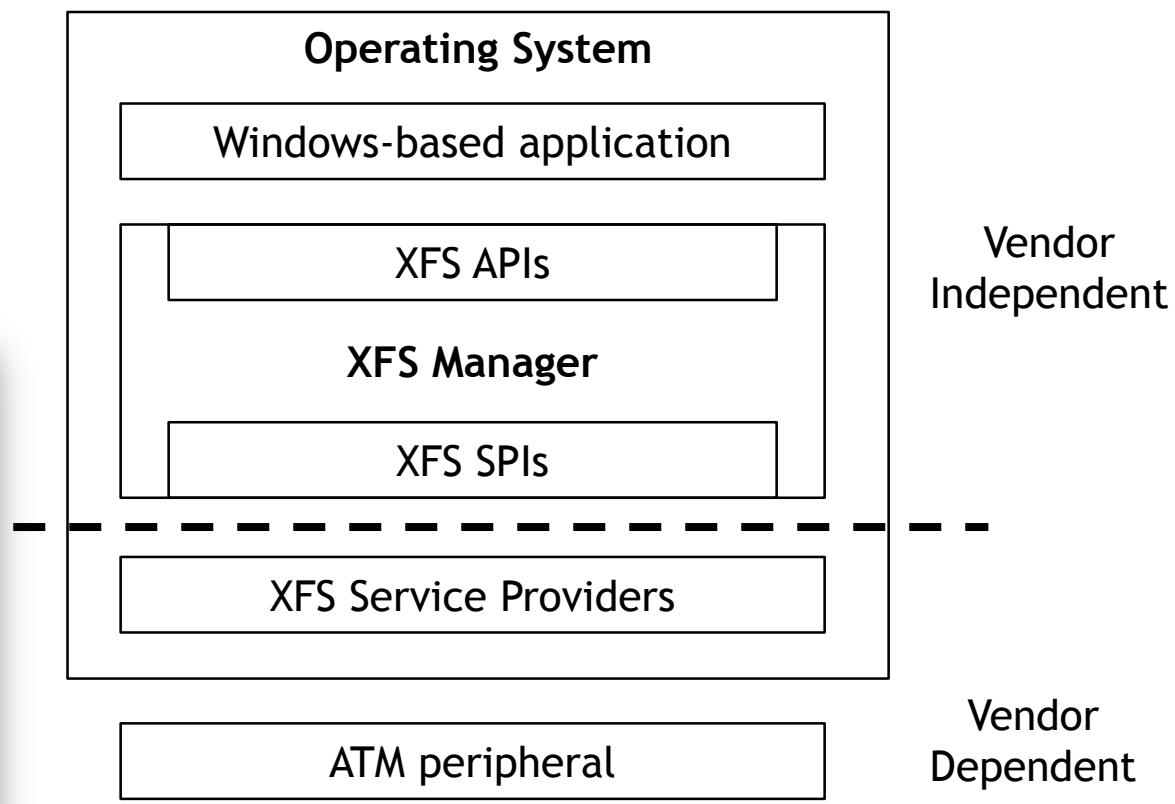
- Printers and Scanners (Ptr)
- Identification Card Units (Idc)
- Cash Dispensers (Cdm)
- Personal Identification Number Keypads (Pin)
- Check Readers and Scanners (Chk)
- Depository Units (Dep)
- Text Terminal Units (Ttu)
- Sensors and Indicators Units (Siu)
- Vendor Dependent Mode (Vdm)
- Cameras (Cam)
- Alarms (Alm)
- Card Embossing Units (Ceu)
- Cash-In Modules (Cim)
- Card Dispensers (Crd)
- Barcode Readers (Bcr)
- Item Processing Modules (Ipmp)



ATM system design



CEN/XFS (eXtensions for Financial Services) provides a standard set of APIs that can be used by Windows applications to operate the ATM peripherals



