Revisiting ATM vulnerabilities for our fun and vendor's profit

Alexey Osipov & Olga Kochetova

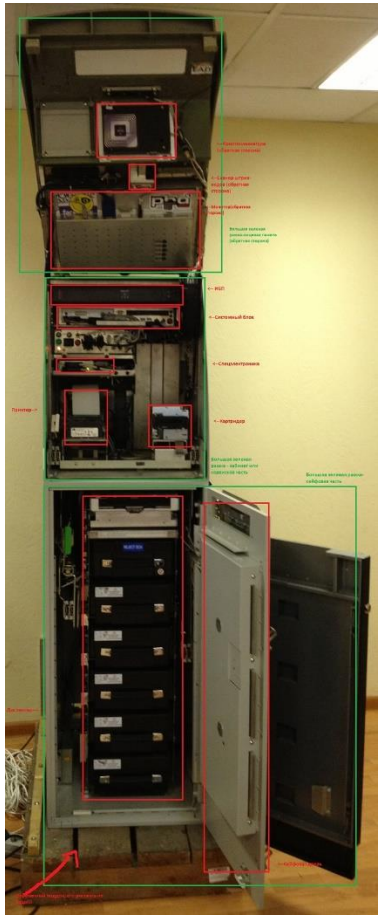
Experts@Security:~# WhoAmI

- Positive Hack Days Team
- Speakers at many IT events
- Pentesters of various systems
- Authors of multiple articles, researches, advisories

Agenda

- Overview
- What makes us roll
- Short stories
- Vendors losses
- Our frustration
- Conclusions

ATM (front view)



Hack in Paris

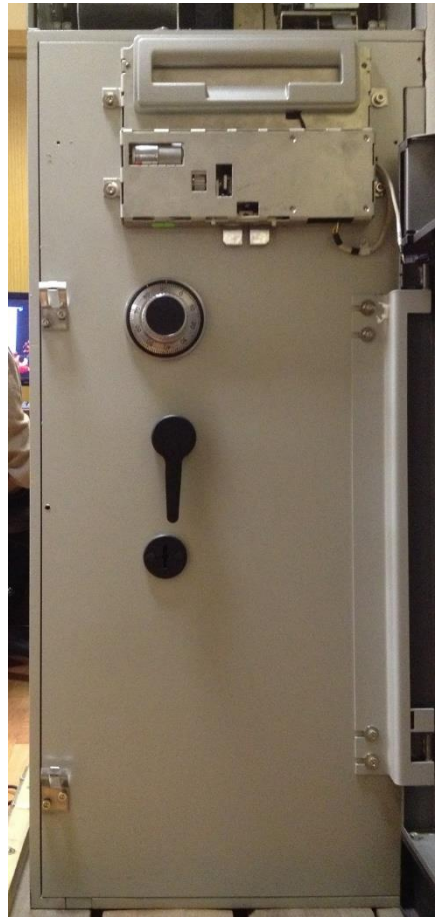
5th edition

ATM Cabinet

Hack in Paris

5th edition

ATM Safe (outside)



ATM Safe (inside)

Software Stack

Host

- MS Windows
- Device control middleware and kiosk
- Some AV/integrity control
- Video surveillance/Radmin/Old flash player and other crap

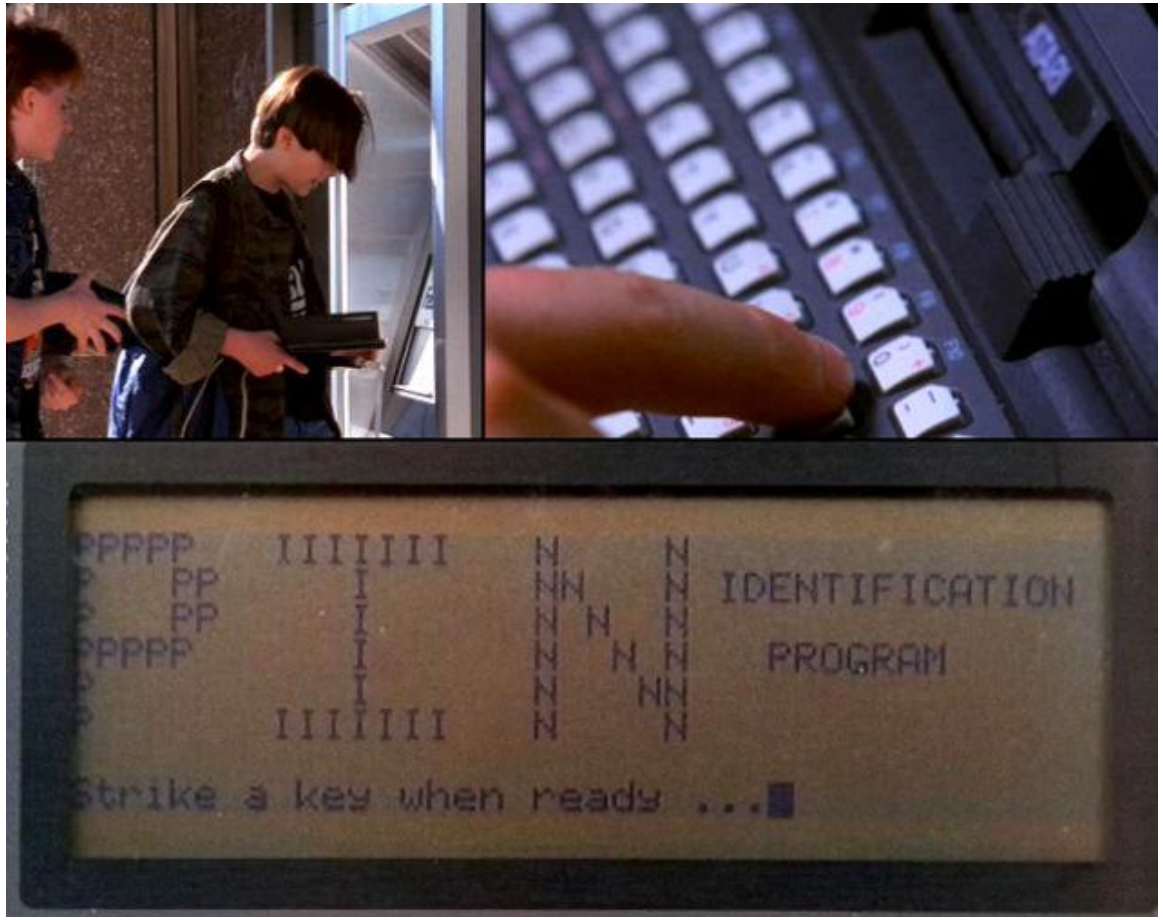
Devices

- RTOS on strange microcontrollers

Windows XP Still Alive

- Early 2014 – 95% of ATMs run on Windows XP
- Support killed off in April 2014
- >9000 vulnerabilities

Rob The Bank



BOOOoooring

Hack in Paris

5th edition

Alternative News

Criminals Hit the ATM Jackpot

Created: 11 Oct 2013 23:05:17 GMT • Updated: 23 Jan 2014 18:03:50 GMT

Daniel Rega

The Hacker News™
Security in a serious way

Tyupkin Malware Hacking ATM Machines Worldwide

Exploiting ATMs: a quick overview of recent hacks

2012-08-10 by lucaskauffman. 12 comments

nakedsecurity
Award-winning news, opinion, advice and research from SOPHOS

malware mac facebook android vulnerability data loss privacy more...

