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

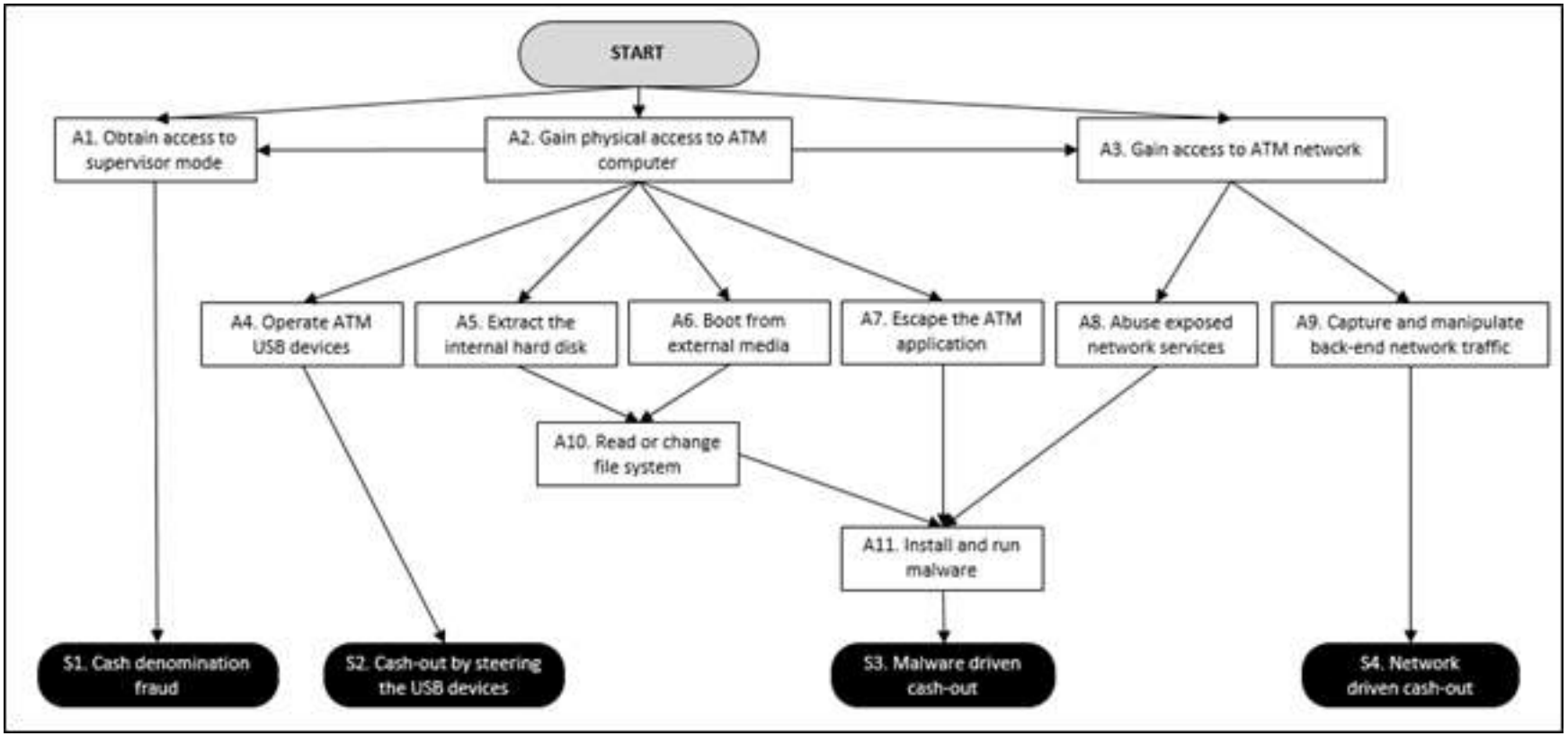
Topics for today

- 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 then 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.

PIN validation

Account balance

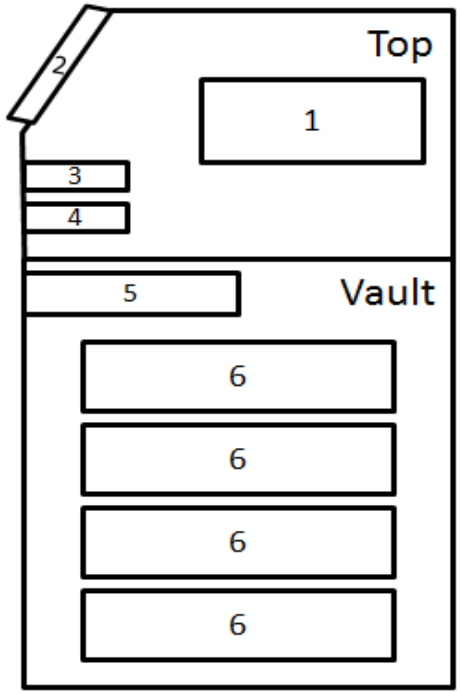
Transfer / withdrawal authorization

...

ATM?