ATM system design

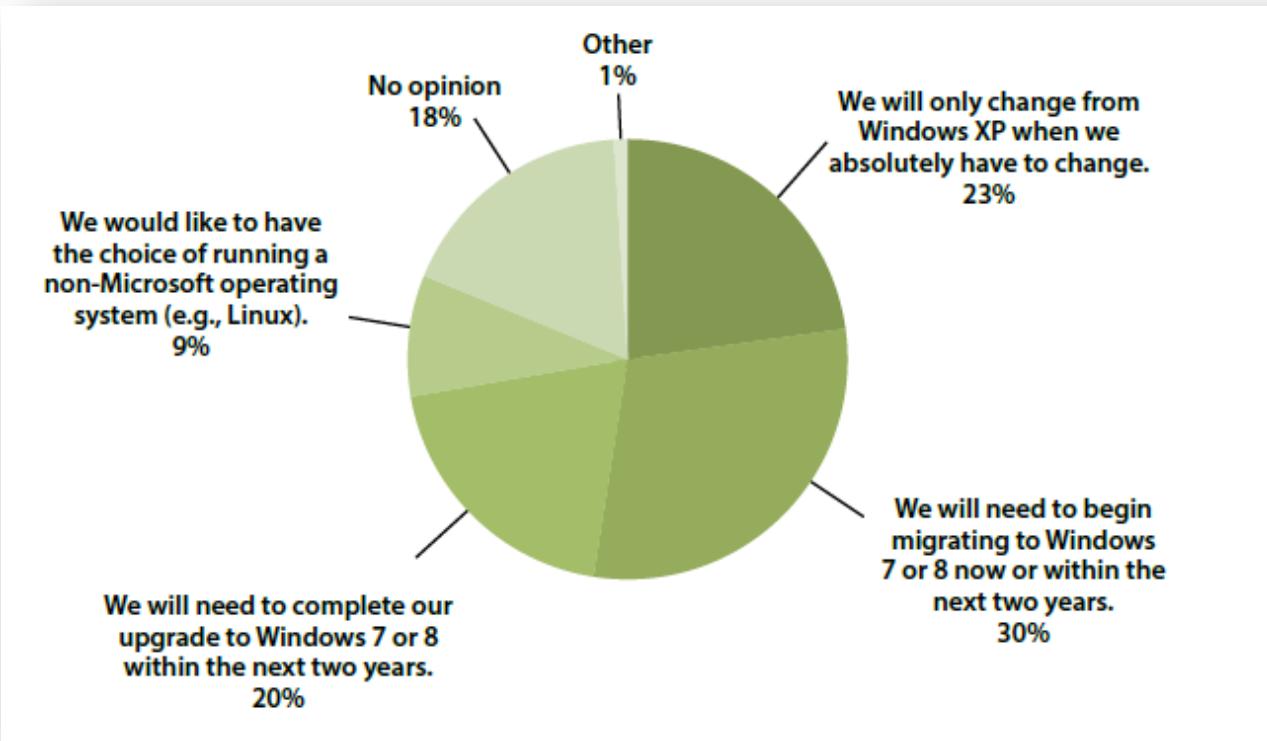
95% of ATMs was running Windows XP in January 2014
(NCR, 2014)



ATM system design

“How will you approach the Windows XP end-of-support?”

(KAL 2013 - ATM Software Trends & Analysis)



Topics for tonight



- Introduction
- Attacking the ATM
- Common ATM system design
- Assessing a sample ATM
- Conclusion



Where to start?



Big Time Deals!
Big Time Savings!

FEBRUARY PACKAGE
G2505

[View more details](#)

**ALWAYS
THE
MONEY**

I  LASH

BUY NOW >

This promotional banner features a football stadium background with two young men in the foreground. One man holds a sign that reads "ALWAYS THE MONEY" and the other holds a large "I  LASH" sign. The text "Big Time Deals!" and "Big Time Savings!" is displayed prominently at the top left. A "FEBRUARY PACKAGE G2505" offer is highlighted in the center. A "View more details" link is located below the package offer. A "BUY NOW >" button is at the bottom right.