◀ Your PIN or your life! Is there malware lurking in your AT

Credit card skimming malware targeting ATMs

Jackpotting makes its way to Western Europe's ATMs

4

Oct. 16, 2014 | by Suzanne Cluckey

SOFTPEDIA DESKTOP MOBILE WEB NEWS

Softpedia › News › Security › Virus alerts

Skimmer Trojan Targets ATMs Made by One of the World's Largest Manufacturers

Hack in Paris

5th edition

“Average Bill”

Typical ATM contains **4** cassettes
with **~2500** notes in each one.

(5+10+20+50)x2500= US$/€ 212 500

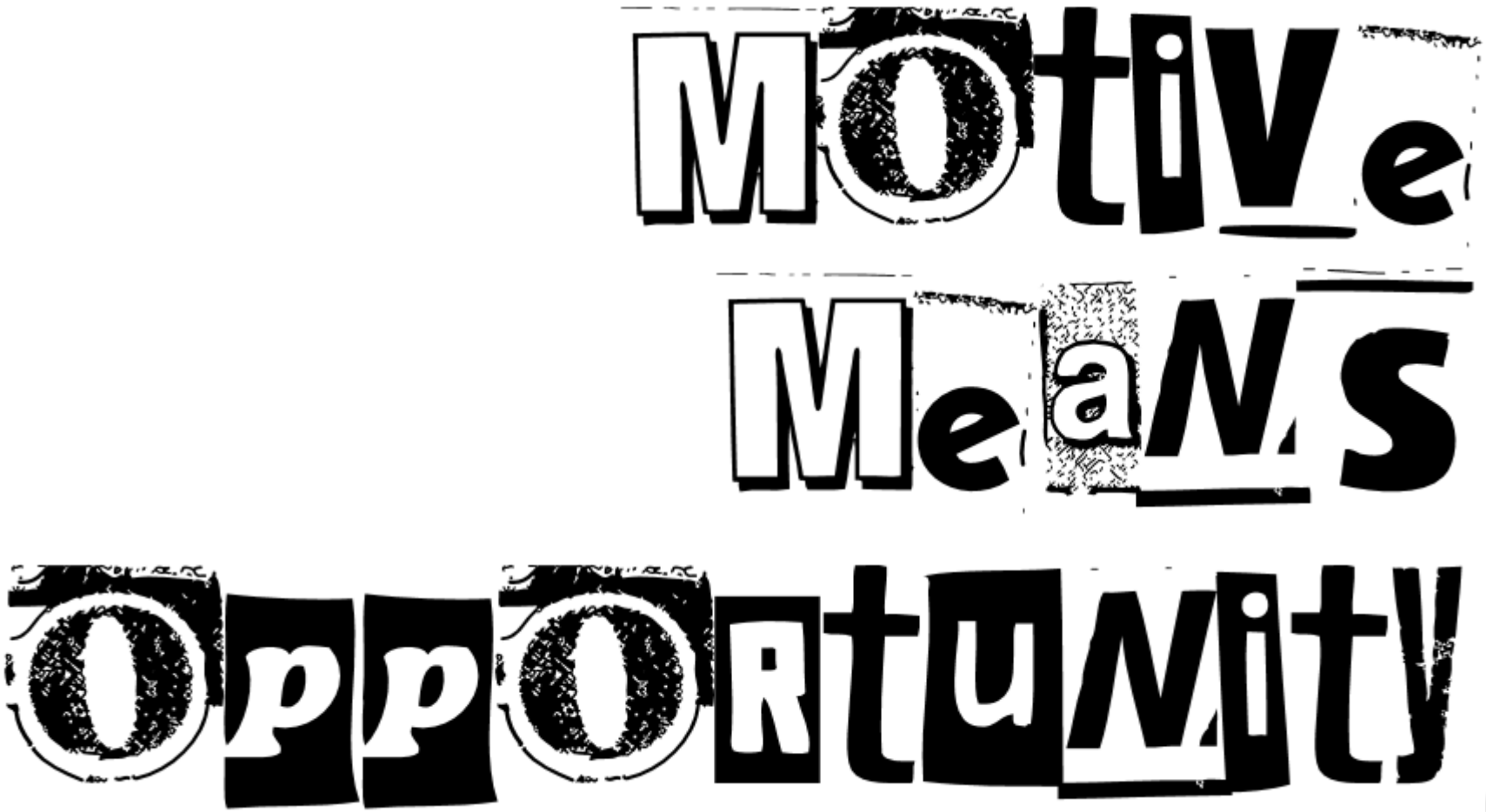
could be stolen from ATM
during single incident.

DO NOT REPEAT IT AT HOME

Hack in Paris

5th edition

Main Parts Of Everything

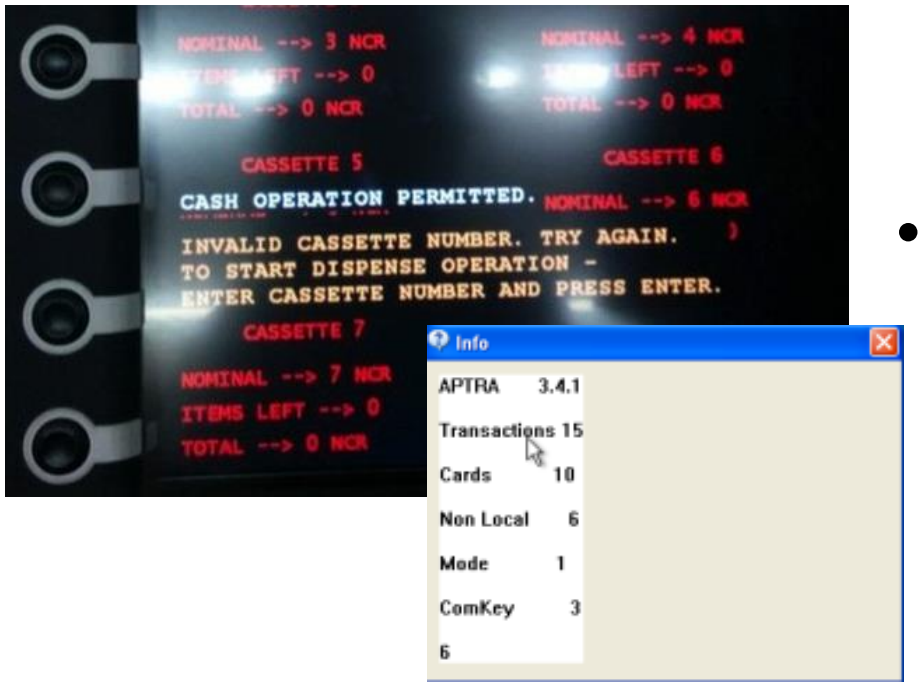


Hack in Paris

5th edition

True Story #1

Malware



- Skimer.A -2008
- .....
- Backdoor.Ploutus – 2013-2014
- Backdoor.Padpin – 2014
- Macau Malware – 2014
- Backdoor.Tyupkin – 2014
- Trojan.Skimmer (new) – 2015