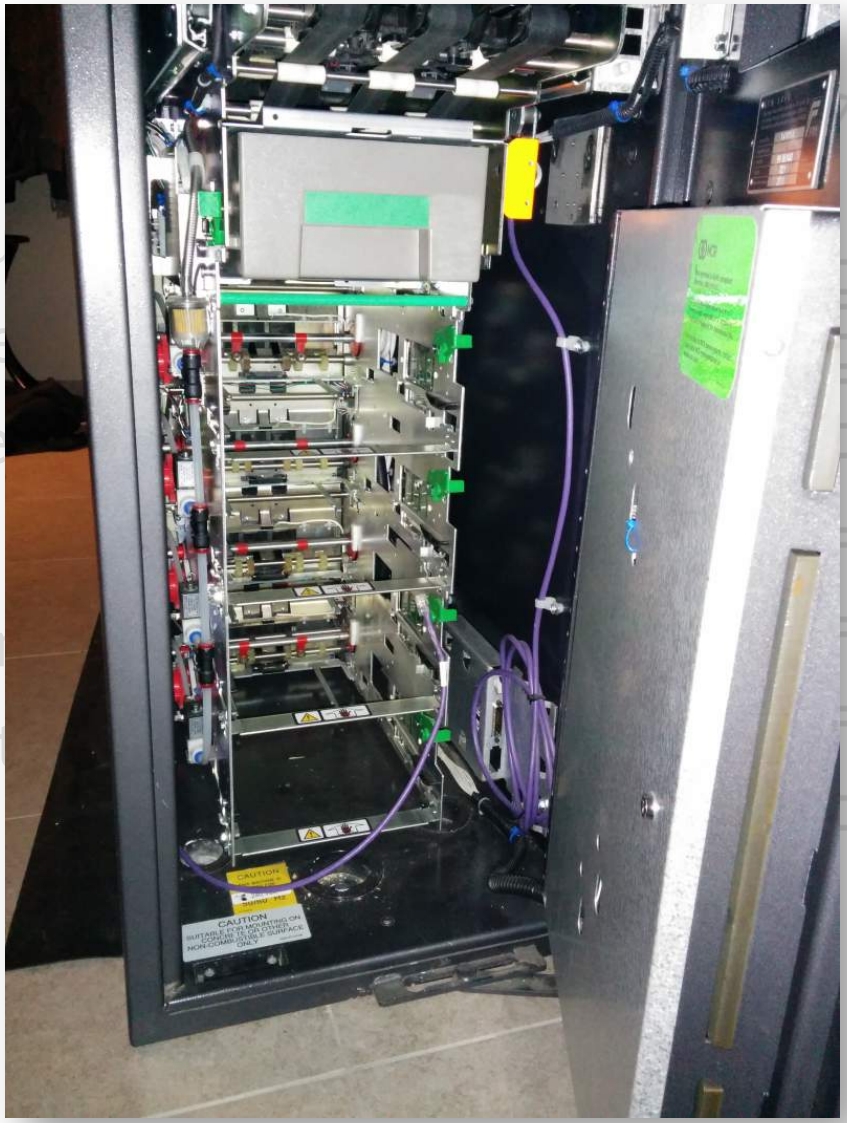
Typical lay-out of a modern ATM

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

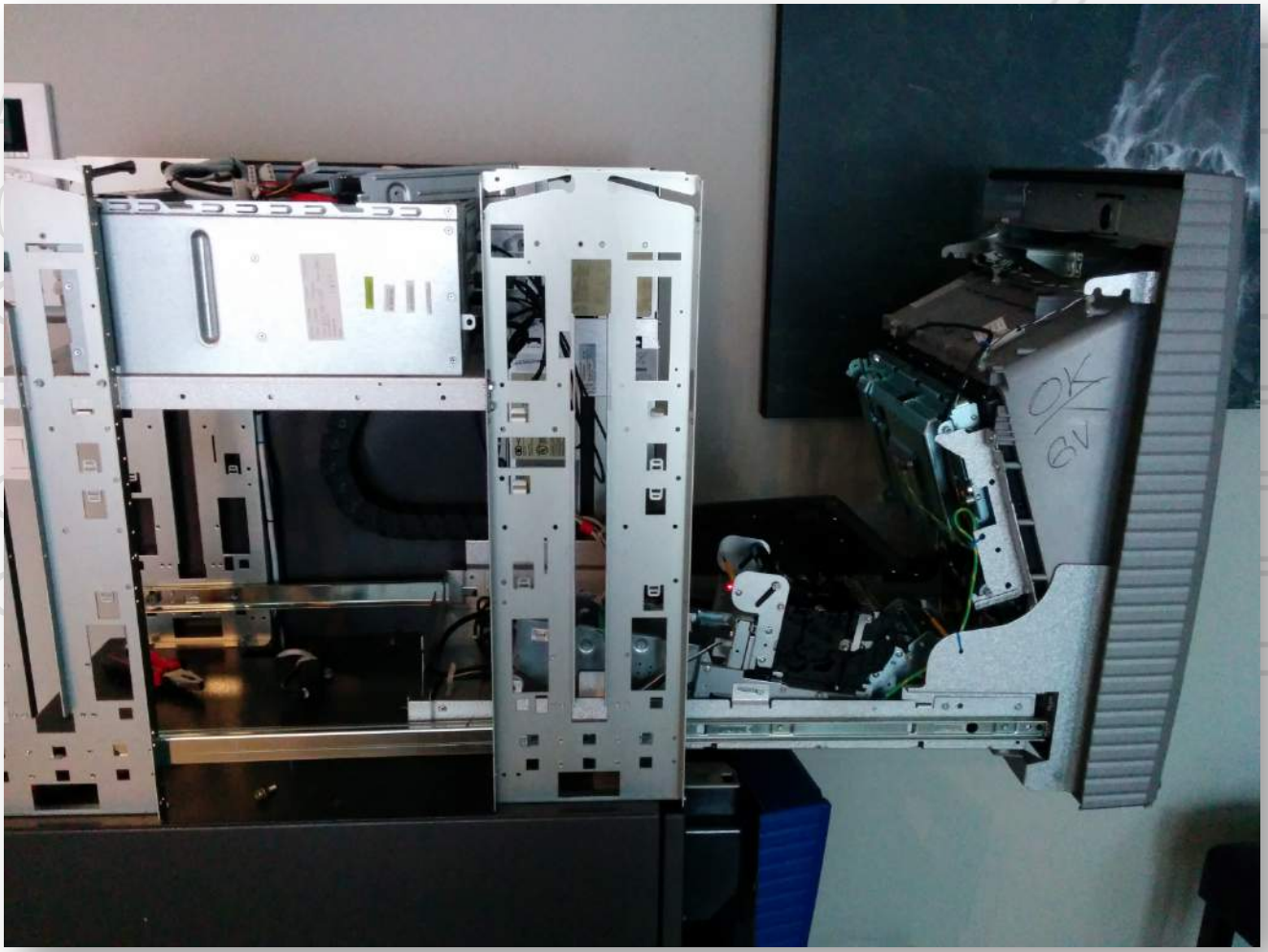


ATM?

1. ATM compu
2. (Touch)scre
3. Card-reade
4. PIN pad
5. Cash disper
6. Cash casset



ATM?



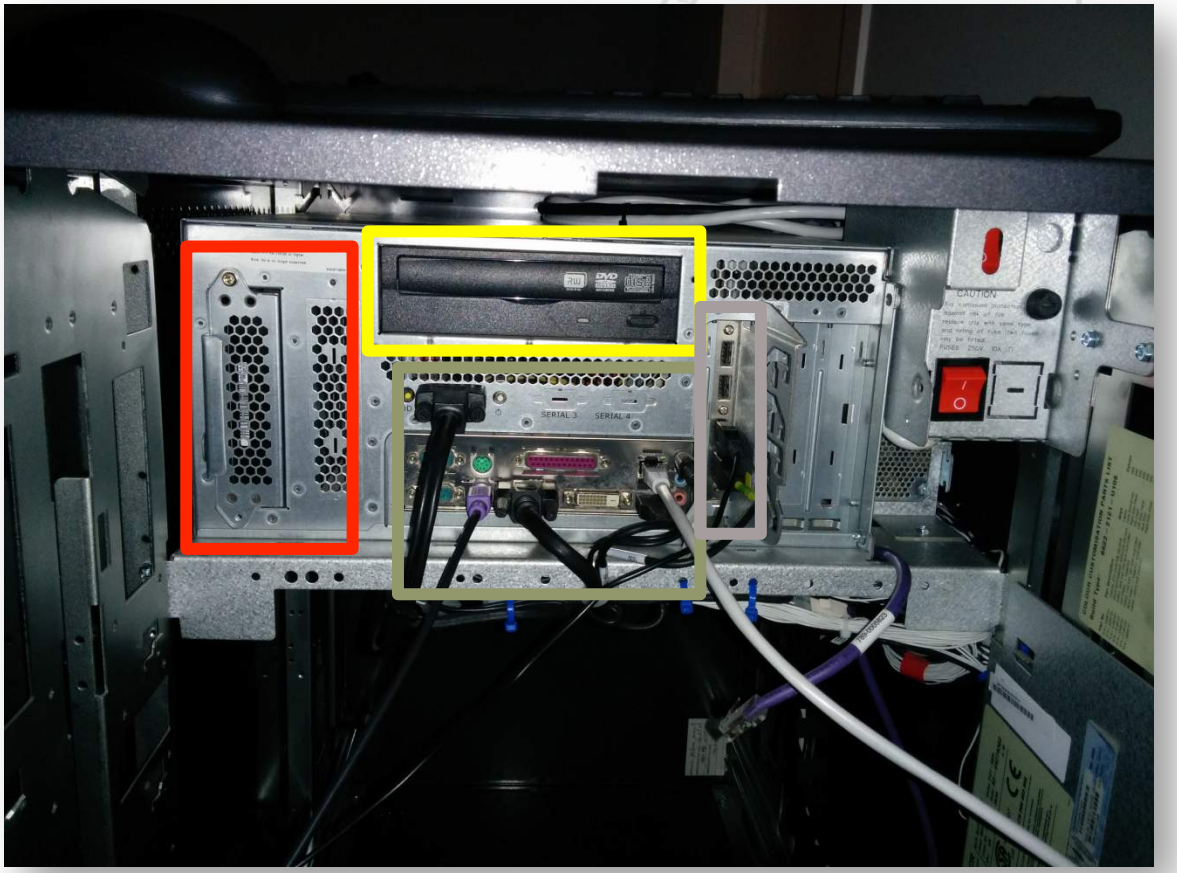
ATM?

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

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

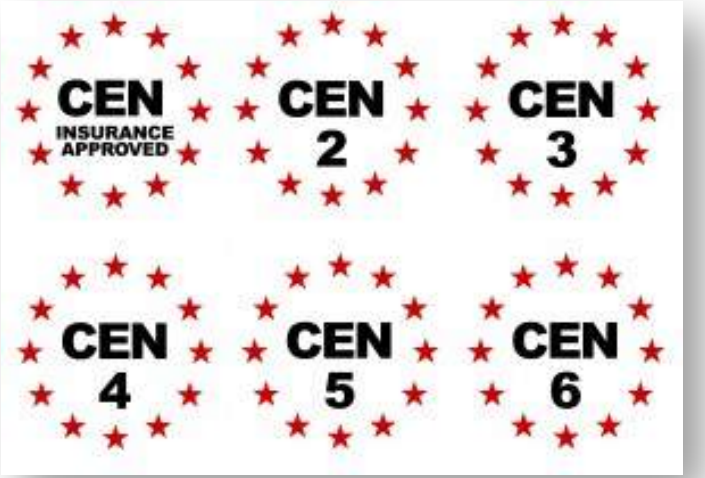
How to attack the ATM?

