ATM Security for Newbies

Kostikov Maxim

Deputy Head of Application Security Analysis Department
Positive Technologies

Moscow, August 25, 2022

About me

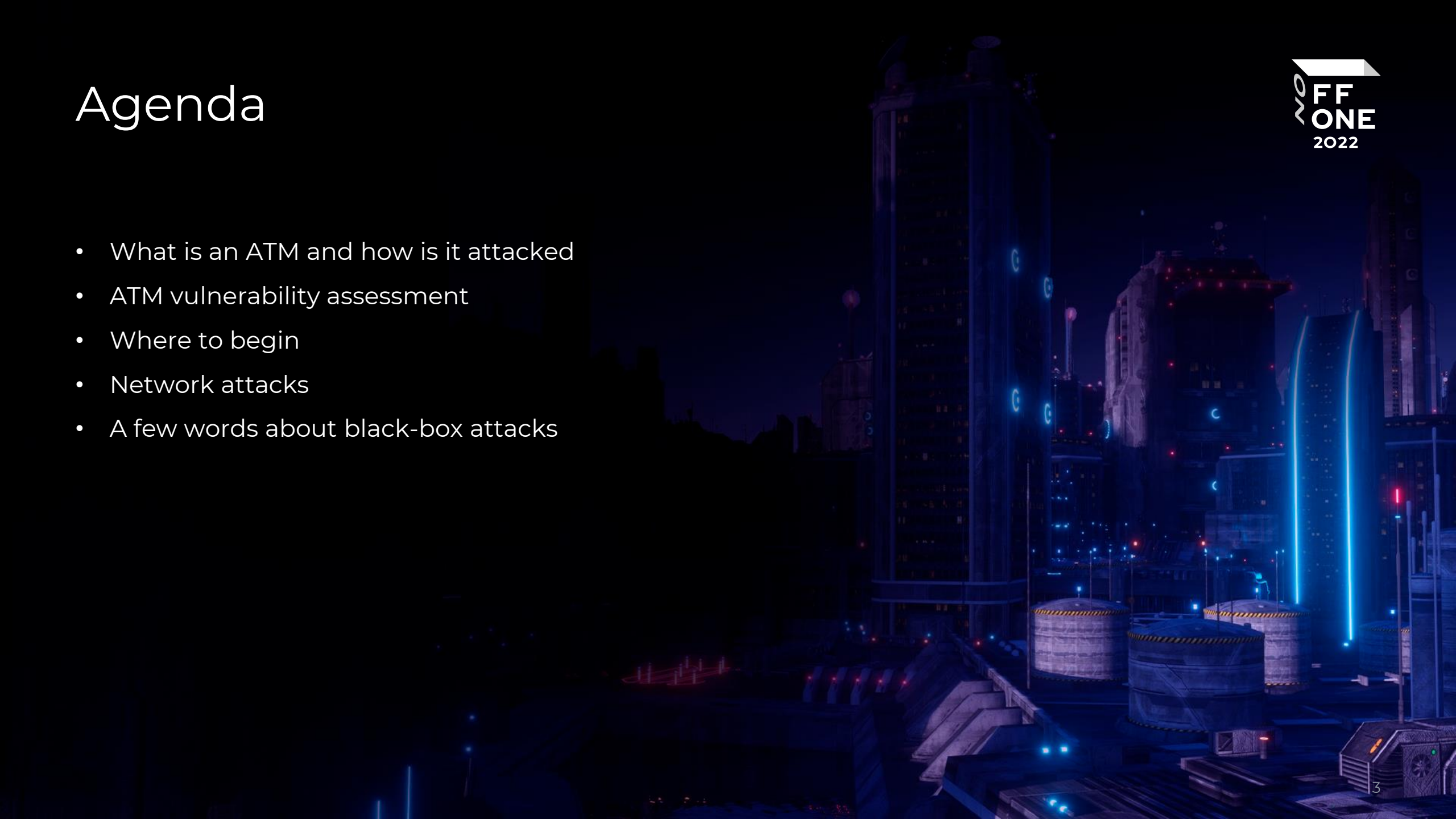
Member of PT SWARM

Certifications: AWAE, OSCP, eWPTX

Web, Android, Banking Security Researcher, bug hunter (GPSRP top 2 on HackerOne)

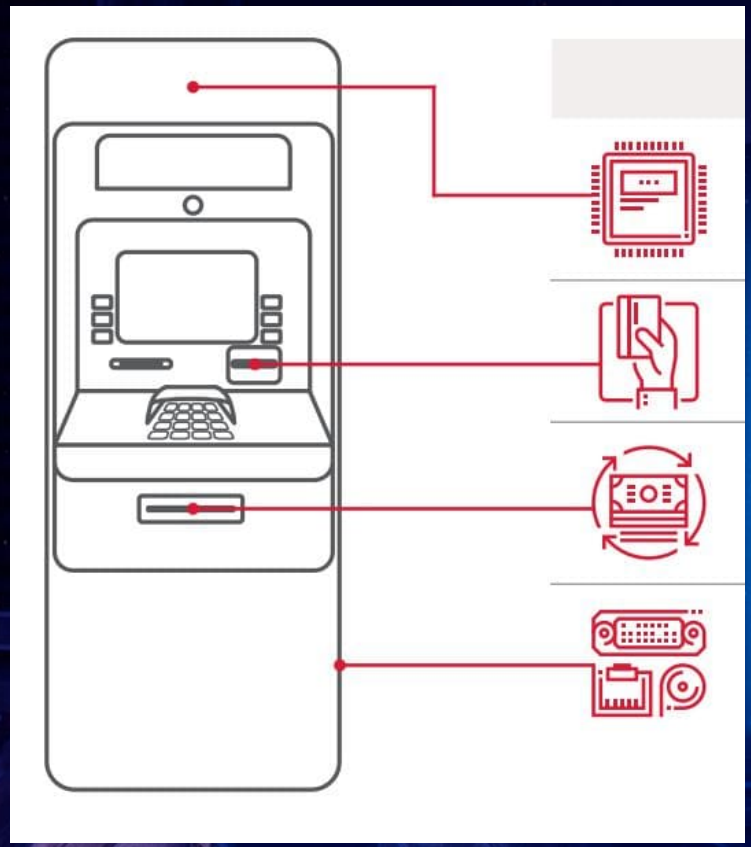
Agenda

- What is an ATM and how is it attacked
- ATM vulnerability assessment
- Where to begin
- Network attacks
- A few words about black-box attacks