Subtotal = 16 < variants of malware

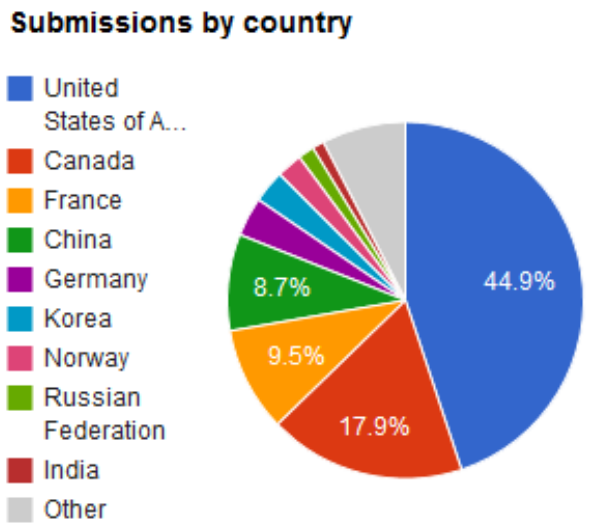
Hack in Paris

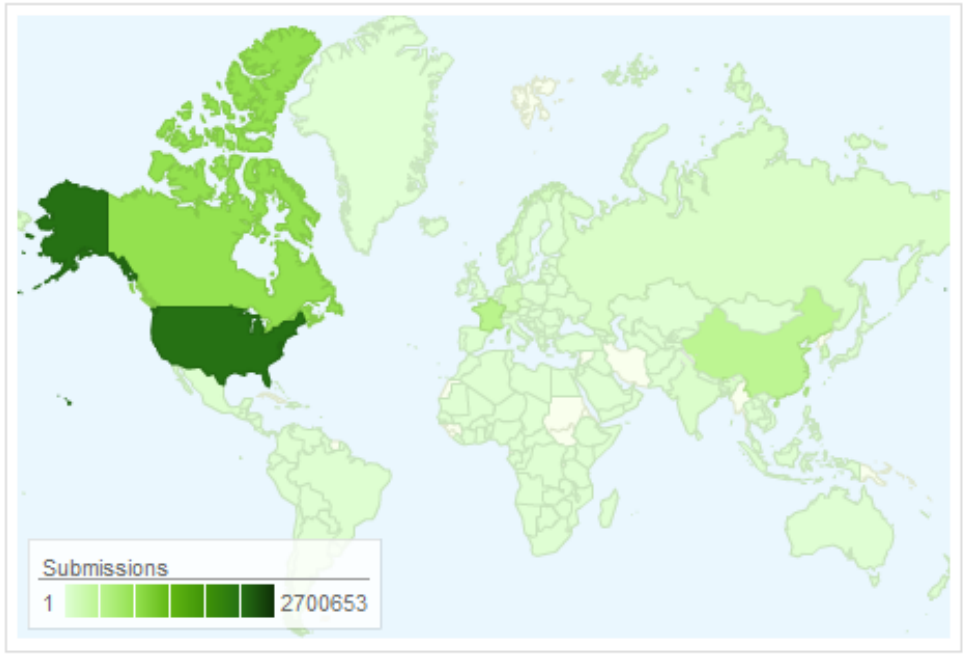
5th edition

Tyupkin: Around The World In 435 Days

virustotal

File statistics during last 7 days





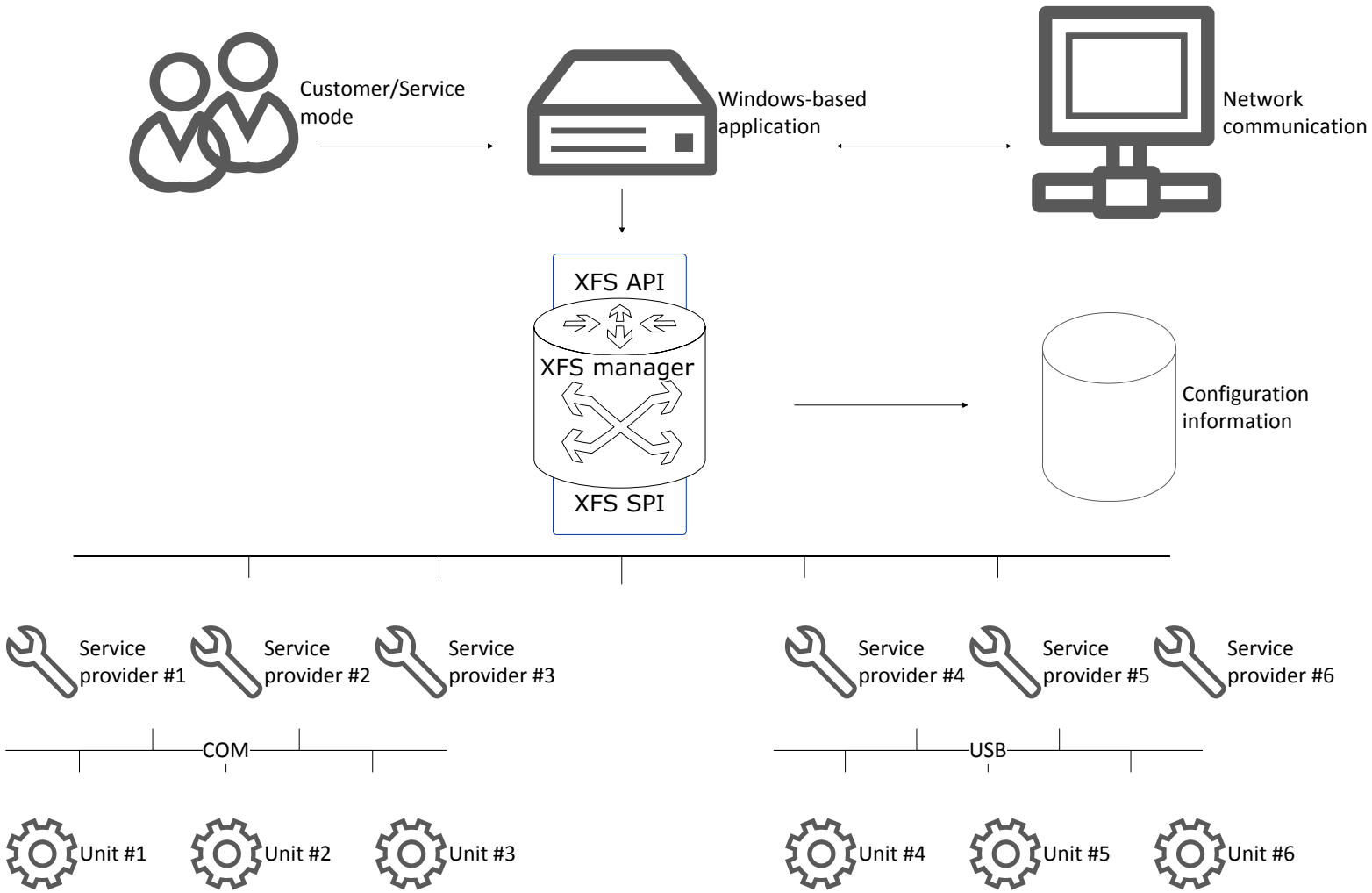
Hack in Paris

5th edition

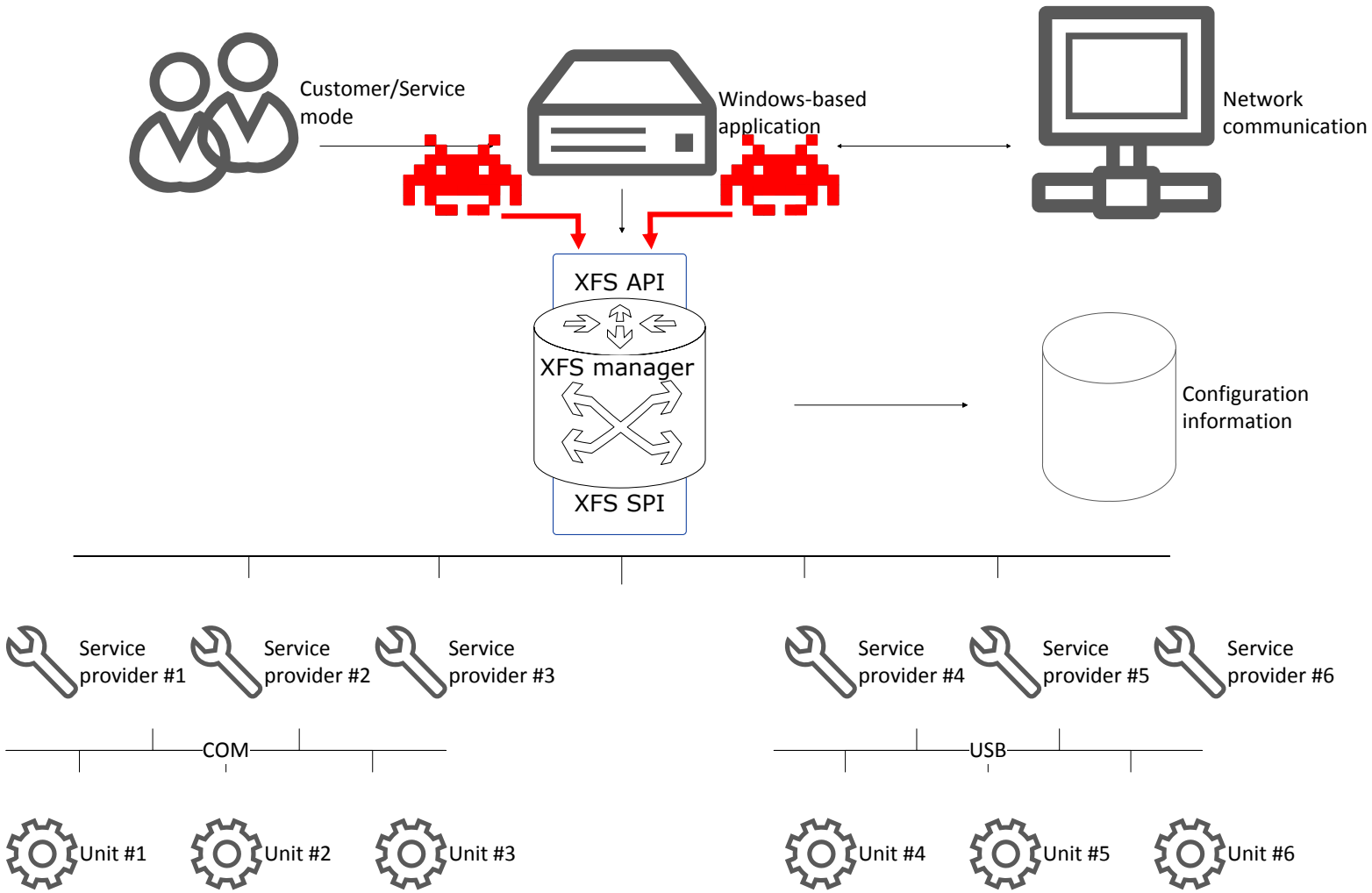
How It Works: Jackpotting Malware

- Access