GENMEGA ATMs



Buy now

HANTLE ATMs



Buy now

Triton ATMs



Buy now

Nautilus ATMs



HYOSUNG

Buy now

This vertical column displays four different ATM brands: GENMEGA, HANTLE, Triton, and Nautilus. Each brand has a small image of its respective ATM model and a green "Buy now" button.



Where to start?

 Cennox

Home NCR Parts ▾ Wincor Parts ▾ Diebold Parts ▾ Contact Us ** SPECIAL OFFERS ** ▾

Pick a currency GBP ▾

Home > NCR Parts > >>NCR-Complete-Machines > Page 1 of 1

NCR Parts

Browse: All items ▾









NCR 5886 BNA Machine
NCR
£1,153.90

ATM delivery 101



ATM delivery 101



Let's get started



Physical access?



Physical access?



Physical access?



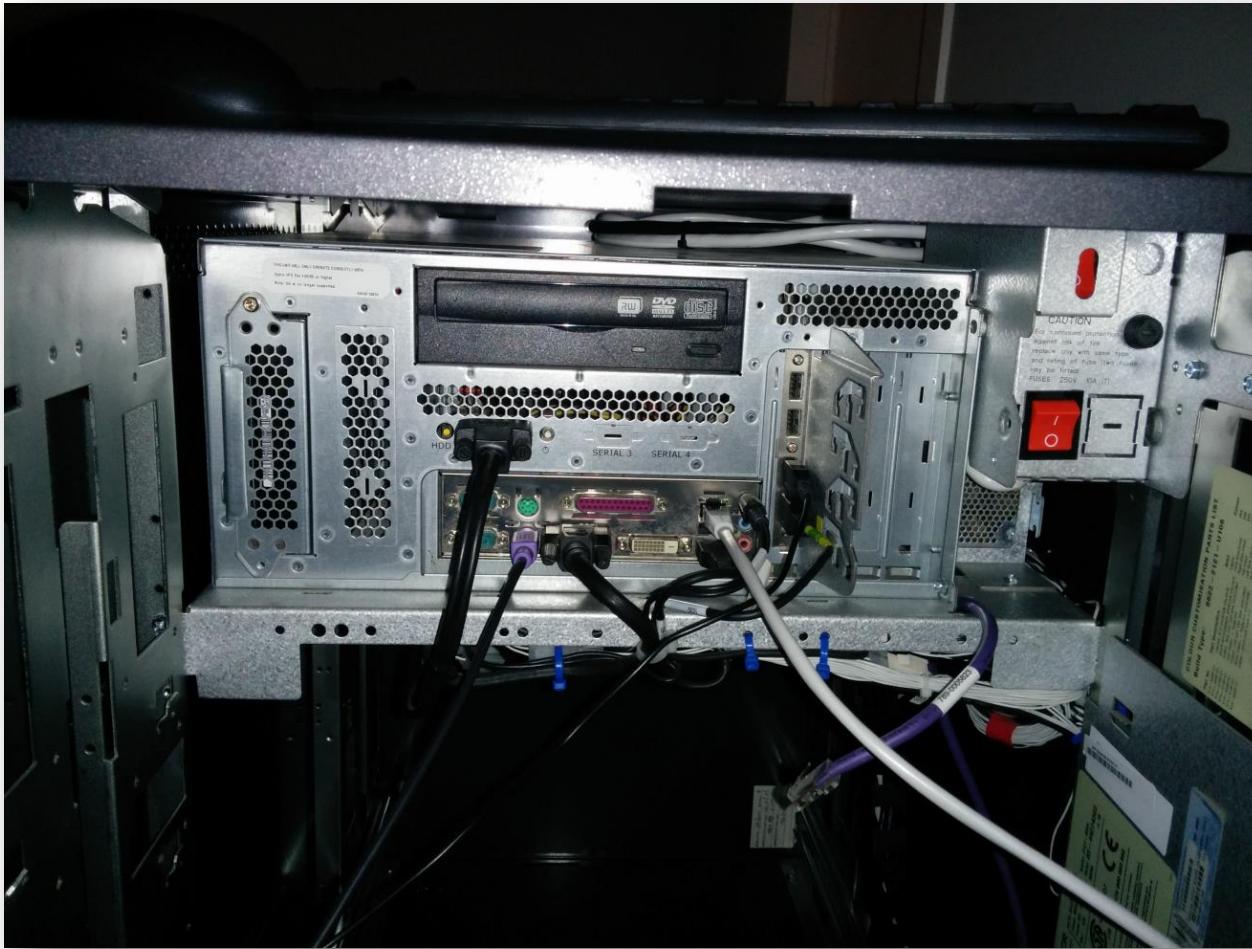
Physical access?