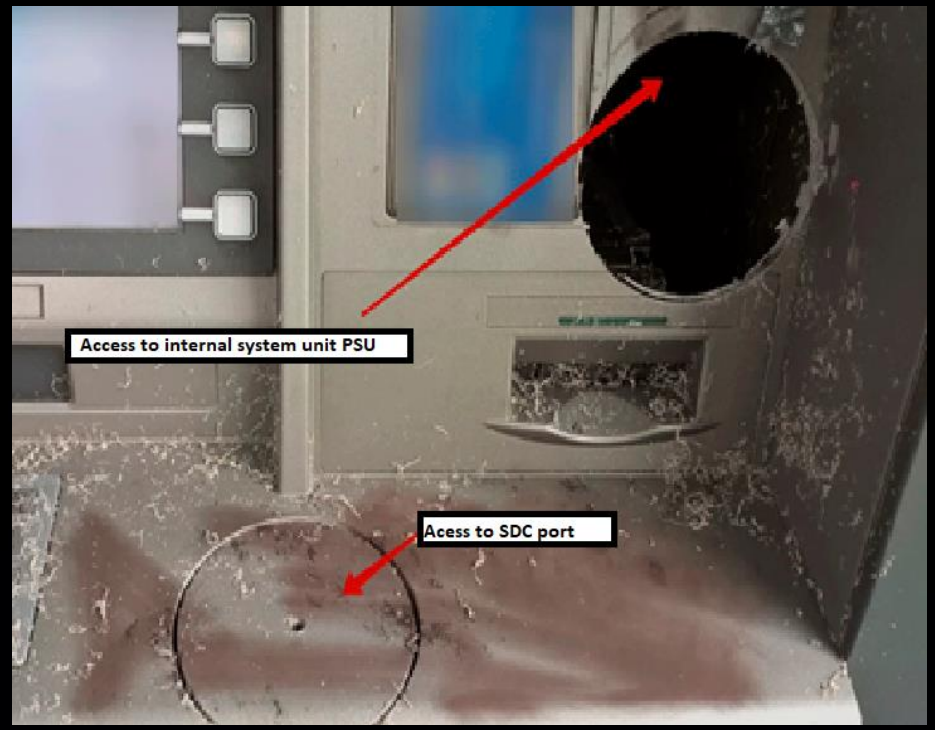
ATM

- System unit – a computer running Windows and special software for working with peripherals.
- PIN pad – numerical keypad.
- Dispenser – cash deposit/withdrawal mechanism
- Printer
- Card reader
- Modem - optional, for internet access or connection to the control network



How an ATM is hacked. Part I

How an ATM is hacked. Part II



ATM vulnerability assessment

Attack surface:

- PC – OS / software vulnerabilities / kiosk mode bypass
- Network
- Dispenser black-box attack
- Card reader

Conditions:

- Requires access to the service area of the ATM

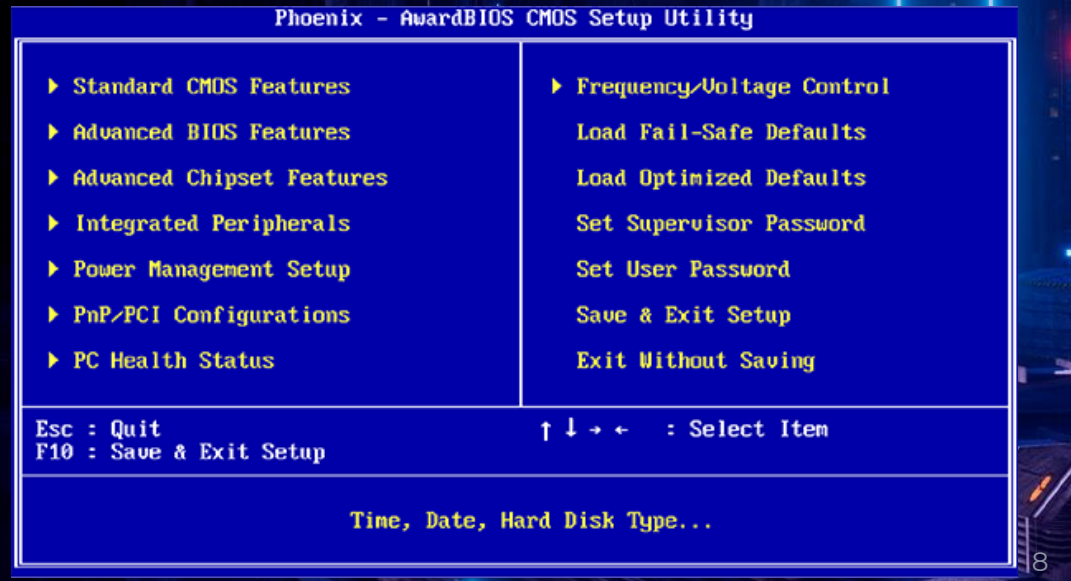
After analyzing the security of an ATM and fixing vulnerabilities, protection against logical attacks on ATMs is significantly increased.