- Infection
- Control
- Theft

How It Works: XFS



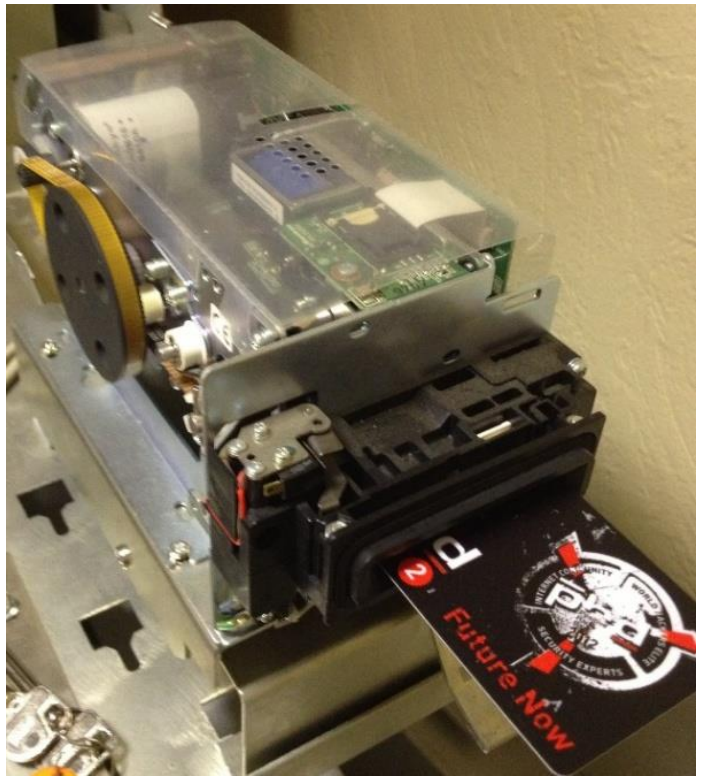
How It Really Works: XFS Insecurity



XFS, Cash Dispenser Device

- Cash withdrawal without authorization
- Cassette and cash control
- Software safe opening

XFS, Identification Card Device



- Insert/eject/retain cards
- Read/write data
- EMV reader (one can access payment history stored in chip)