Blow up the safe

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 communication

...

How to attack the ATM?

Blow up the safe

Attack back-end

Copy cards & steal PIN codes

Steal the entire thing

...

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

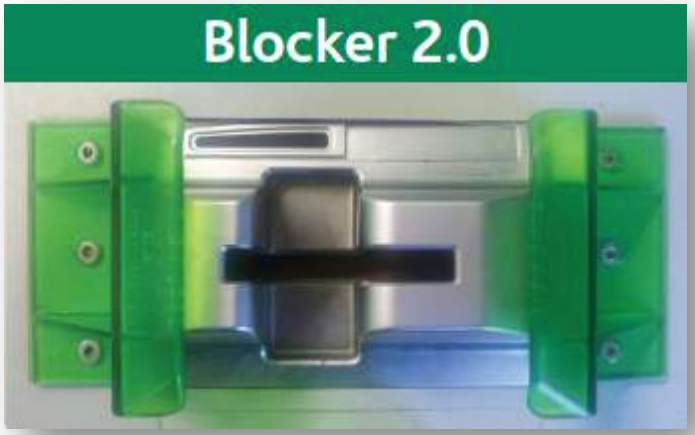
Have you seen this person? Police allege the suspect has stolen $47,000 from area bank machines.

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

Comment 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

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.

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

Attack back-end communication

Copy cards & steal PIN codes

Attack the OS

Steal the entire thing

Access "operator" mode

...

How to attack the ATM?

Adam Greenberg, Reporter

October 28, 2013

ATM malware Ploutus updated with English-language version

Attack back-end

communication

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

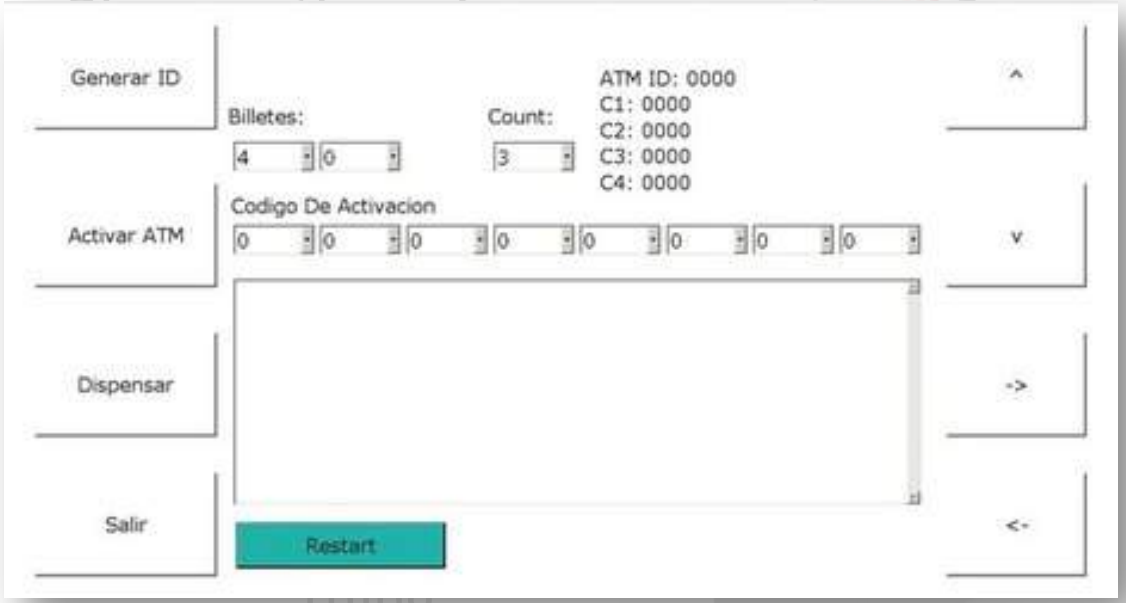
Access
"operator" mode

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

...

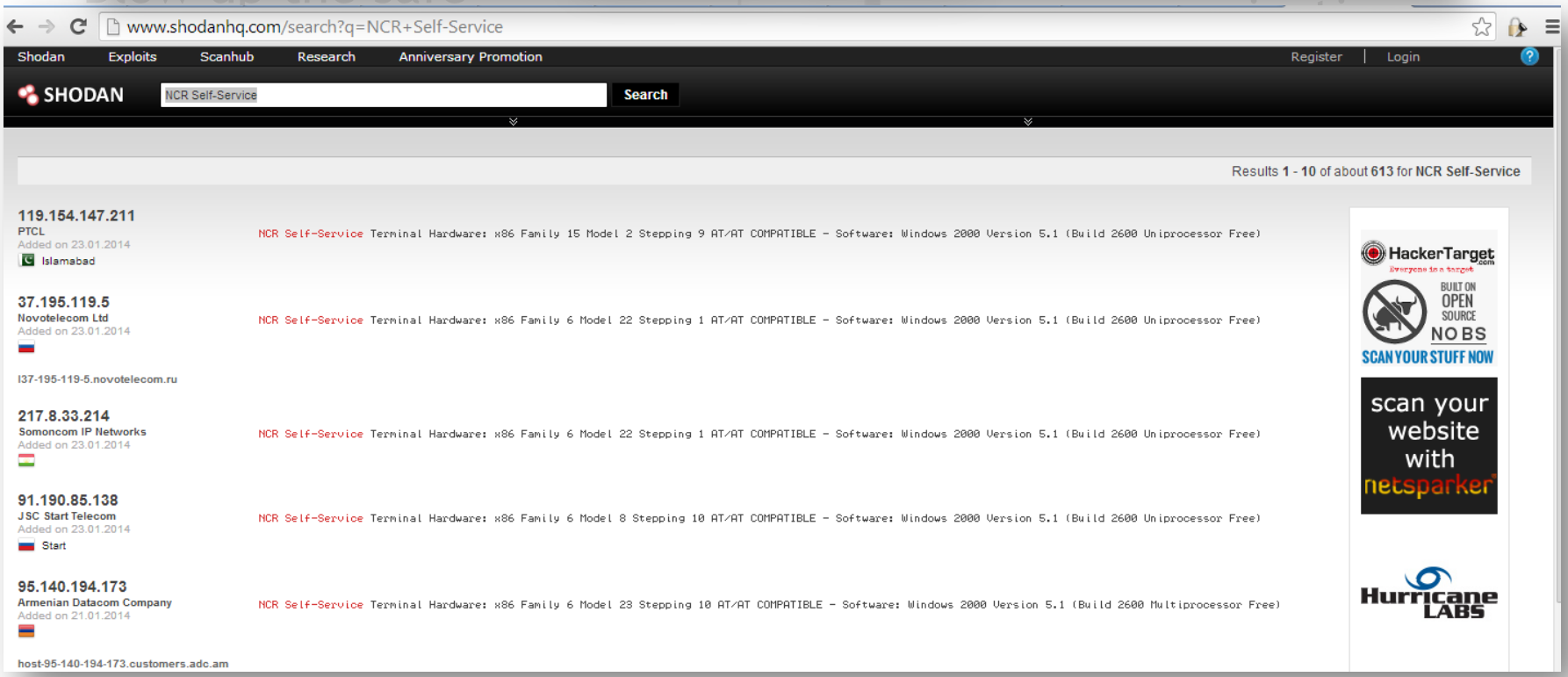
How to attack the ATM?