Where to begin. ATM startup

Given: the system is booting

Goal: get command execution/impact on system files

- BIOS password
- Hard drive encryption
- Boot order



Where to begin. Windows

Given: booting windows/kiosk

Task: get the execution of commands

- Safe mode
- Hotkeys
- Race condition

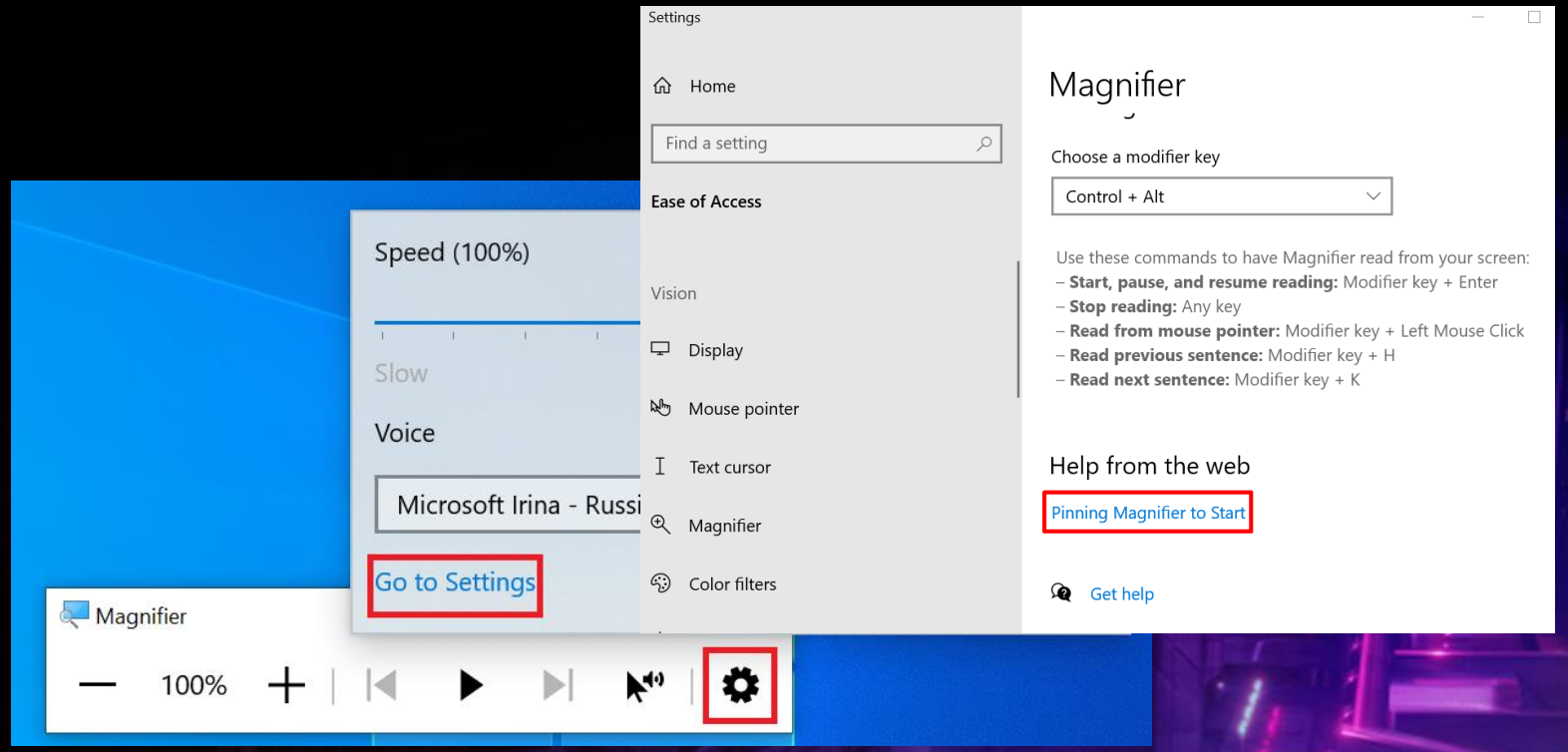
Windows XP/7/10

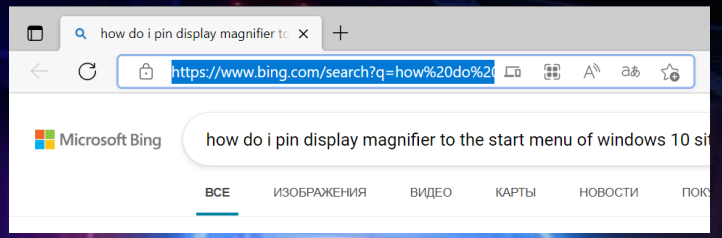
Hotkeys

After loading Windows, our task is to exit the kiosk.

Kiosk security is usually done by blocking hotkeys through software or Windows policies.

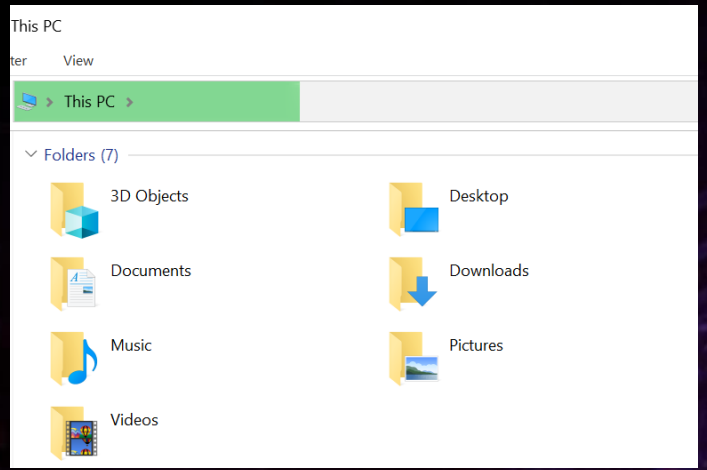
Kiosk bypass example: Win + “+” > Settings > Control Panel > Browser > cmd > Win