XFS, PIN Keypad Device

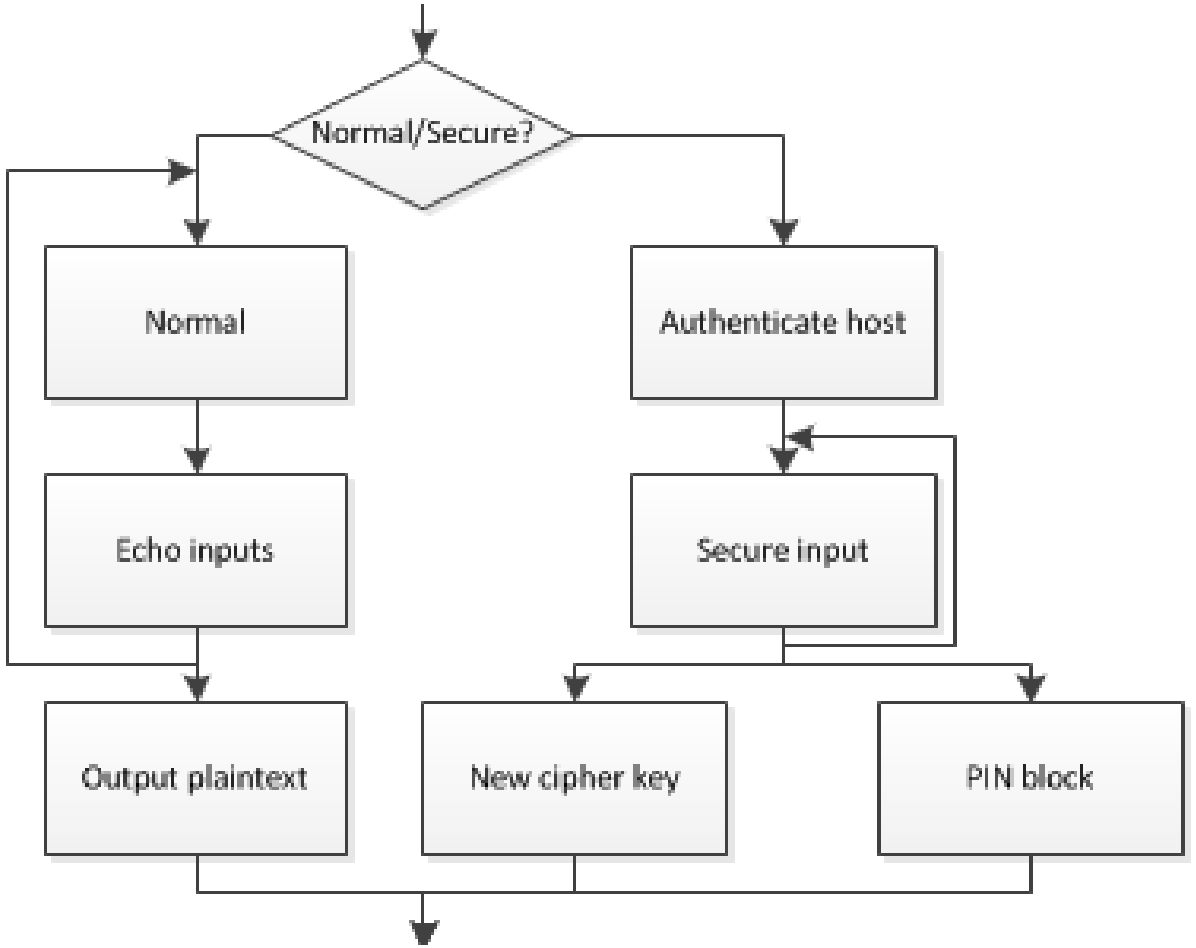
- Export of the key is not available
- Open mode and secure mode read data

(for stealing PIN: an ATM software sets “secure mode” for entering PIN, and intruder changes it to “open mode” to capture the PIN)

Hack in Paris

5th edition

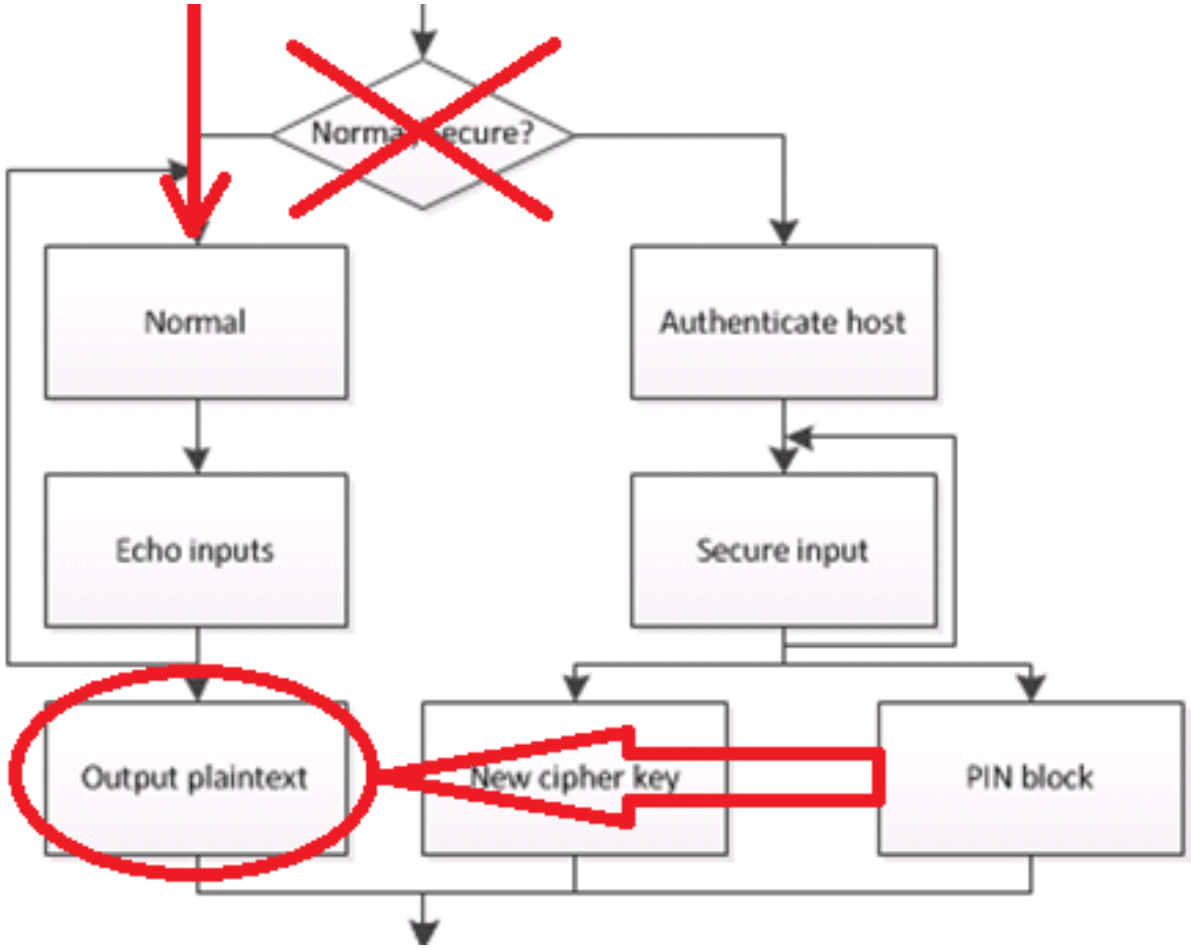
PIN Device Flow



PIN Device Flow

- If entering PIN/encryption keys
  - Authenticate host on currently used keys
  - Send empty button press events
  - Send PIN block to host
- If entering open string
  - Send all button press events with button values to host