Barnaby Jack
"Jackpotting ATMs" - 2010

Attack the OS

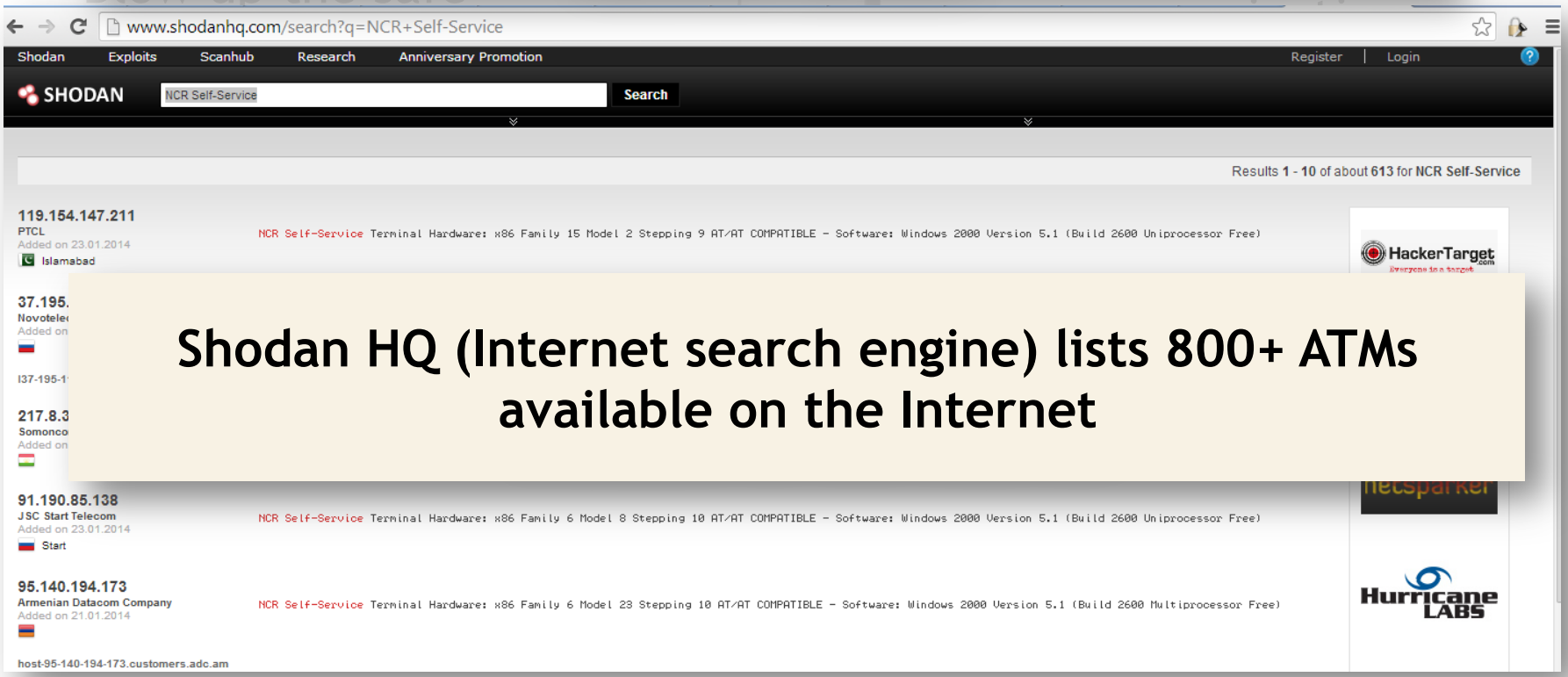
How to attack the ATM?

Network access?



How to attack the ATM?

Network access?



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

How to attack the ATM?

