Trust No One
ATMs and their dirty little secrets

Olga Kochetova, Alexey Osipov
Kaspersky Lab
root@root:~# whoami

Penetration Testing Department, Kaspersky Lab
> @_Endless_Quest_, @GiftsUngiven
> ATM/POS security assessment
> Penetration Testing
> Forensic Investigation
Speakers at many IT events
Authors of multiple articles, researches and advisories
Lego for adults
About hardware
About soft

Host (computer)

- MS Windows
- GUI and device control
- Antivirus/Integrity control software
- Video surveillance
- Radmin/TeamViewer and other crap

Devices

- Some microcontrollers with RTOS
How it works?

- Windows-based app
- XFS Manager
  - XFS APIs
    - WFSRegister
    - WFSEOpen
    - WFSEExecute
  - XFS SPIs
    - WFPRegister
    - WFPOpen
    - WFPExecute
- Service Providers
- Windows OS
- ATM
- Network
- Processing center
- Hardware units
Are you kidding me?
WHAT IS IT INSIDE?
NETWORK
ATM network
Wired communication

- Types
  - X.25
  - Ethernet
Wireless communication
Attacks through GSM/GPRS modems

- CDMA
- GPRS/EDGE
- UMTS/3G/LTE

Over-the-air encryption
- CDMA – commercially available tools for interception
- GSM – broken
- UMTS/3G/LTE – state of the art solutions

BHUSA 2010 by Karsten Nohl
BHUSA 2015 by Alexey Osipov & Alexander Zaitsev
VPN. What VPN?

Types
- Software
- Hardware
- Not used

Software
- OS internal
- Third-party

Hardware
- Outside of ATM
- Inside of ATM
VPN. Hardware

▶ Pros
▶ Built-in firewall
▶ Works regardless of host computer
▶ It’s peace of metal/plastic, you can grab it with hand
VPN. Hardware

Pros
- Built-in firewall
- Works regardless of host computer
- It’s peace of metal/plastic, you can grab it with hand

Cons
- Doesn’t protect against physical access
- Works regardless of host computer
- It’s peace of metal/plastic, you can grab it with hand
VPN. Software

Pros
- Cheaper
- Easier to deploy
- Doesn’t degrade with age
VPN. Software

Pros
- Cheaper
- Easier to deploy
- Doesn’t degrade with age

Cons
- With access to OS can be disabled
- Not always provide firewallsing functionality
- If VPN-connection is interrupted it is common, that all data from this moment will be transmitted in clear-text
Deadly sins of ATM network organization

- Software VPN without firewall protection
- Hardware VPN without physical security
- Wireless communications without application level encryption
- Lack of knowledge about real issues and advantages of used devices and software
HOW TO BREAK
Let me in:
There are no ATMs in the internet (c)
Unprotected networks

Service Providers

Windows-based app

XFS Manager

Windows OS

ATM

Hardware units

Processing center

Network
How it works: processing center emulators

Processing center

Network

Host Simulator

- Go In Service
- Go out of Service
- Select Message
- Send Message
- Force download
- Load IN File
- Toggle ONLINE/OFFLINE

XFS Manager

- XFS APIs
- XFS SPIs

- WFPRegister
- WFPOpen
- WFPExecute

Windows OS

ATM

Service Providers

Hardware units
How it works: rogue processing center

- Windows-based app
- XFS Manager
- XFS APIs
  - WFSRegister
  - WFSOpen
  - WFSExecute
- XFS SPIs
  - WFPRegister
  - WFPOpen
  - WFPExecute

Hardware units

Network

Processing center
Rogue processing center
## Direct connect protocols - overview

- **Stages**
- **Customization data**
- **Go in/out service**
- **Get abnormal statuses**
- **Transaction response**
Direct connect protocols - security

- Internal security mechanisms
- SSL/TLS
- MAC protection
Direct connect protocols - Internal security mechanisms

- SSL/TLS – haven’t seen
- MAC protection is complex
  - Multiple choices not protect some packets
  - Don’t check MAC on packet that configures MAC
  - Add MAC but don’t check
  - Server and client have different configurations
ATM Network
Network, that can be managed more easily
One for all…
... and all for one
THIS VIDEO IS A PROOF-OF-CONCEPT OF AN ATTACK AGAINST AN ATM NETWORK VIA A COMPROMISED MACHINE.
WHO’S THERE?
How to get in

Who buys these ATM keys? Tell locksmith the code and get it cut. Totally unrelated: why is it "Top selling product"?
But should we?
HARDWARE – BLACK BOX
Common tale: No money and no logs

Translation: There is NO money for a long time!!!
Shoebox wizardry
Black box
How it works: black box

Windows-based app

XFS Manager
- XFS APIs: WFSRegister, WFOpen, WFSExecute
- XFS SPIs: WFRegister, WFOpen, WFEExecute

Windows OS

ATM

Hardware units

Network

Processing center
Skimmer inside

Sensitive information disclosure
  Track2 from magstripe
  Transaction history from EMV-chip
Atm jackpotting via black box
Advantages Of COM/USB

• Direct device control
• Execution of undocumented functions
• Intercept unmasked sensitive data
• Possibility of producing hardware sniffer, which can’t be detected by visual examination

https://www.youtube.com/watch?v=ZyuohKnTH9s
TRUST ZONE
Trust zone in theory

➢ Trust no one
➢ Encrypt everything and on all levels
➢ Check MAC then decrypt
Trust zone in practice

- Everyone trusts everyone
  - ATMs sees their neighbors
  - USB communications considered secure and uninterceptable
  - The same goes for wireless communications
- Encryption increases costs and often disabled, VPN considered as silver bullet
- MAC doesn’t provide secrecy
It’s dangerous to go alone
Banks: What to do?

- Enable, finally, all security options according to vendor’s best practices
- Force vendor to fix vulnerabilities
- PCI DSS compliance doesn’t guarantee security
- Proactive analysis of security issues is better than forensics
Banks: What to do?

- Enable, finally, all security options according to vendor’s best practices
- Force vendor to fix vulnerabilities
- PCI DSS compliance doesn’t guarantee security
- Proactive analysis of security issues is better than forensics
Banks: What to do?

- Enable, finally, all security options according to vendor’s best practices
- Force vendor to fix vulnerabilities
- PCI DSS compliance doesn’t guarantee security
- Proactive analysis of security issues is better than forensics
Banks: What to do?

▷ Enable, finally, all security options according to vendor’s best practices
▷ Force vendor to fix vulnerabilities
▷ PCI DSS compliance doesn’t guarantee security
▷ Proactive analysis of security issues is better than forensics
Banks: What to do?

I’m watching you...
Keep calm and have a plan B
Kudos

- Alexander Tlyapov @_Rigmar_
- Artem Kondratenko @artkond
- Alexander Zaytsev @arbitrarycode
- And all other folks
HAVE FUN! STAY SAFE!

Olga Kochetova, Olga.Kochetova@kaspersky.com, @_Endless_Quest_
Alexey Osipov, Alexey.Osipov@kaspersky.com, @GiftsUngiven