PIN MITM Attack



PIN Device MITM Attacks

- Request open mode from PIN pad when user is going to insert PIN code
  - Acknowledge host about button presses
  - Send erroneous PIN block (we don't know keys)
    - Host refuses transaction, but attacker knows client PIN code
- Next transaction will be unmodified

XFS Authentication

- Authentication?

- Exclusive access to XFS manager/service provider?

XFS Authentication

- Authentication? What authentication?
- Exclusive access to XFS manager/service provider?

Exists, but not intended to be used for security

XFS specification

- Where?

XFS specification

- Where?
- "We don't know yet" (c)

but try google "XFS ATM"

True Story #2

06 Thieves Jackpot ATMs With 'Black Box' Attack

JAN 15

Previous stories on KrebsOnSecurity about ATM skimming attacks have focused on innovative fraud devices made to attach to the outside of compromised ATMs. Security experts are now warning about the emergence of a new class of skimming scams aimed at draining ATM cash deposits via a novel and complex attack.

At issue is a form of ATM fraud known as a "black box" attack. In a black box assault, the crooks gain physical access to the top of the cash machine. From there, the attackers are able to disconnect the ATM's cash dispenser from the "core" (the computer and brains of the device), and then connect their own computer that can be used to issue commands forcing the dispenser to spit out cash.

In this particular attack, the thieves included an additional step: They plugged into the controller a USB-based circuit board that NCR believes was designed to fool the ATM's core into thinking it was still connected to the cash dispenser.

The attackers responsible for this "black box" ATM hack relied on a mobile device and a USB-based circuit board.