Attack back-end communication

Attack the OS

Access "operator" mode

CCC 2013
"Electronic bank robberies"
Boot ATMs from USB

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

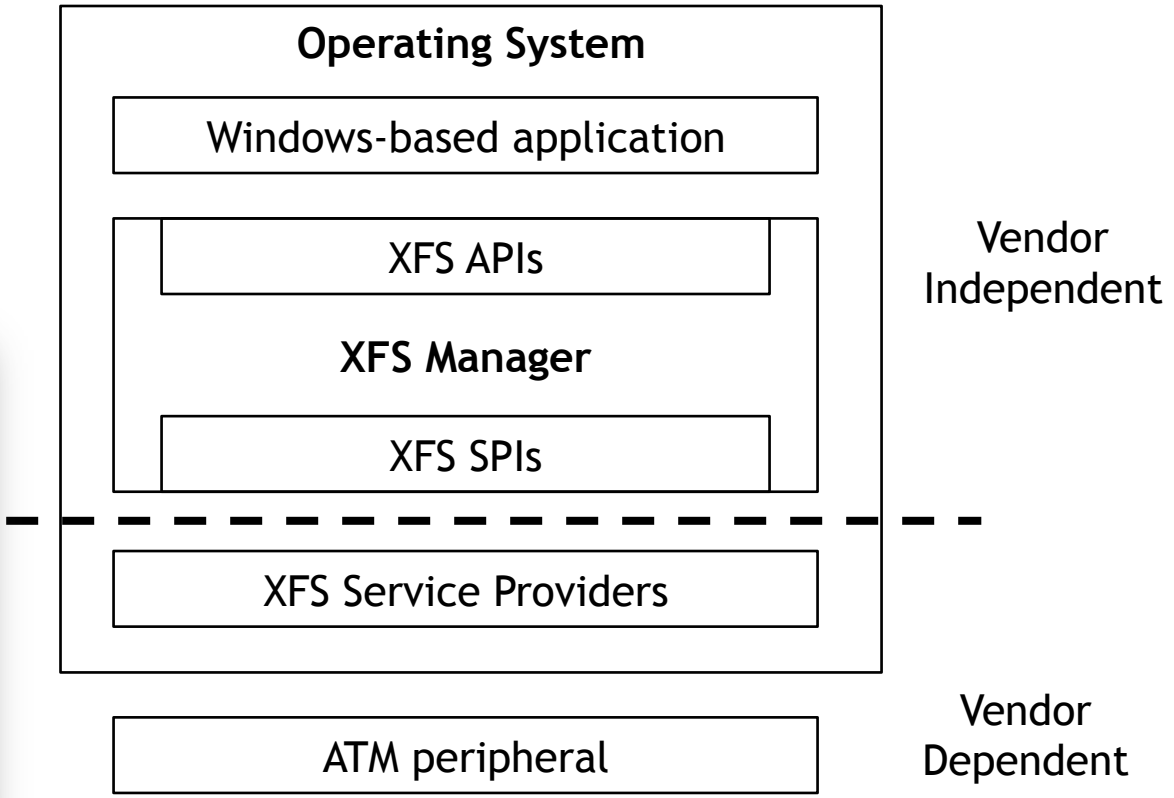
CEN/XFS Device Classes

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

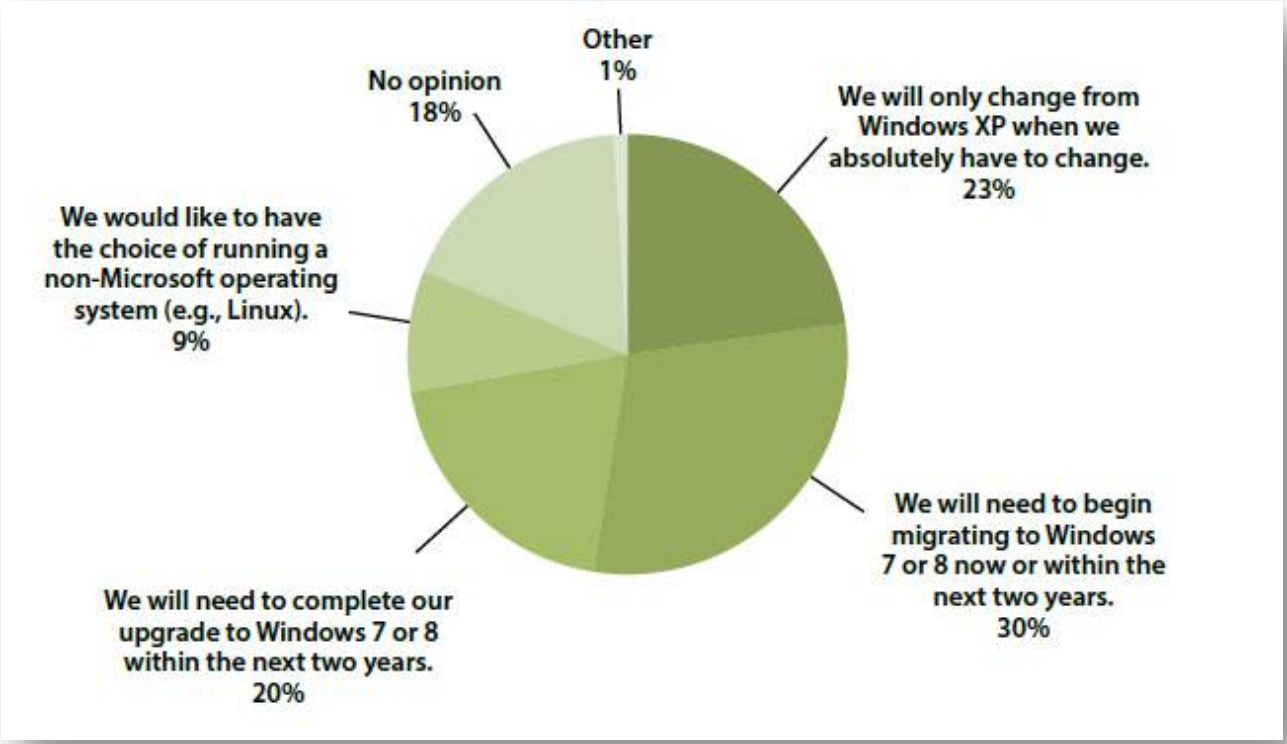


ATM system design

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

ATM system design

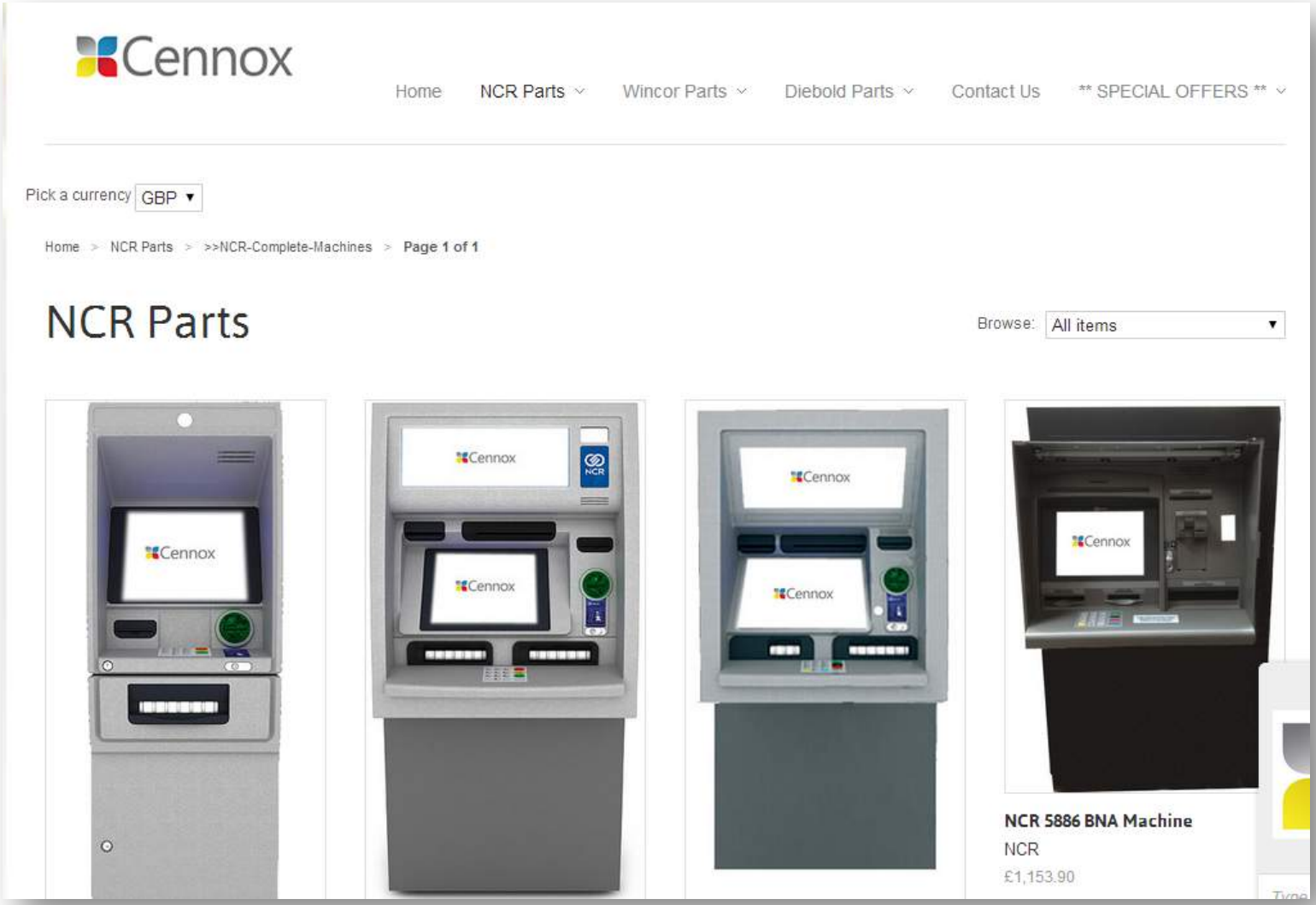
“How will you approach the Windows XP end-of-support?”
(KAL 2013 – ATM Software Trends & Analysis)



Topics for today

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

Where to start?



ATM delivery 101

Let’s get started

Physical access?

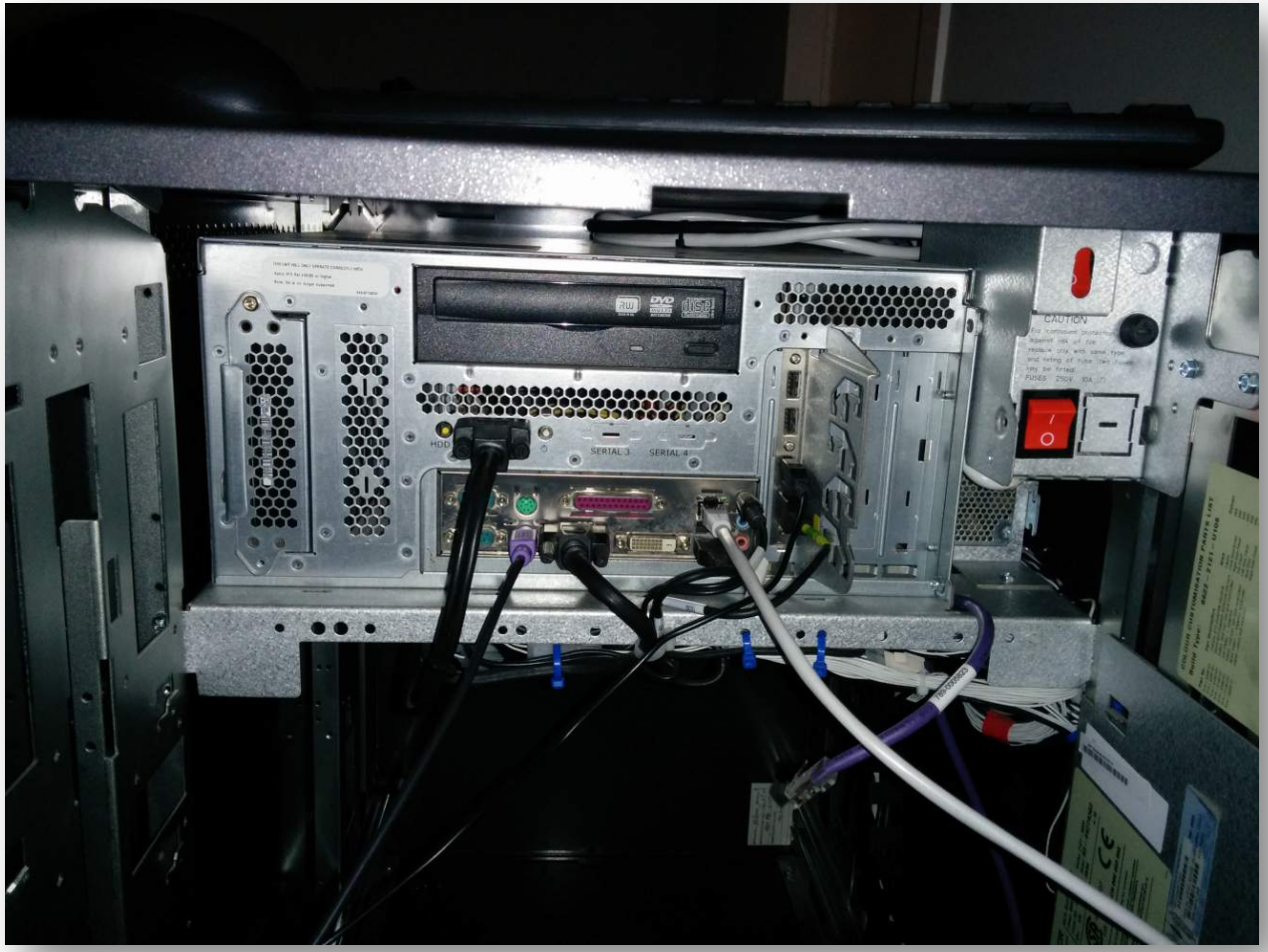
Physical access?