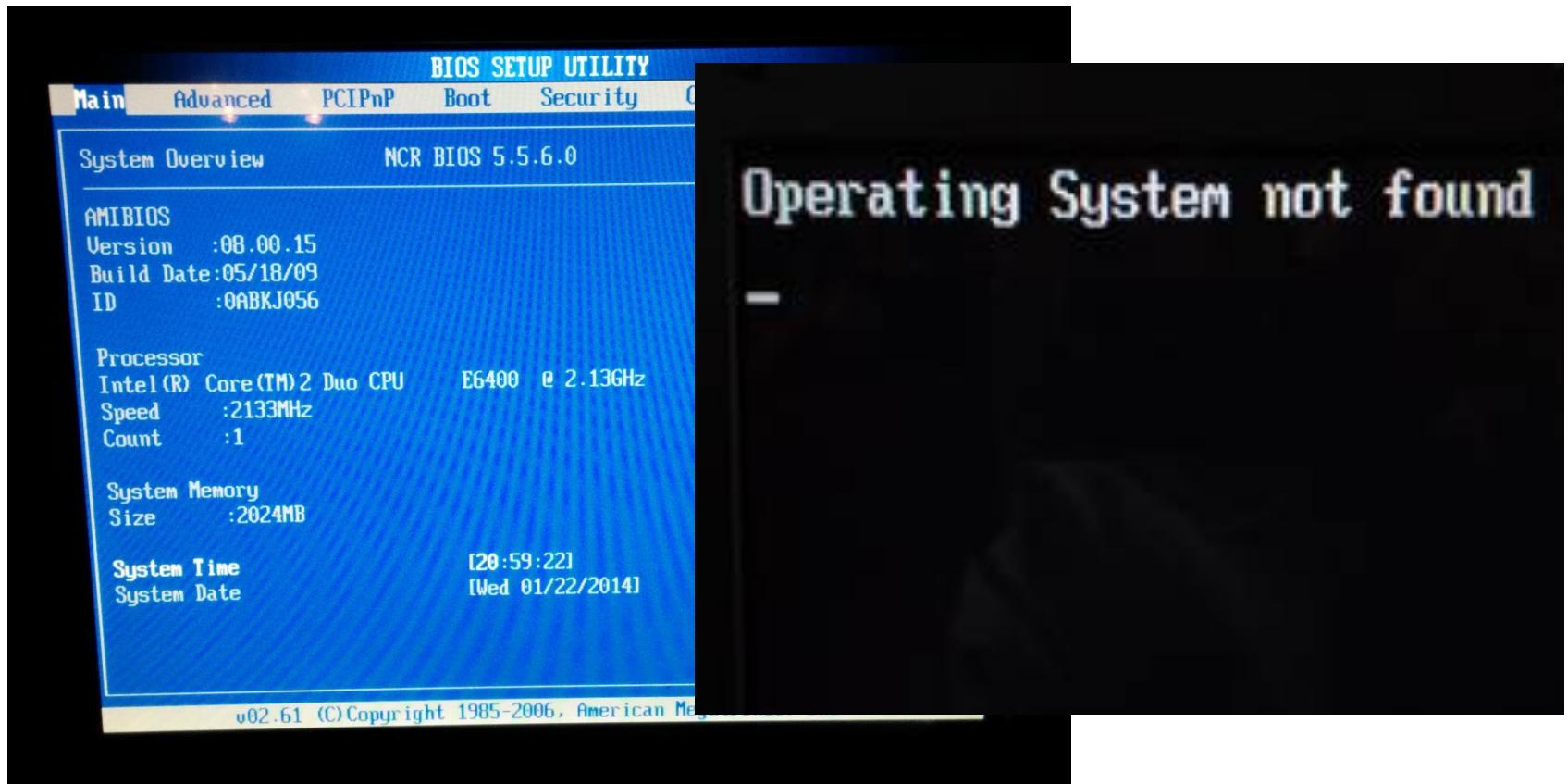
Physical access?