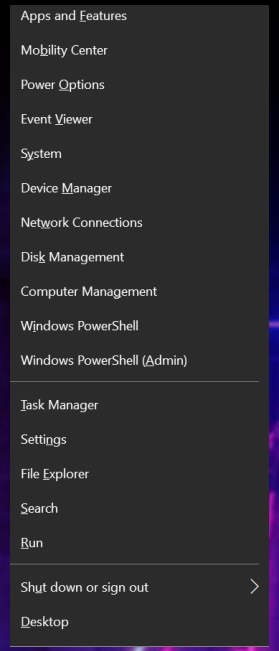


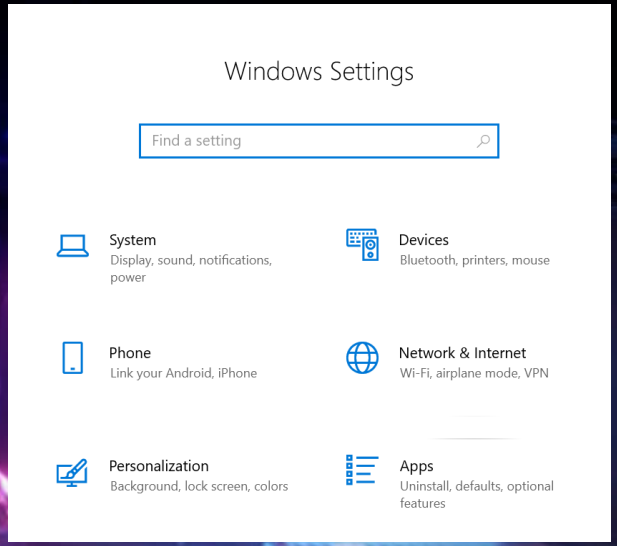


Hotkeys

- Windows logo key + E to open File Explorer
- Windows logo key + X to open the Quick Link menu
- Windows logo key + I to open Settings
- Etc.







What’s next?

Now we’ve bypassed kiosk mode. What’s next?

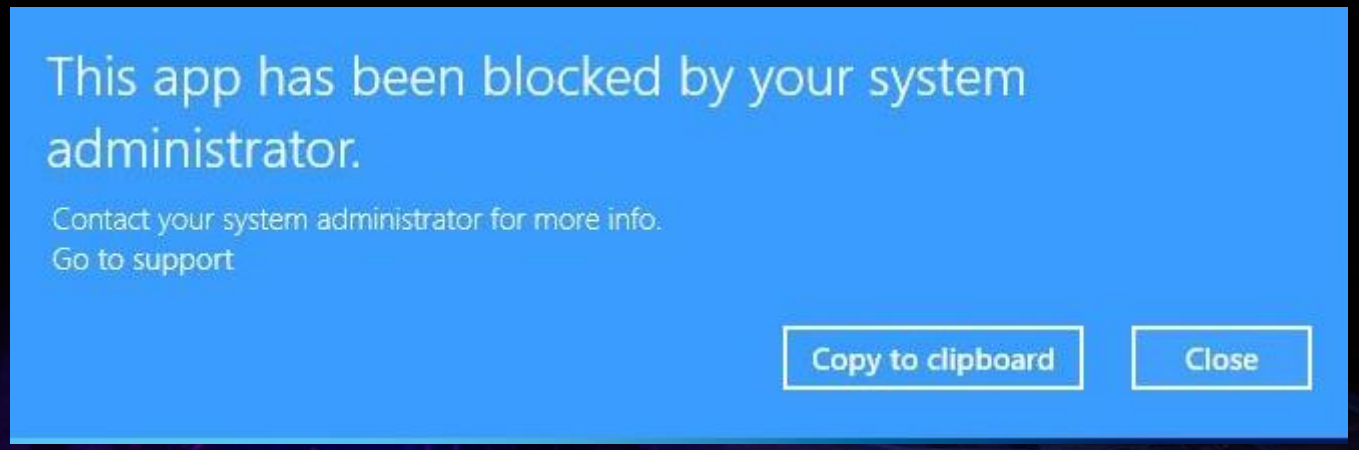
If the ATM doesn’t have additional security, we can run cmd and try to get administrative privileges.

If the ATM has addition security rules or applocker, we can try to bypass them, then run cmd and try to get administrative privileges.

ATM security

Popular methods ATMs use to block apps:

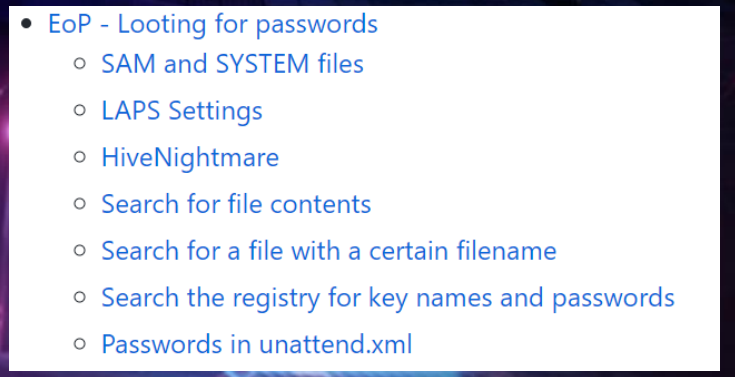
- Hash and allow list
- Trusted process
- Trusted folder
- Trusted apps
- Antivirus
- Group policy
- Etc.



Bypass security

We can bypass security checks by:

- Privilege escalation
  - Hardcoded/saved passwords (cmd/powershell logs, etc.)
  - Windows vulnerability exploits
  - Etc.
- Trusted process/folder/apps
  - Compile .Net app with command execution
  - Place our .exe to trusted folder
  - Run process from trusted process (e.g. from startup cmd)
  - Etc.



Now what...?