Physical access?

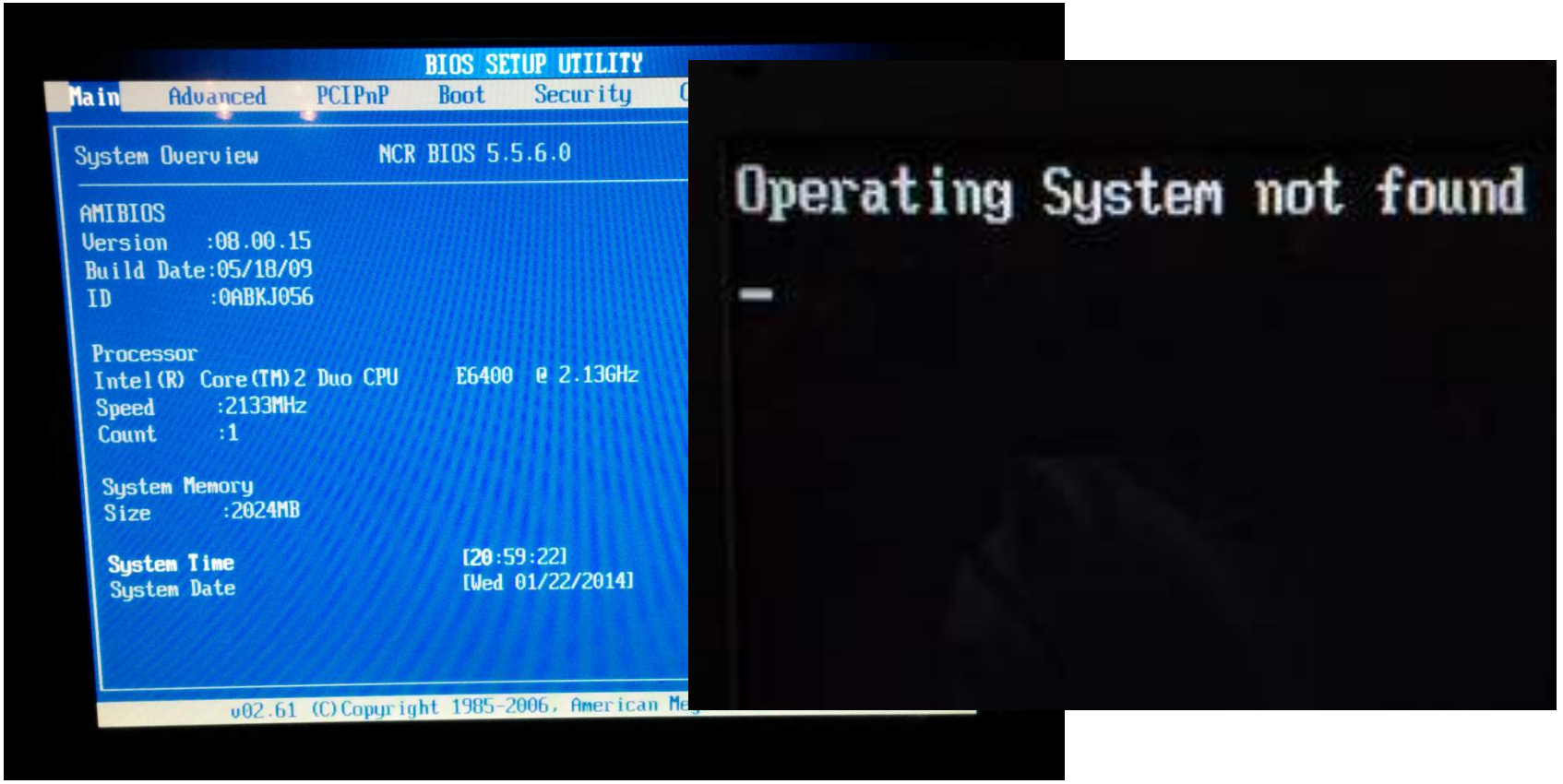
Physical access?

Physical access?

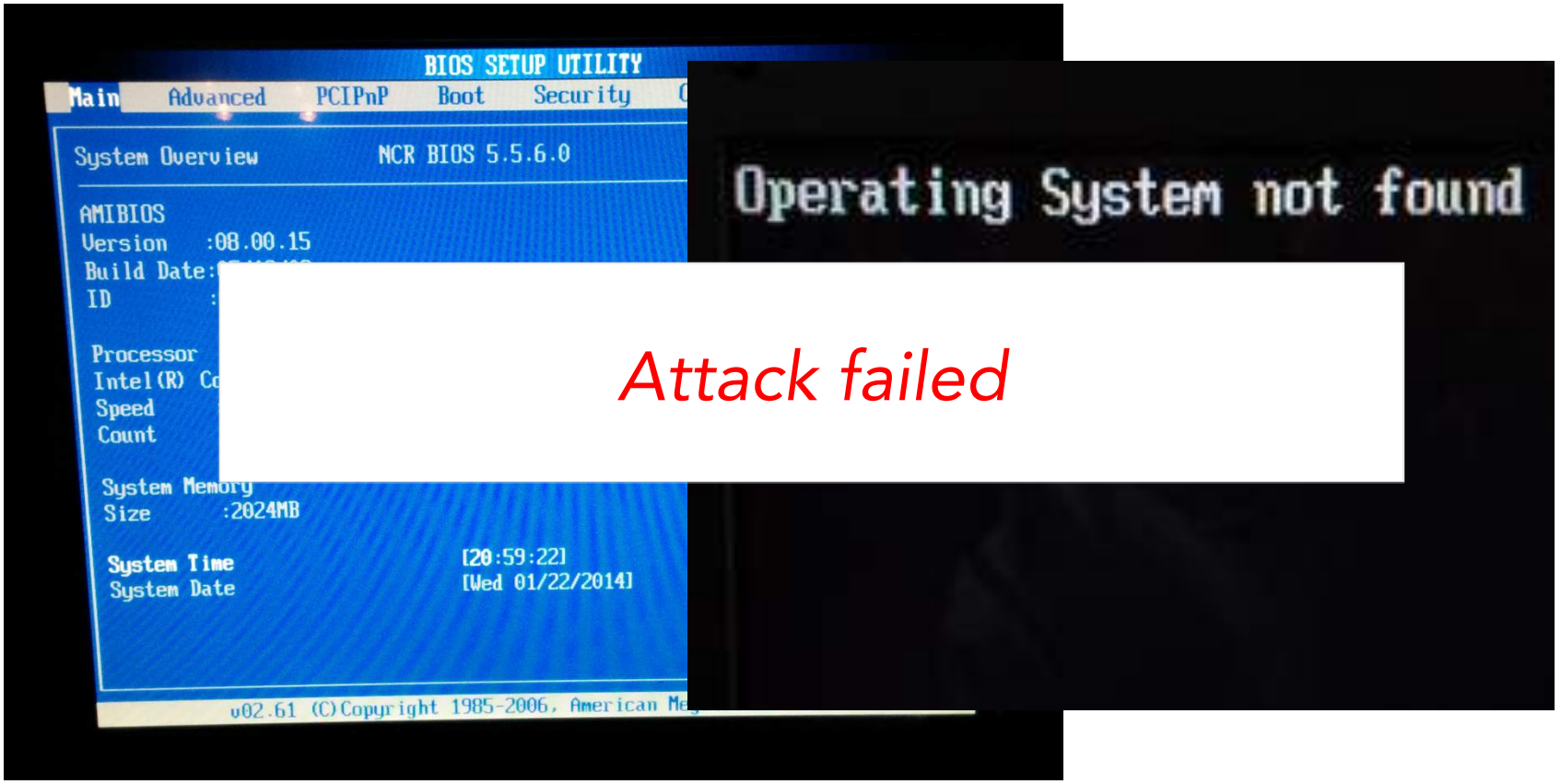
Physical access?