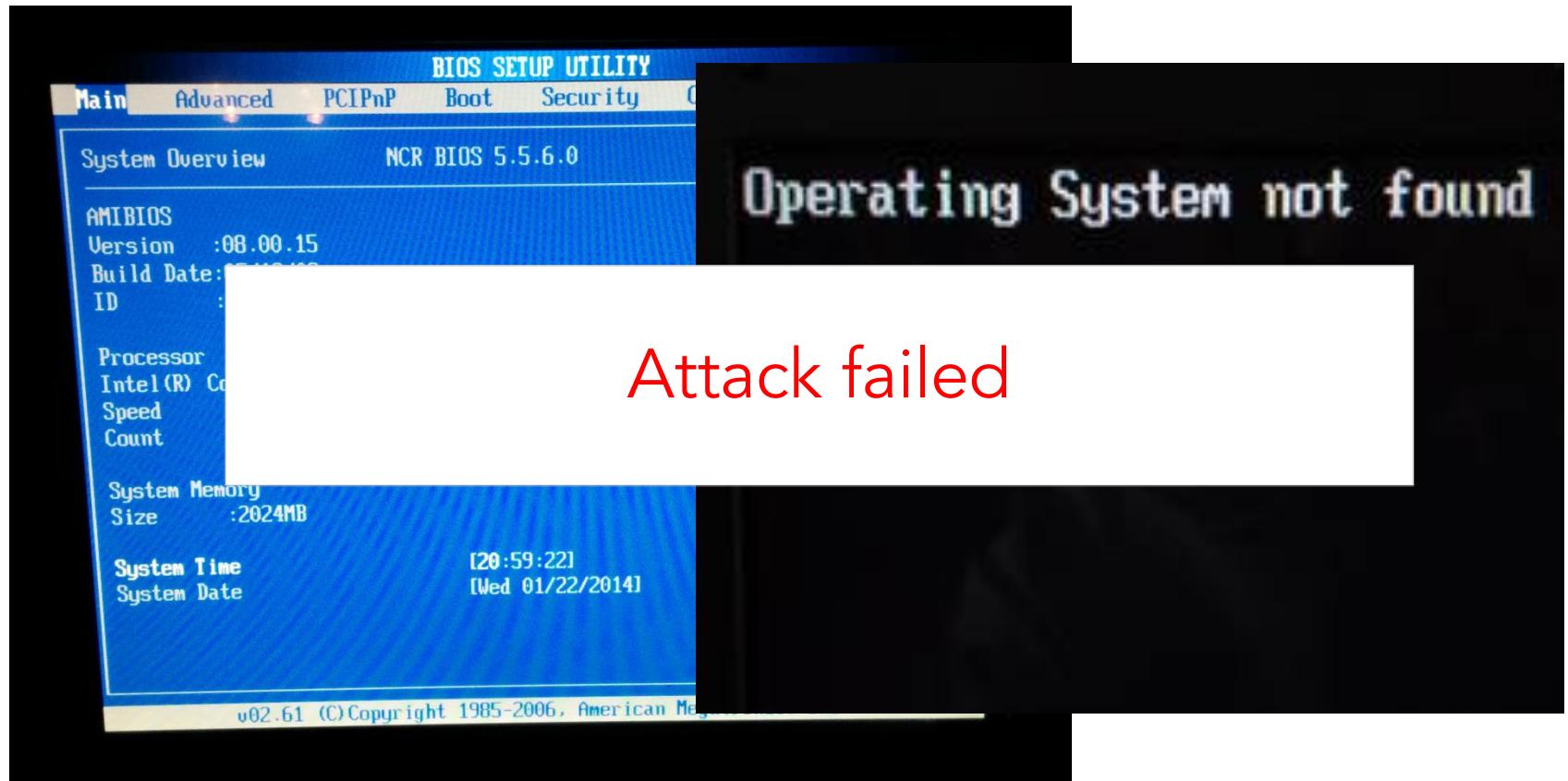
Physical access?