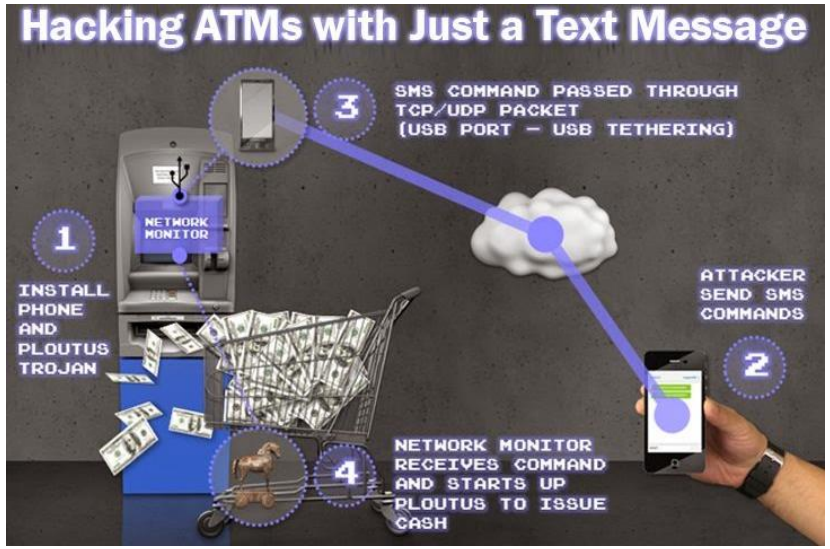
Hack in Paris

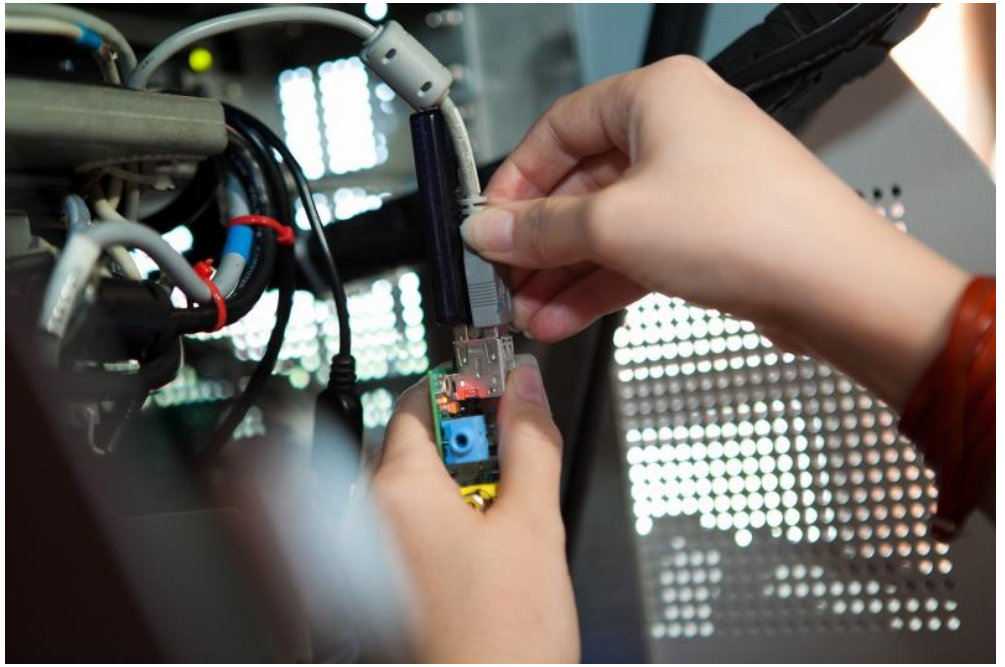
5th edition

http://krebsonsecurity.com/2015/01/thieves-jackpot-atms-with-black-box-attack/

Black Box Attacks

- Directly control ATM

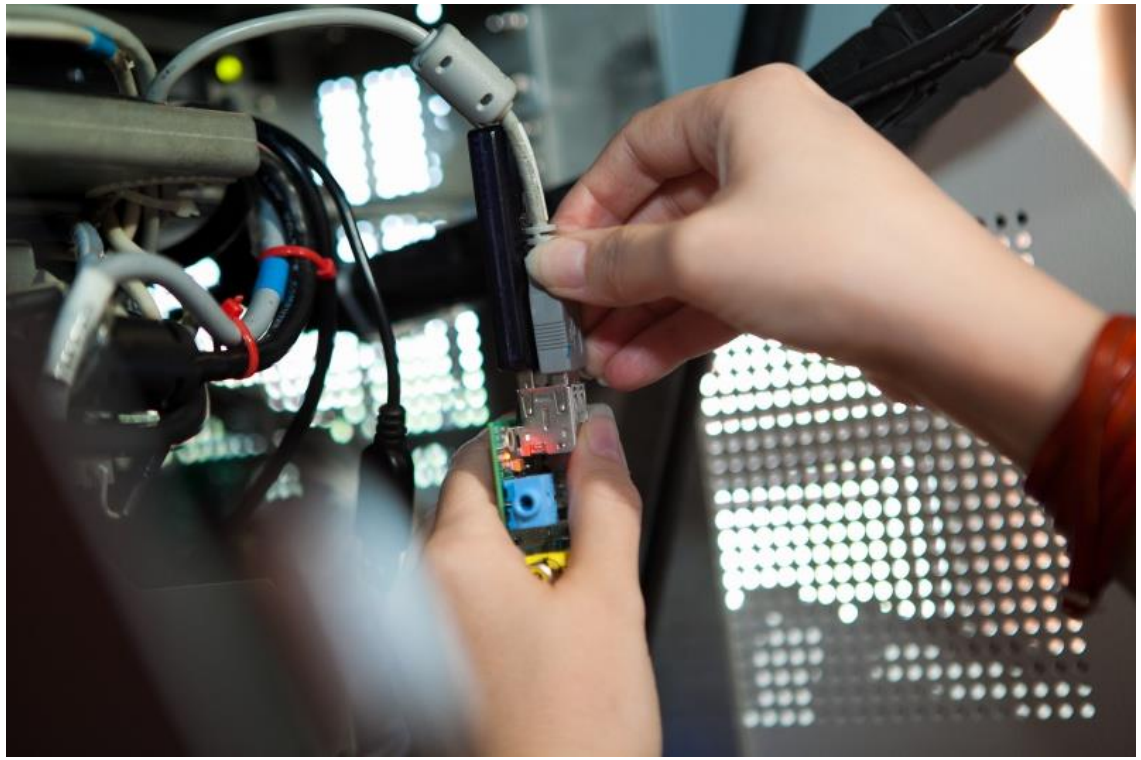




Hack in Paris

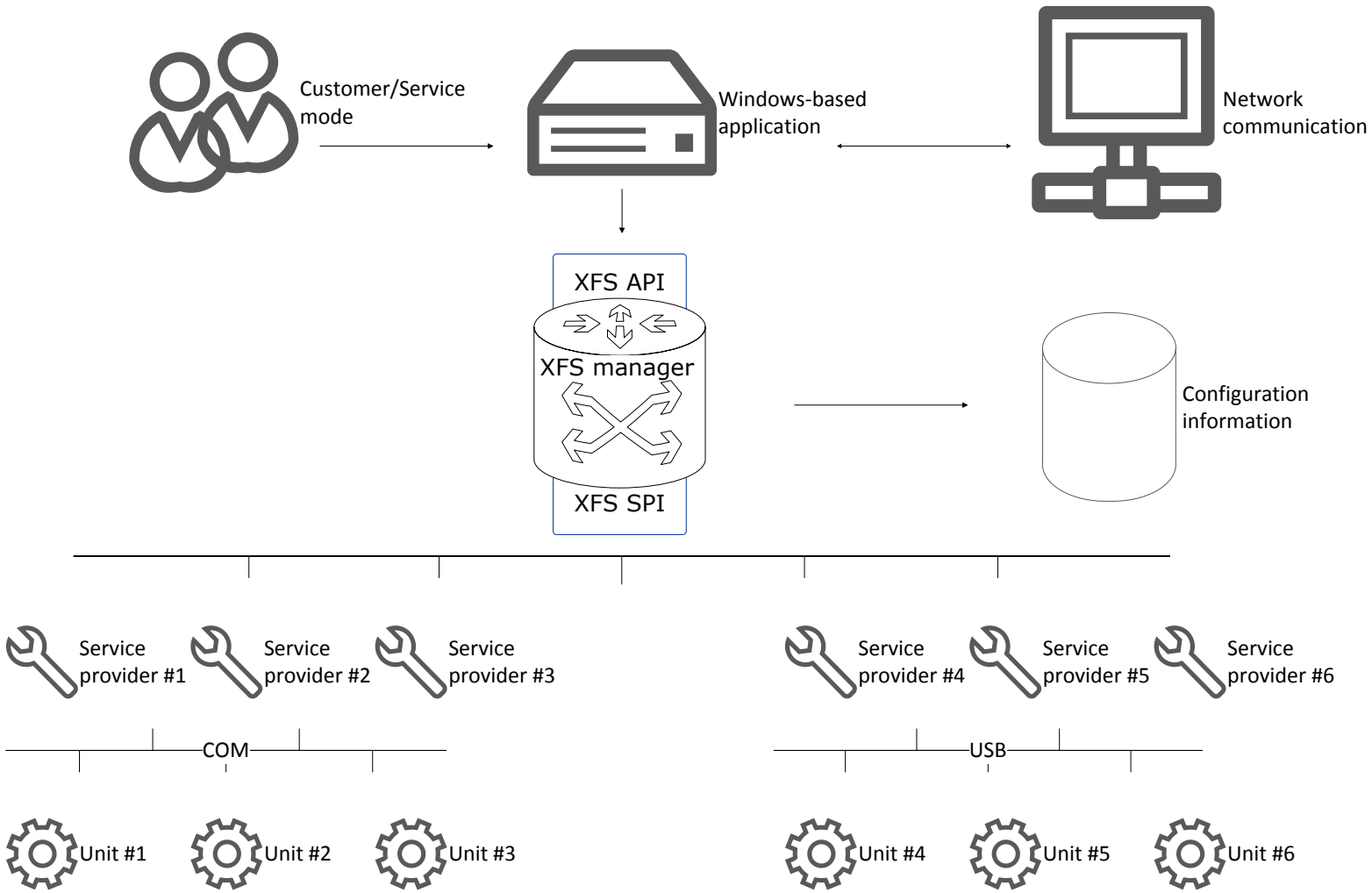
5th edition

How It Works: Black Box Attacks

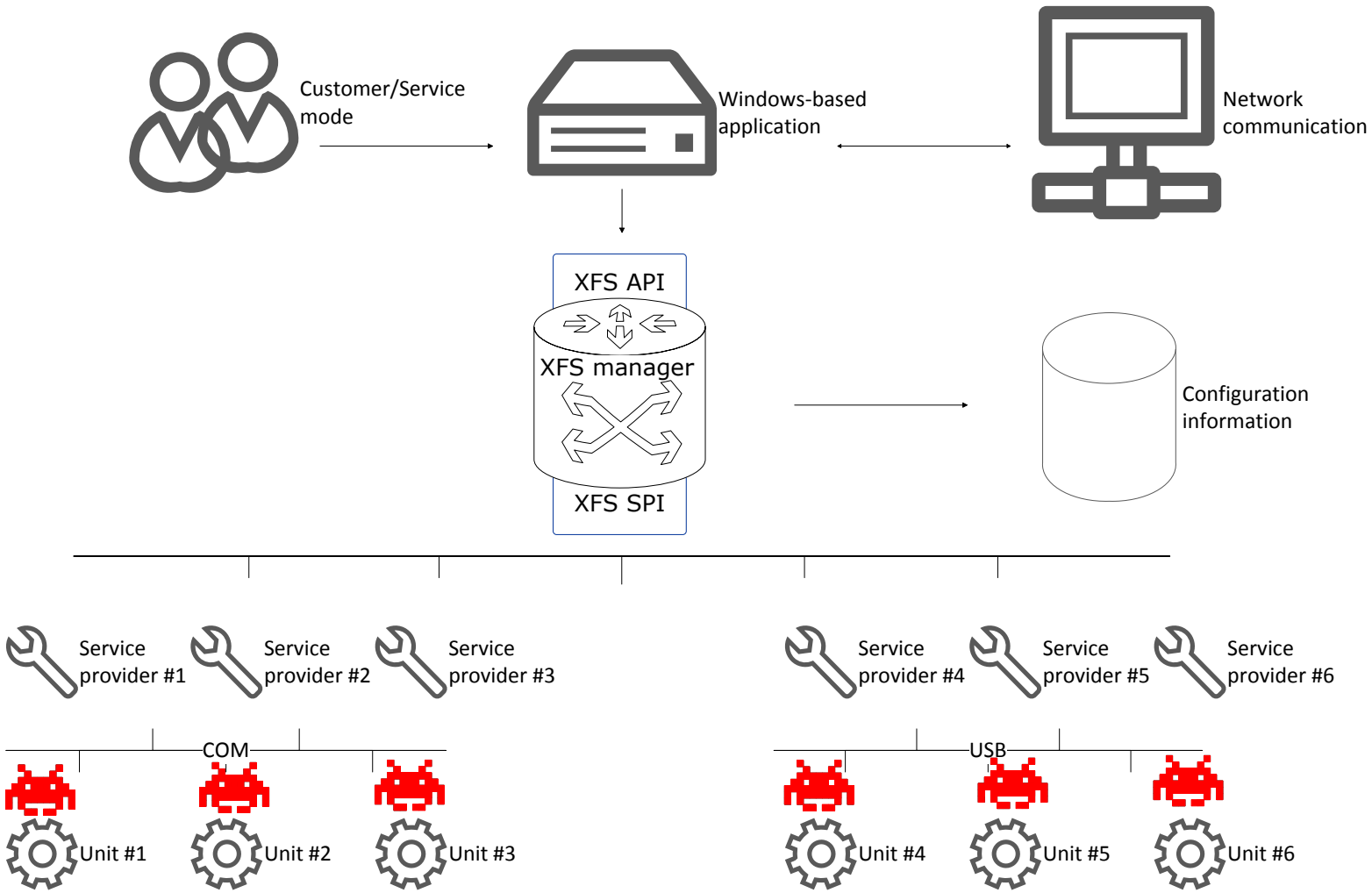


- Dispenser
- Card reader
- Encrypted PIN-pad
- Sensors

How It Works: Physical Interfaces COM/USB



How It Really Works: COM/USB Insecurity



Hack in Paris

5th edition

DinosauRS232

- Standard interface
- No specific drivers
- No authorization
- Insecure proprietary protocols (just sniff and replay)

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

Advantages Of COM/USB

- Direct device control