Running the ATM

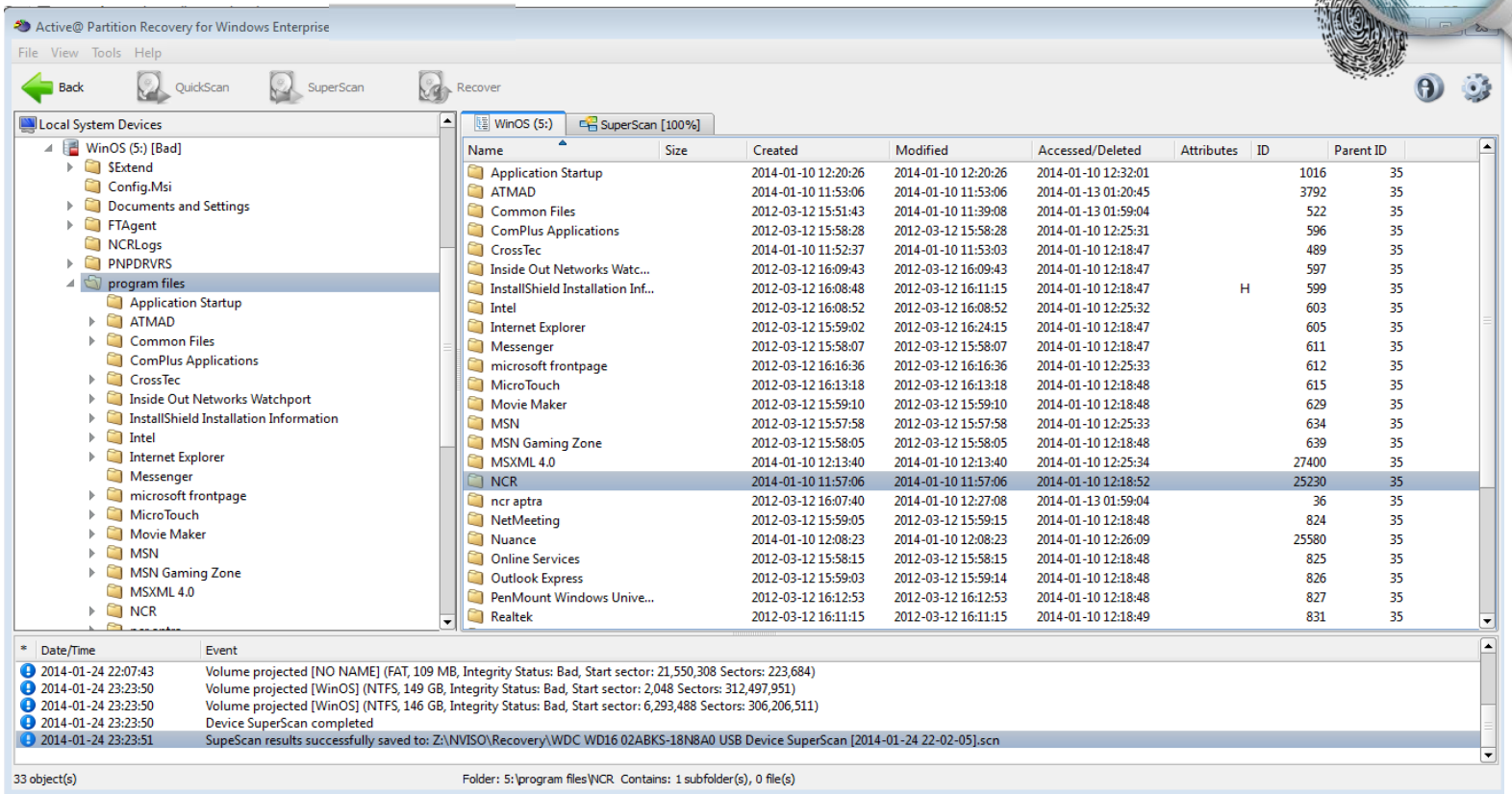


Running the ATM



ATM Forensics 101

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



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

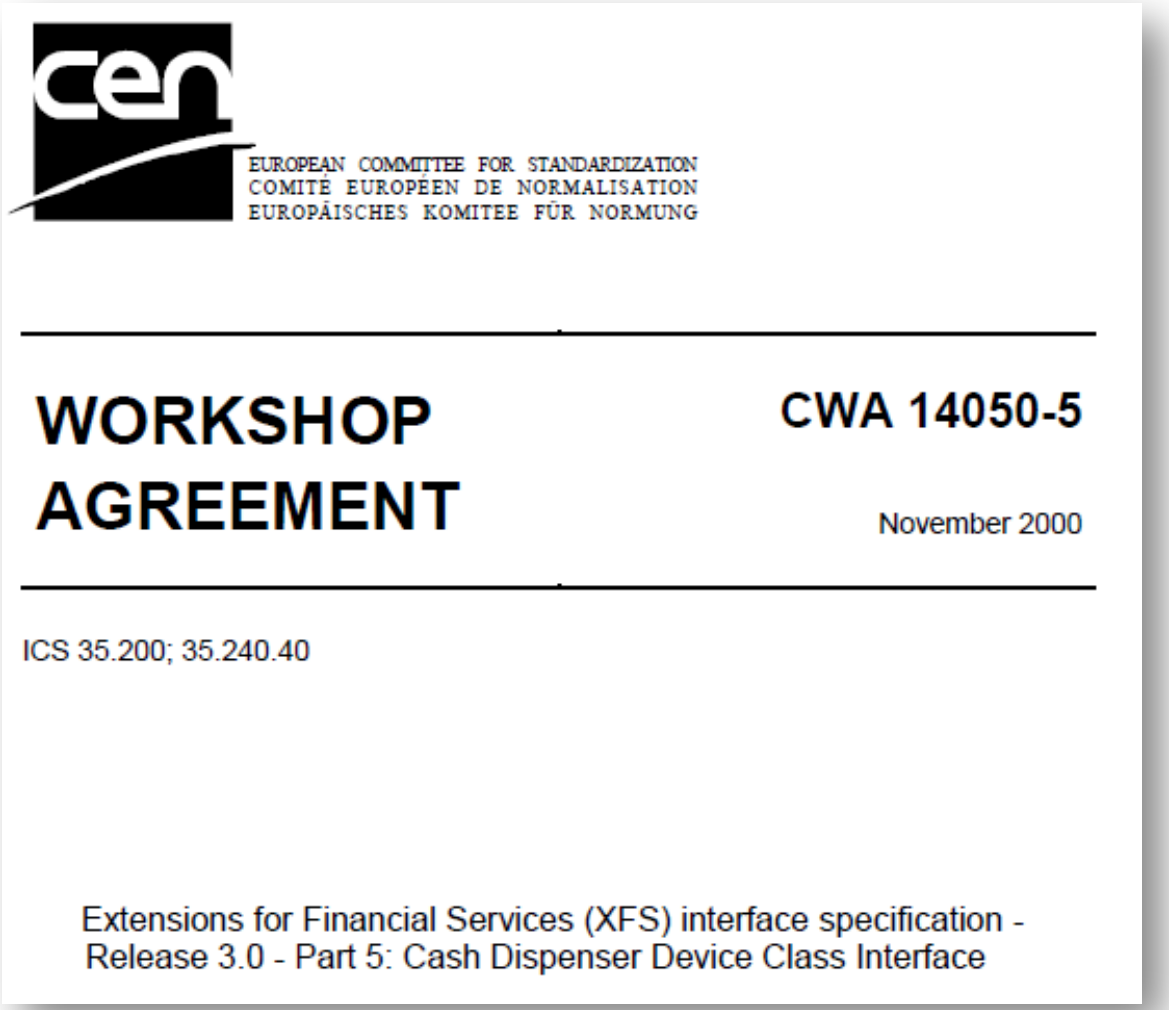
CWA 14050-1

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

```
WFSCDMDENOMINATION 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);
```