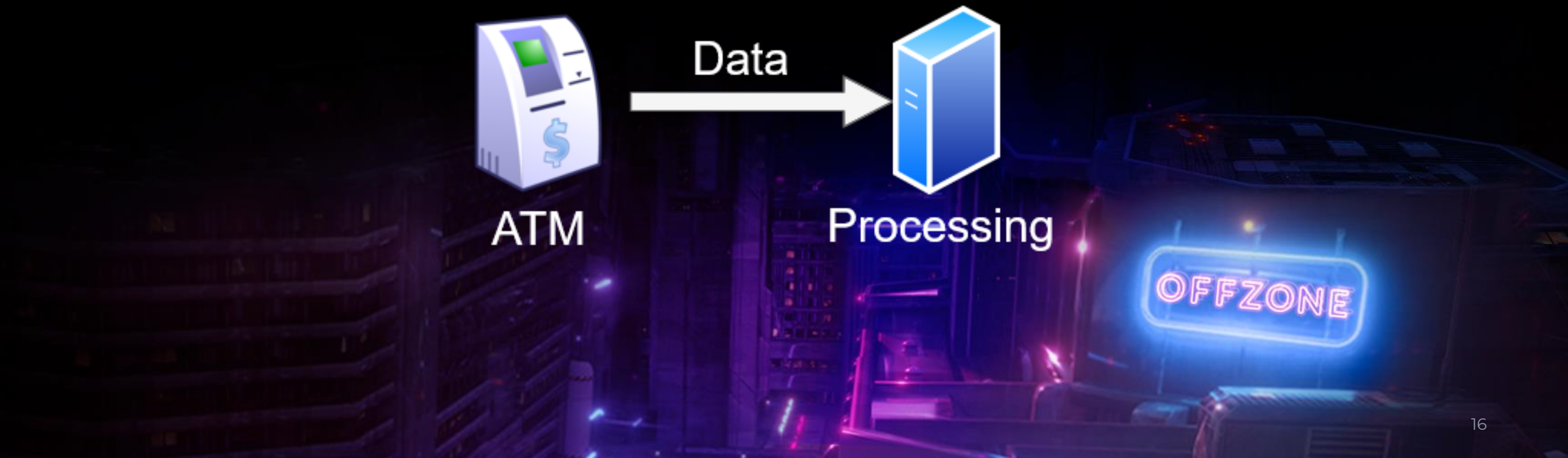
After finding all the ways to exit kiosk mode, bypass security policy/applocker, and get administrative privileges...

The next step is to check the ATM's network security:

- Who does the ATM communicate with?
- What open ports are there?
- What are protocol protection mechanisms?
- What connection encryption mechanisms are used?

Processing

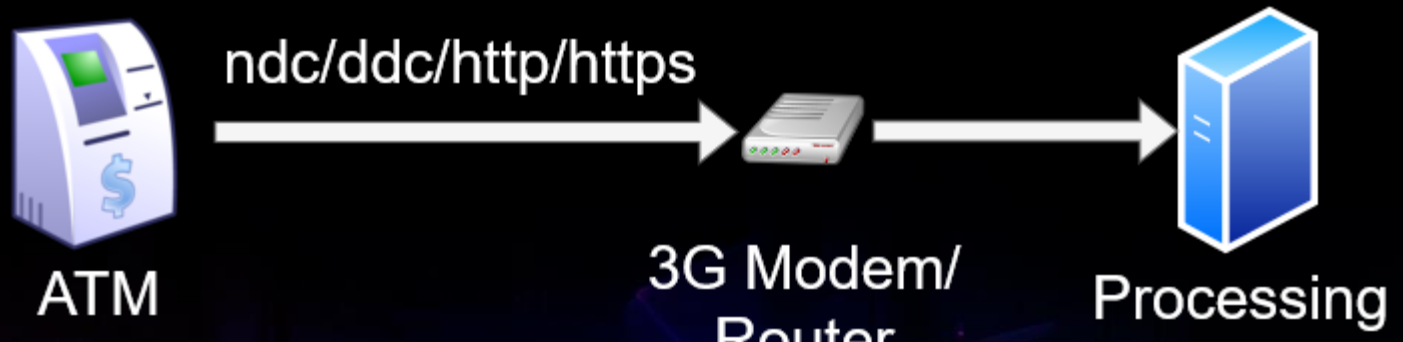
Processing is a server for processing transactions and operations performed at an ATM.



Networking

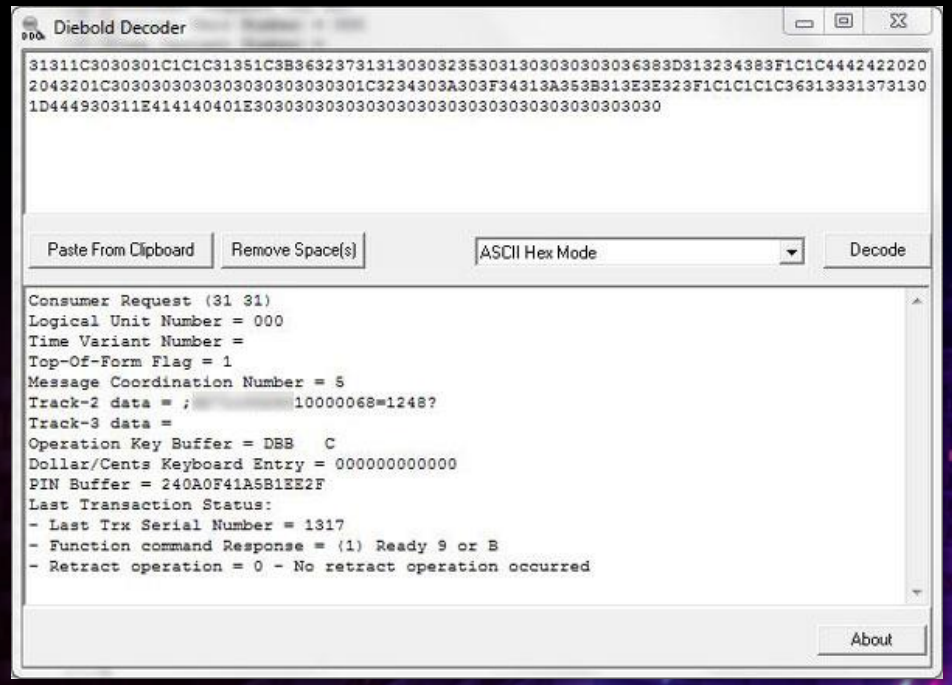
Services:

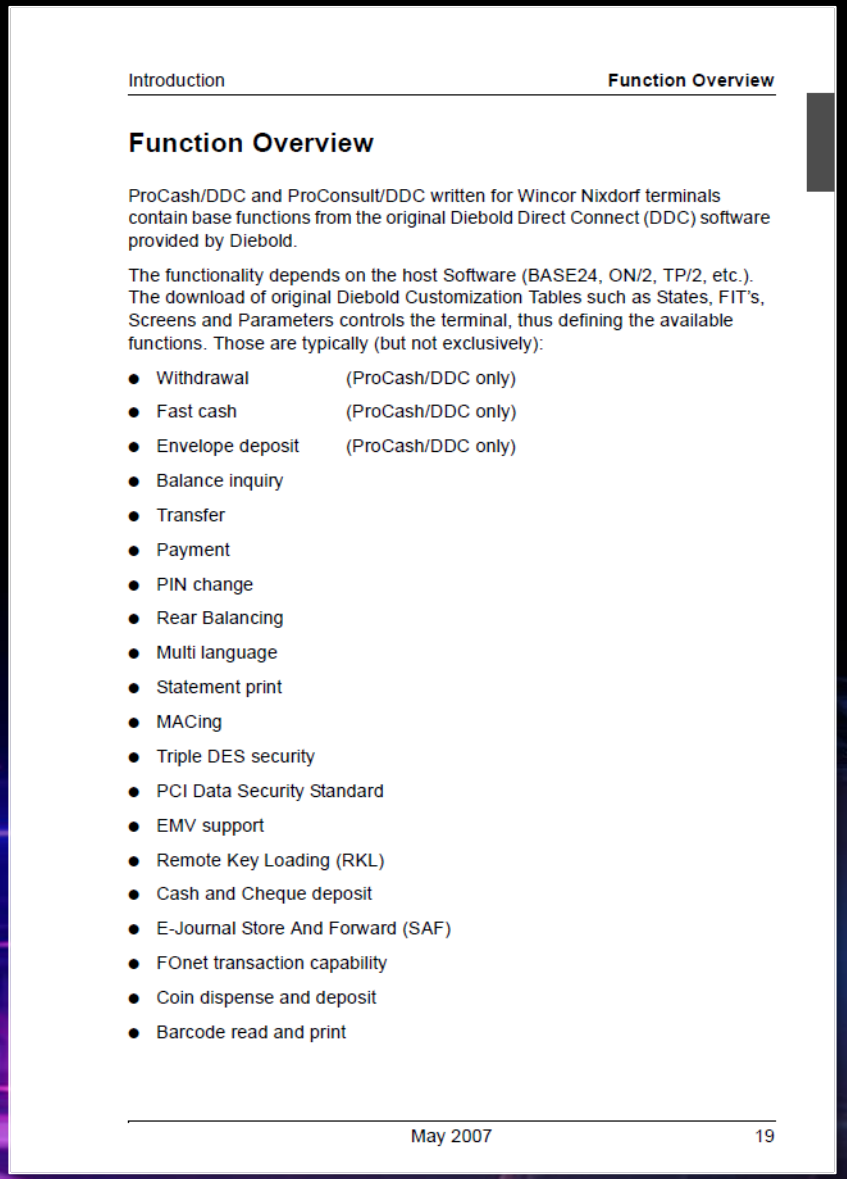
- ATM-specific (processing)
  - NDC
  - DDC
  - Custom
- Remote management
- OS



Diebold Direct Connect (DDC)

- Proprietary, but…
- Online documentation
- Easy to implement
- Reveals information about cards





Introduction **Function Overview**

Function Overview

ProCash/DDC and ProConsult/DDC written for Wincor Nixdorf terminals contain base functions from the original Diebold Direct Connect (DDC) software provided by Diebold.

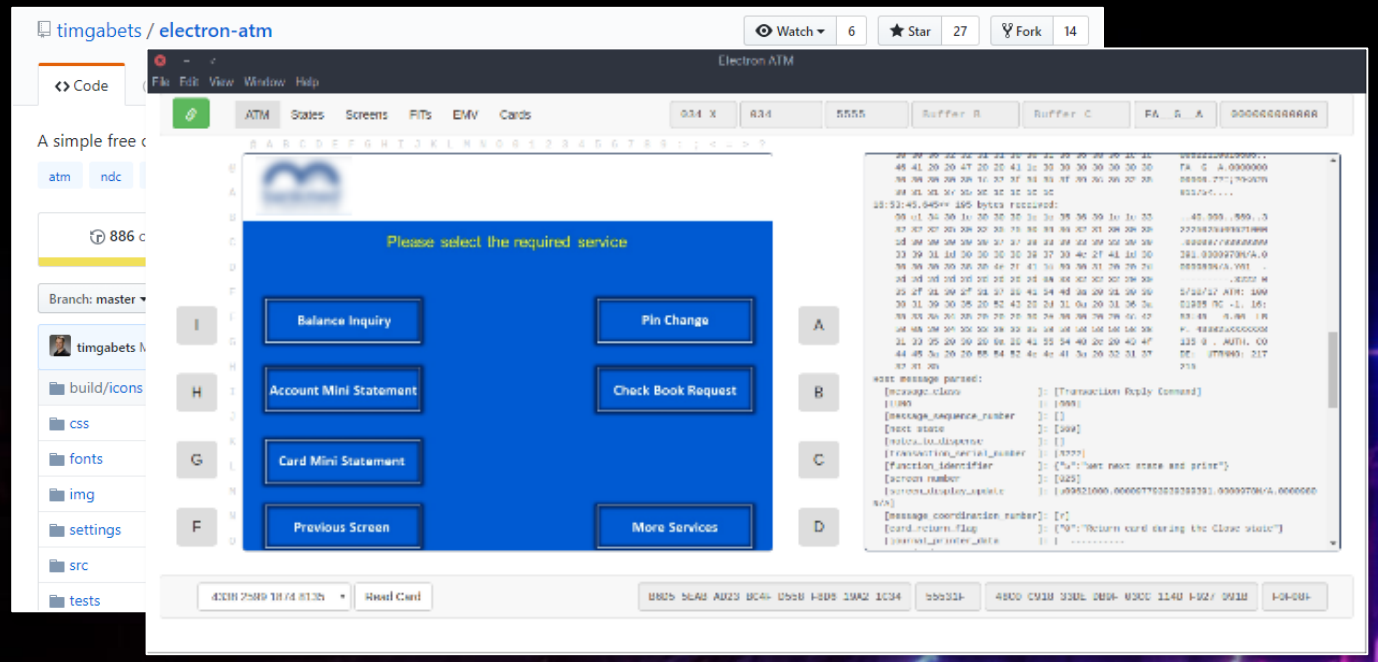
The functionality depends on the host Software (BASE24, ON/2, TP/2, etc.). The download of original Diebold Customization Tables such as States, FIT's, Screens and Parameters controls the terminal, thus defining the available functions. Those are typically (but not exclusively):