Running the ATM



Running the ATM



ATM Forensics 101

Using openly available forensic toolkits we managed to recover the majority of the original hard disk content.



Active@ Partition Recovery for Windows Enterprise

File View Tools Help

Back QuickScan SuperScan Recover

Local System Devices

WinOS (5) [Bad]

- \$Extend
- Config.Msi
- Documents and Settings
- FTAgent
- NCRLogs
- PNPDRVRVS
- program files
 - Application Startup
 - ATMAD
 - Common Files
 - ComPlus Applications
 - CrossTec
 - Inside Out Networks Watchport
 - InstallShield Installation Information
 - Intel
 - Internet Explorer
 - Messenger
 - microsoft frontpage
 - MicroTouch
 - Movie Maker
 - MSN
 - MSN Gaming Zone
 - MSXML 4.0
 - NCR
 - ncr aptra
 - NetMeeting
 - Nuance
 - Online Services
 - Outlook Express
 - PenMount Windows Unive...
 - Realtek

SuperScan [100%]

Name	Size	Created	Modified	Accessed/Deleted	Attributes	ID	Parent ID
Application Startup		2014-01-10 12:20:26	2014-01-10 12:20:26	2014-01-10 12:32:01		1016	35
ATMAD		2014-01-10 11:53:06	2014-01-10 11:53:06	2014-01-13 01:20:45		3792	35
Common Files		2012-03-12 15:51:43	2014-01-10 11:39:08	2014-01-13 01:59:04		522	35
ComPlus Applications		2012-03-12 15:58:28	2012-03-12 15:58:28	2014-01-10 12:25:31		596	35
CrossTec		2014-01-10 11:52:37	2014-01-10 11:53:03	2014-01-10 12:18:47		489	35
Inside Out Networks Watchport		2012-03-12 16:09:43	2012-03-12 16:09:43	2014-01-10 12:18:47		597	35
InstallShield Installation Information		2012-03-12 16:08:48	2012-03-12 16:11:15	2014-01-10 12:18:47	H	599	35
Intel		2012-03-12 16:08:52	2012-03-12 16:08:52	2014-01-10 12:25:32		603	35
Internet Explorer		2012-03-12 15:59:02	2012-03-12 16:24:15	2014-01-10 12:18:47		605	35
Messenger		2012-03-12 15:58:07	2012-03-12 15:58:07	2014-01-10 12:18:47		611	35
microsoft frontpage		2012-03-12 16:16:36	2012-03-12 16:16:36	2014-01-10 12:25:33		612	35
MicroTouch		2012-03-12 16:13:18	2012-03-12 16:13:18	2014-01-10 12:18:48		615	35
Movie Maker		2012-03-12 15:59:10	2012-03-12 15:59:10	2014-01-10 12:18:48		629	35
MSN		2012-03-12 15:57:58	2012-03-12 15:57:58	2014-01-10 12:25:33		634	35
MSN Gaming Zone		2012-03-12 15:58:05	2012-03-12 15:58:05	2014-01-10 12:18:48		639	35
MSXML 4.0		2014-01-10 12:13:40	2014-01-10 12:13:40	2014-01-10 12:25:34		27400	35
NCR		2014-01-10 11:57:06	2014-01-10 11:57:06	2014-01-10 12:18:52		25230	35
ncr aptra		2012-03-12 16:07:40	2014-01-10 12:27:08	2014-01-13 01:59:04		36	35
NetMeeting		2012-03-12 15:59:05	2012-03-12 15:59:15	2014-01-10 12:18:48		824	35
Nuance		2014-01-10 12:08:23	2014-01-10 12:08:23	2014-01-10 12:26:09		25580	35
Online Services		2012-03-12 15:58:15	2012-03-12 15:58:15	2014-01-10 12:18:48		825	35
Outlook Express		2012-03-12 15:59:03	2012-03-12 15:59:14	2014-01-10 12:18:48		826	35
PenMount Windows Universe		2012-03-12 16:12:53	2012-03-12 16:12:53	2014-01-10 12:18:48		827	35
Realtek		2012-03-12 16:11:15	2012-03-12 16:11:15	2014-01-10 12:18:49		831	35