Set up XFS session with the "CurrencyDispenser1", no logging is required ☺

```
WFSCDMDISPENSE tDispense;
```

Create a dispense object "tDispense"

```
WFSCDMDENOMINATION tDenomination;
```

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';
```

€€€

I want “EUR” ☺

```
tDenomination.ulAmount=nviso_amount;

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

The amount is specified dynamically by a command line argument

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

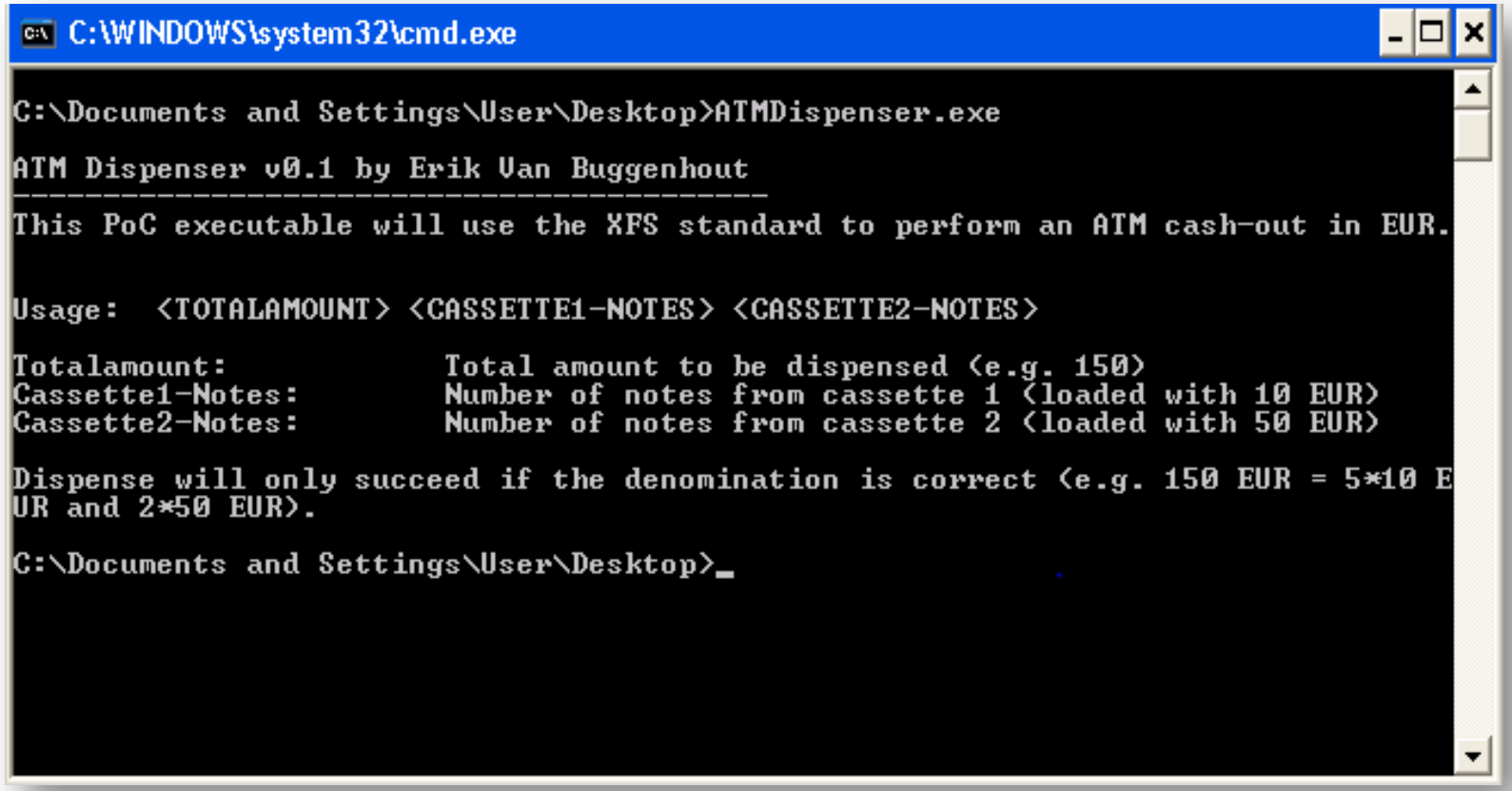
Specify how many notes you want per cassette

Software engineering 101

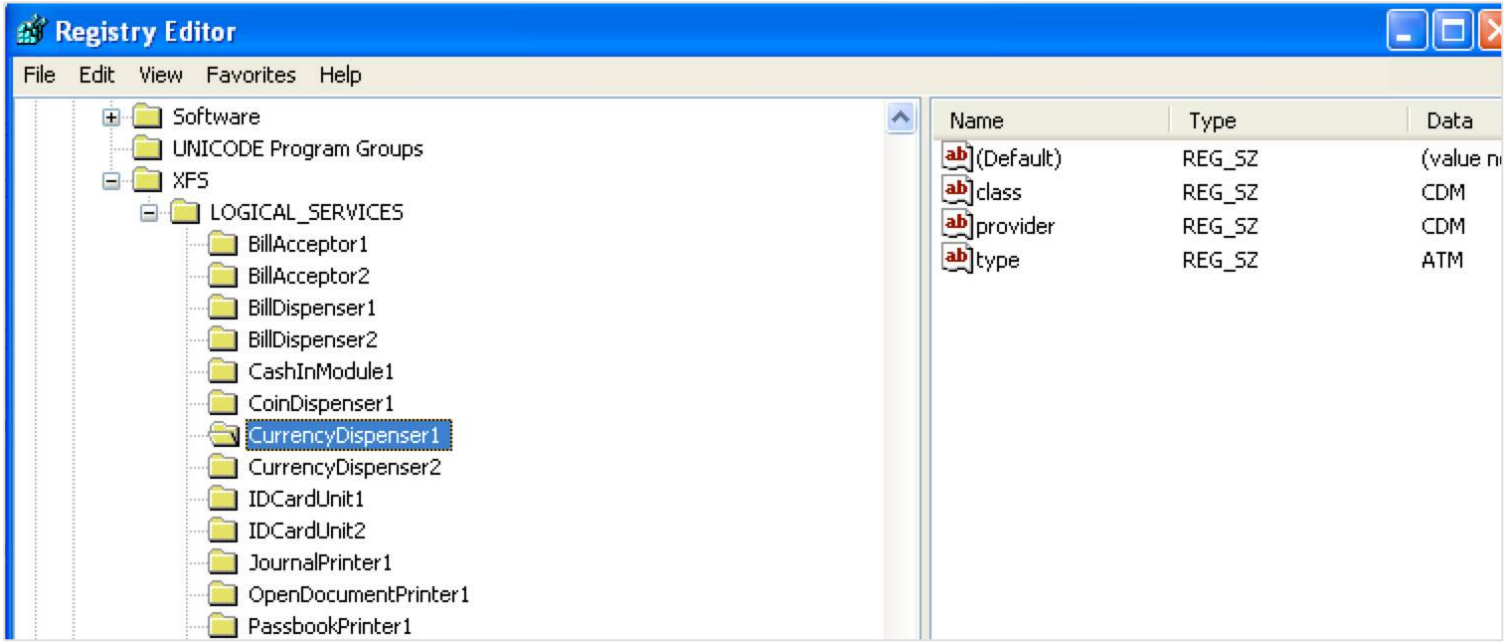
```
tDenomination.lpulValues = ulaValues;
tDispense.lpDenomination= &tDenomination;

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

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

Software engineering 101



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