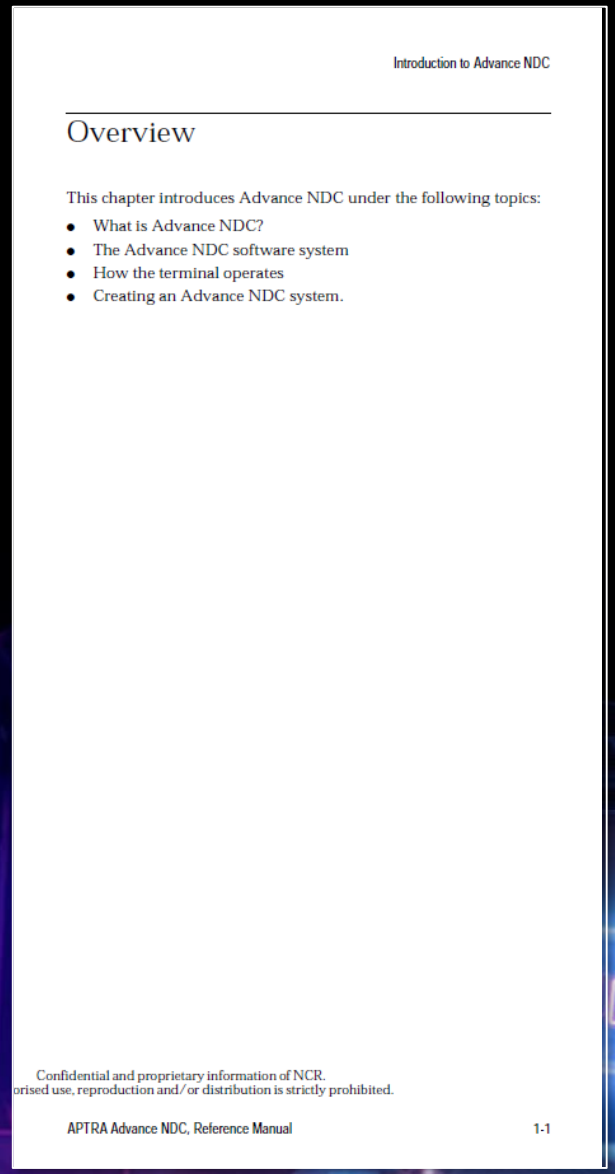
- Withdrawal (ProCash/DDC only)
- Fast cash (ProCash/DDC only)
- Envelope deposit (ProCash/DDC only)
- Balance inquiry
- Transfer
- Payment
- PIN change
- Rear Balancing
- Multi language
- Statement print
- MACing
- Triple DES security
- PCI Data Security Standard
- EMV support
- Remote Key Loading (RKL)
- Cash and Cheque deposit
- E-Journal Store And Forward (SAF)
- FOnet transaction capability
- Coin dispense and deposit
- Barcode read and print

May 2007 19

NCR Direct Connect (NDC)

- Proprietary, but...
- Online documentation
- Easy to implement
- Reveals information about cards





Introduction to Advance NDC

Overview

This chapter introduces Advance NDC under the following topics:

- What is Advance NDC?
- The Advance NDC software system
- How the terminal operates
- Creating an Advance NDC system.

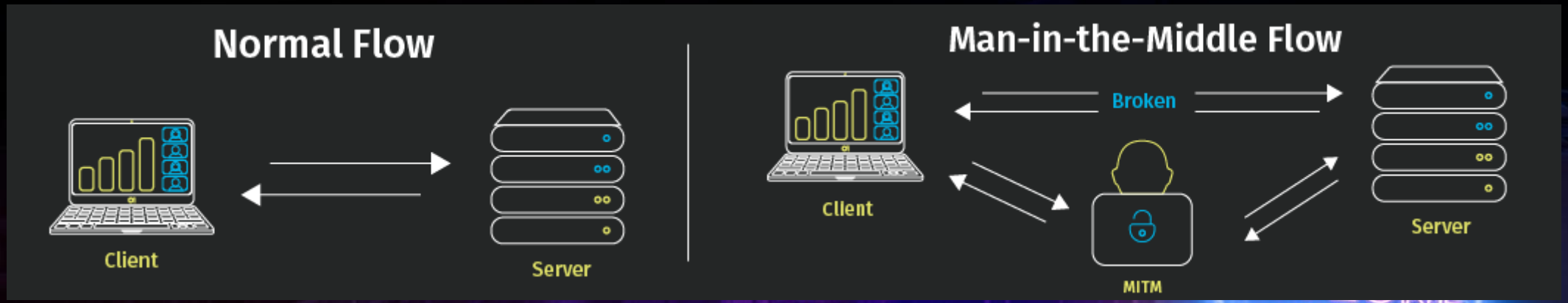
Protocol security ndc/ddc

- VPN/Firewall
- Protocol level protection
  - MAC – cryptography that signs a series of commands, such as issuing money. The latest versions are protected from replay attacks using a nonce. in this case track2 is still transmitted in the clear.
  - Plain text
- Protocol level encryption – ssl

How to MITM

Ways to connect to the ATM network:

- Service area access
- Access to an external router



Attacks

- MITM and read unencrypted traffic
- Data spoofing
- Attacks on encrypted traffic
- RCE in third party services