Date/Time Event

2014-01-24 22:07:43 Volume projected [NO NAME] (FAT, 109 MB, Integrity Status: Bad, Start sector: 21,550,308 Sectors: 223,684)
2014-01-24 23:23:50 Volume projected [WinOS] (NTFS, 149 GB, Integrity Status: Bad, Start sector: 2,048 Sectors: 312,497,951)
2014-01-24 23:23:50 Volume projected [WinOS] (NTFS, 146 GB, Integrity Status: Bad, Start sector: 6,293,488 Sectors: 306,206,511)
2014-01-24 23:23:50 Device SuperScan completed
2014-01-24 23:23:51 SuperScan results successfully saved to: Z:\NVISO\Recovery\WDC WD16 02ABKS-18N8A0 USB Device SuperScan [2014-01-24 22-02-05].scn

33 object(s)

Folder: 5:\program files\NCR. Contains: 1 subfolder(s), 0 file(s)

ATM Forensics 101



Sweet... But I don't have a bank back-end (yet)



Software engineering 101



EUROPEAN COMMITTEE FOR STANDARDIZATION
COMITÉ EUROPÉEN DE NORMALISATION
EUROPÄISCHES KOMITEE FÜR NORMUNG

WORKSHOP AGREEMENT

CWA 14050-1

November 2000

ICS 35.200; 35.240.15; 35.240.40

Extensions for Financial Services (XFS) interface specification -
Release 3.0 - Part 1: Application Programming Interface (API) - Service
Provider Interface (SPI); Programmer's Reference



Software engineering 101



EUROPEAN COMMITTEE FOR STANDARDIZATION
COMITE EUROPEEN DE NORMALISATION
EUROPÄISCHES KOMITEE FÜR NORMUNG

**WORKSHOP
AGREEMENT**

CWA 14050-5

November 2000

ICS 35.200; 35.240.40

Extensions for Financial Services (XFS) interface specification -
Release 3.0 - Part 5: Cash Dispenser Device Class Interface



Software engineering 101

```
C:\WINDOWS\system32\cmd.exe
C:\Documents and Settings\User\Desktop>ATMDispenser.exe
ATM Dispenser v0.1 by Erik Van Buggenhout
-----
This PoC executable will use the XFS standard to perform an ATM cash-out in EUR.

Usage: <TOTALAMOUNT> <CASSETTE1-NOTES> <CASSETTE2-NOTES>
Totalamount:           Total amount to be dispensed (e.g. 150)
Cassette1-Notes:       Number of notes from cassette 1 (loaded with 10 EUR)
Cassette2-Notes:       Number of notes from cassette 2 (loaded with 50 EUR)

Dispense will only succeed if the denomination is correct (e.g. 150 EUR = 5*10 EUR and 2*50 EUR).

C:\Documents and Settings\User\Desktop>
```



Software engineering 101

DEMONSTRATION



Topics for tonight



- Introduction
- Attacking the ATM
- Common ATM system design
- Developing ATM “malware”
- Conclusion



Conclusion

Modern ATMs are **standard, Windows-based**, computers full of money

Developing ATM “malware” is a piece of cake



Highly interesting target, protection is required!

Patch management (No WIN XP)

Application whitelisting

Network segmentation

Disk encryption

Protect the BIOS

