

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)



William manning

Agenda

• What is an ATM and how is it attacked

FF ONE

2022

William manna

- 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

Choose Advanced Options for: Windows10 (Use the arrow keys to highlight your choice.)

Safe Mode Safe Mode with Networking Safe Mode with Command Prompt

Enable Boot Logging Enable low-resolution video Debugging Mode Disable automatic restart on system failure Disable Driver Signature Enforcement Disable Early Launch Anti-Malware Driver

Start Windows Normally

Sescription: View a list of system recovery tools you can use to repair startup problems, run diagnostics, or restore your system.

Advanced Boot Options

ENTER=Choose

ESC=Cancel

Windows XP/7/10

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

- 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.

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.

This app has been blocked by your system administrator.

Contact your system administrator for more info. Go to support

Copy to clipboard

OFFZONE

Close

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.

Living Off The Land Binaries, Scripts and Libraries

For more info on the project, click on the logo.

If you want to contribute, check out our <u>contribution guide</u>. Our <u>criteria list</u> sets out what we define as a LOLBin/Script/Lib.

MITRE ATT&CK® and ATT&CK® are registered trademarks of The MITRE Corporation. You can see the current ATT&CK® mapping of this project on the <u>ATT&CK® Navigator</u>.

If you are looking for UNIX binaries, please visit gtfobins.github.io.

PayloadsAllTheThings / Methodology and Resources / Windows - Privilege Escalation.md

- EoP Looting for passwords
 - SAM and SYSTEM files
 - LAPS Settings
 - HiveNightmare
 - Search for file contents
 - Search for a file with a certain filename
 - Search the registry for key names and passwords
 - Passwords in unattend.xml

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?

OFFZONE

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

Diebold Decoder	- Building + 1995		0	
31311C3030301C1C1C 2043201C303030303030 1D444930311E414140	31351C3B363237313130 303030303030301C3234 401E3030303030303030303030	303235303130303030303036383D2 303A303F34313A353B313E3E323 303030303030303030303030303030	313234383F1C1C 3F1C1C1C1C3631	444242202 333137313
Paste From Clipboard	Remove Space(s)	ASCII Hex Mode	•	Decode
Consumer Request (Logical Unit Numbe Time Variant Numbe Top-Of-Form Flag = Message Coordinati Track-2 data = ; Track-3 data = Operation Key Buff Dollar/Cents Keybo PIN Buffer = 240A0 Last Transaction S - Last Trx Serial Function command - Retract operatio	31 31) r = 000 r = 1 00 Number = 5 10000068=124 er = DBB C ard Entry = 00000000 F41A5B1EE2F tatus: Number = 1317 Response = (1) Read n = 0 - No retract o	8? 0000 y 9 or B peration occurred		
				About

r	0	d		0	ŧi	in	n
	υ	u	u	L		U	

Function Overview

FF

ONE 2022

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

19

NCR Direct Connect (NDC)

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

🛛 timgabets / ele	ctron-atm	O Watch → 6 ★ Star 27 % Fork 14
↔ Code	Electro Alt: View Window Help	iron ATM
A simple free c	ATM States Screens Fits EMV Cards 0.34 X 4 0 4 B C F F H N 0 2.3 4 D 0.34 X F	R24 5555 Ruffer R Ruffer C FA_6_A 0006666666666666 > 2 2
atm ndc	m	49 50 24 25<
🕞 886 c	 Please select the required service 	00 0.0
Branch: master	F Balance Inquiry D	A 197 21 20 20 27 52 20 24 54 45 54 46 20 20 25 20 50 50 50 252/27 ATH: 100 20 21 20 25 20 25 20 25 43 25 20 31 21 00 20 31 26 50 20 21 20 20 25 20 25 20 25 21 25 20 20 20 20 20 20 20 20 20 20 20 20 20
build/icons	H 3 Account Mini Statement Check Book Request	44 45 50 20 20 85 54 52 4c 4c 41 50 20 52 51 27 55. (TTM00): 217 213 214 8051: Bestage paraset: (processor: classor 11: [990] 11: [990] 11: [990]
fonts	G Card Mini Statement	C [function_identifier]: (200] [restoration_identifier]: (200] [restoration_identifier]: (200]
img settings	F Previous Screen More Services	DecreewLiteratory_specific I: (1999521000,00000775252525353),000097704/4,0000000 Bossaage coordination surface): [r] [outroit_criters.file]: [r]("")"Return card during the Close state"] [period_printer_outs]: []
src tests	430H 25H9 1874 8135 • Head Cerd	BC4+ U558 +806 1942 1C34 55531+ 4800 C918 330E 080+ 0300 1140 +027 0918 +0408+

Overview

This chapter introduces Advance NDC under the following topics:

Introduction to Advance NDC

1-1

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

Confidential and proprietary information of NCR. prised use, reproduction and/or distribution is strictly prohibited.

APTRA Advance NDC, Reference Manual

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

OFFZONE

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

OFFZONE

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	1 c	1c	31	3a	1 c	Зb	34	.`11.002	1:;4
00000011	38															3d	8	=
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	Α.

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

OFFZONE

RCE in third party services

Attack surface:

- Monitoring
- Administration services
- Services on open ports

==					
#	Name	Disclosure Date	Rank	Check	Description
-					
0 mo	auxiliary/admin/smb/ms17_010_command te Windows Command Execution	2017-03-14	normal	No	MS17-010 EternalRomance/EternalSynergy/EternalChampion SMB
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 n	exploit/windows/smb/ms17_010_eternalblue	2017-03-14	average	Yes	MS17-010 EternalBlue SMB Remote Windows Kernel Pool Corrup
4 n	exploit/windows/smb/ms17_010_eternalblue_win8 for Win8+	2017-03-14	average	No	MS17-010 EternalBlue SMB Remote Windows Kernel Pool Corrup
5 mo	exploit/windows/smb/ms17_010_psexec te Windows Code Execution	2017-03-14	normal	Yes	MS17-010 EternalRomance/EternalSynergy/EternalChampion SMB

<u>msf5</u> >

msf5 > search ms17-010

BURPSUITE 2.0

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.

Proactively defend your Personas ATMs

Most security patches only address known current attacks, but threast from criminals continue to explice. NCR Personal Depender Encryption Solution is designed to not only limit the success from the attacks identified in the market today – but also to provide a functional enhancement to the Personal ATM to reduce the risk of modified versions of attacks in the future.

Protect your Personae ATMs from "black hox" attacks Criminal attacks on ATMs have become more sophisticated and now include attempts to bypass the ATMs core PC processor and connect unauthorized electronic devices to the cash idspension. The NCR Personas Dispenser Encryption Solution protectively protects your Personas ATM from this type of "black hos" attack.

Bring more enhanced security functionality to your Personas ATMs

NCR has continued to invest in security enhancements. Recognizing the roked for our customers to protect their self-service channel, RCR is note able to offer customers with Persons ARMs an upportunity to provide similar levels of incidem encryption technology.

For index information, whit www.httattr, or errort formelablent/cost

Thank you!