Read unencrypted traffic

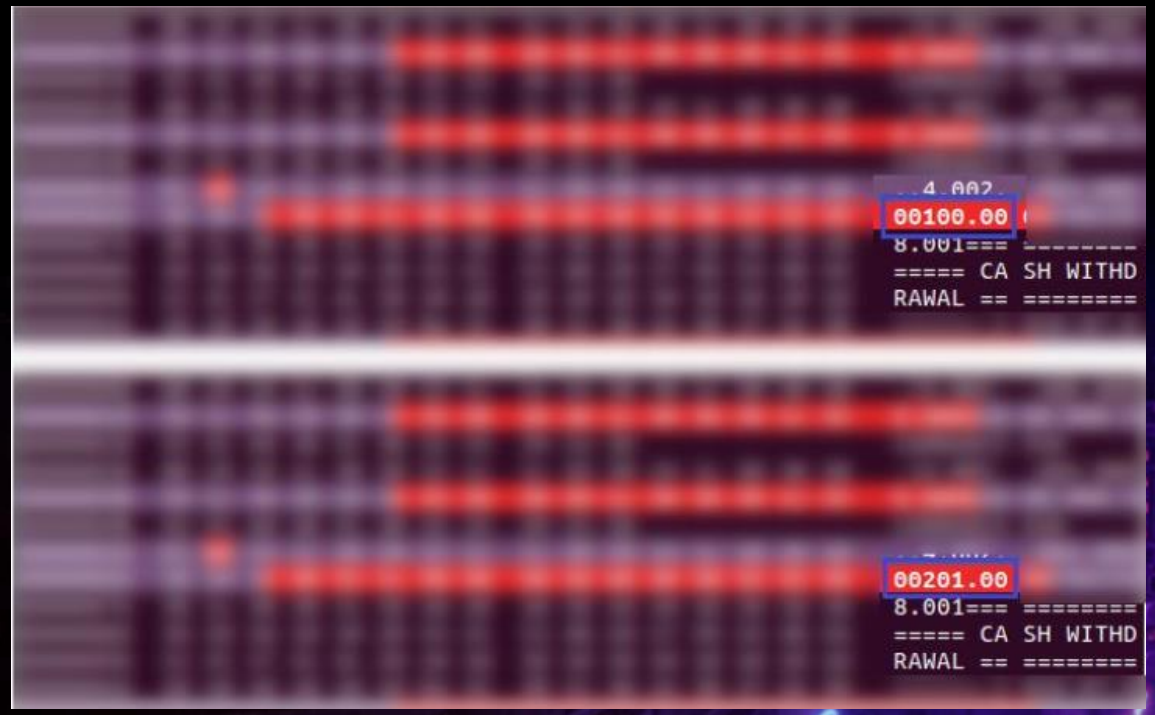
Track2 –PAN, Exp Date

Wireshark · Follow TCP Stream (tcp.stream eq 0)

```
00000000  00                                                .
00000001  01 60 31 31 1c 30 30 32  1c 1c 1c 31 3a 1c 3b 34  .`11.002 ...1:.;4
00000011  38 [redacted]                                    3d  8[redacted]=
00000021  31 38 30 38 32 30 31 32  34 38 31 33 30 30 30 30  18082012 48130000
00000031  30 35 33 30 3f 1c 1c 41  41 20 20 20 20 20 20 1c  0530?..A A      .
```

Substitution of data when interacting with processing

Changing the number of cashed banknotes



Changing the number of dispensed cassettes

Attacks on encrypted traffic

- Using weak encryption mechanisms
- Using a proprietary encryption protocol
- No SSL pinning

RCE in third party services

Attack surface:

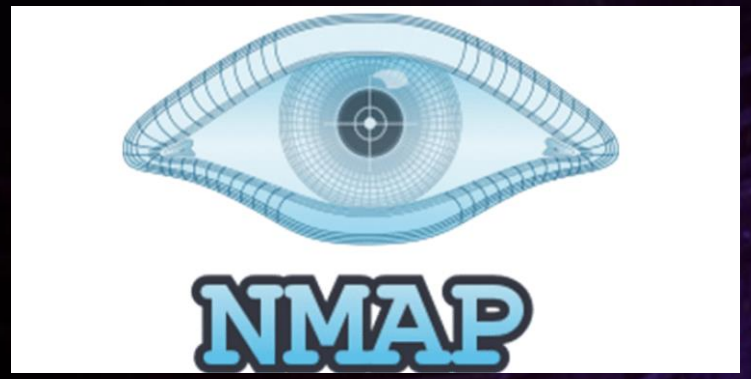
- Monitoring
- Administration services
- Services on open ports

```
msf5 > search ms17-010

Matching Modules
================

   #  Name                                      Disclosure Date  Rank     Check  Description
   -  ----                                      ---------------  ----     -----  -----------
   0  auxiliary/admin/smb/ms17_010_command      2017-03-14       normal   No     MS17-010 EternalRomance/EternalSynergy/EternalChampion SMB
 Remote Windows Command Execution
   1  auxiliary/scanner/smb/smb_ms17_010                         normal   No     MS17-010 SMB RCE Detection
   2  exploit/windows/smb/doublepulsar_rce      2017-04-14       great    Yes    DOUBLEPULSAR Payload Execution and Neutralization
   3  exploit/windows/smb/ms17_010_eternalblue  2017-03-14       average  Yes    MS17-010 EternalBlue SMB Remote Windows Kernel Pool Corrup
tion
   4  exploit/windows/smb/ms17_010_eternalblue_win8  2017-03-14  average  No     MS17-010 EternalBlue SMB Remote Windows Kernel Pool Corrup
tion for Win8+
   5  exploit/windows/smb/ms17_010_psexec       2017-03-14       normal   Yes    MS17-010 EternalRomance/EternalSynergy/EternalChampion SMB
 Remote Windows Code Execution


msf5 >
```



Some words about black-box attacks

- Type of logical attacks (along with XFS attacks and processing center emulation) using H/W devices to connect directly to dispenser for cash withdrawal
- Leave no traces, logs, etc. in most cases
- Requires knowledge of ATM’s internals and hardware
- Doesn’t depend on OS, processing center or application control software

What we do with it?

- Protocol encryption
- For old models: additional overlays that encrypt connections
- Buy latest dispenser model
  - USB
  - Protection against black box attacks
  - The dispenser has a firmware to protect the dispenser

What now

Most of ATM has a blacbkox security and an encryption of the command set.

But... This protection still has vulnerabilities. For more info:

- **BlackHat USA 2020 - Black Box is Dead. Long Live Black Box!**
- **Hardwear.io NL 2021 - Blackboxing Diebold-Nixdorf ATMs by Vladimir Kononovich**

Resume:

Even modern dispenser firmware needs security analysis.

Thank you!


OFF
ONE
2022