- Command execution mitigating all host-based checks, e.g. cash withdrawal without notes counter checks

01.09.2014 14:16:17.90164 (+0.0000 seconds)

02 30 [redacted] 01 01 02 00 03 00 04 00 05 00 06 00 10 03 42

01.09.2014 14:16:17.91764 (+0.0156 seconds)

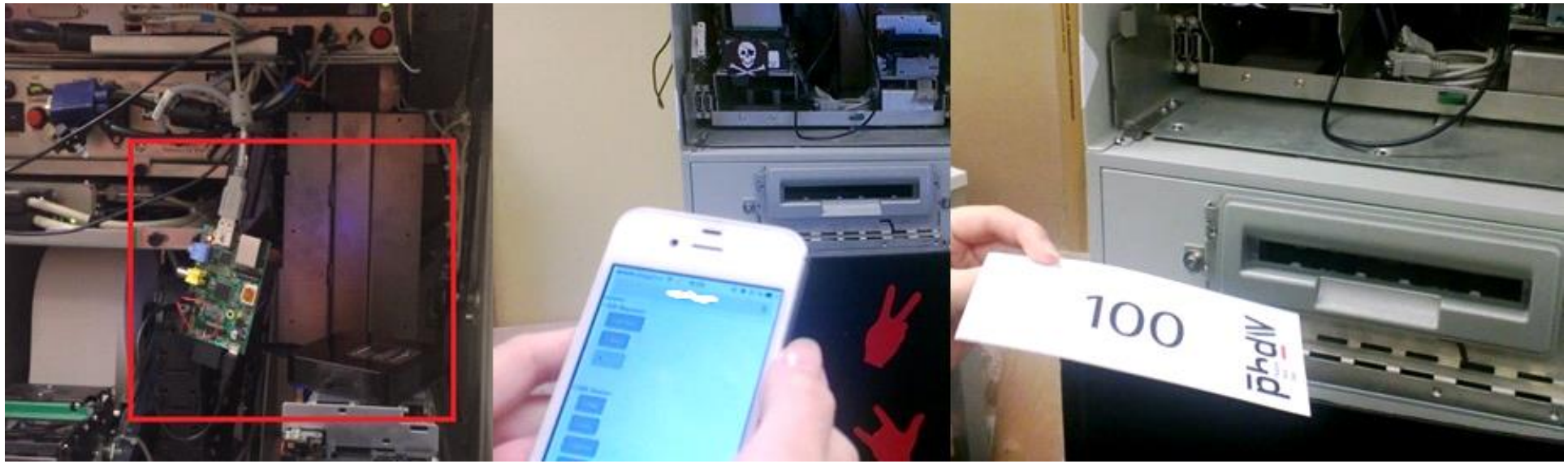
02 30 06 20 10 03 07

- 02 30 / 10 03 – start-stop sentinels
- XX XX– op-code
- XX – Unknown
- 01 01 … – data
- 42 – CRC8

Hack in Paris

5th edition

We Had Two Libs Of Python, 35 USD, Power Bank And Wi-Fi Dongle



RS232 vs USB-HID

ls /dev/tty*

import serial

ser = serial.Serial('/dev/ttyUSB0')

ser.write("**0230XXXXXX010102000300040005000600100342**“.decode(‘hex’))

ser.close()

lsusb

import hid

h = hid.device(0x????, 0x20)

h.write([0x80] + map(ord, "**0230XXXXXX010102000300040005000600100342**“.decode(‘hex’)))

h.close()

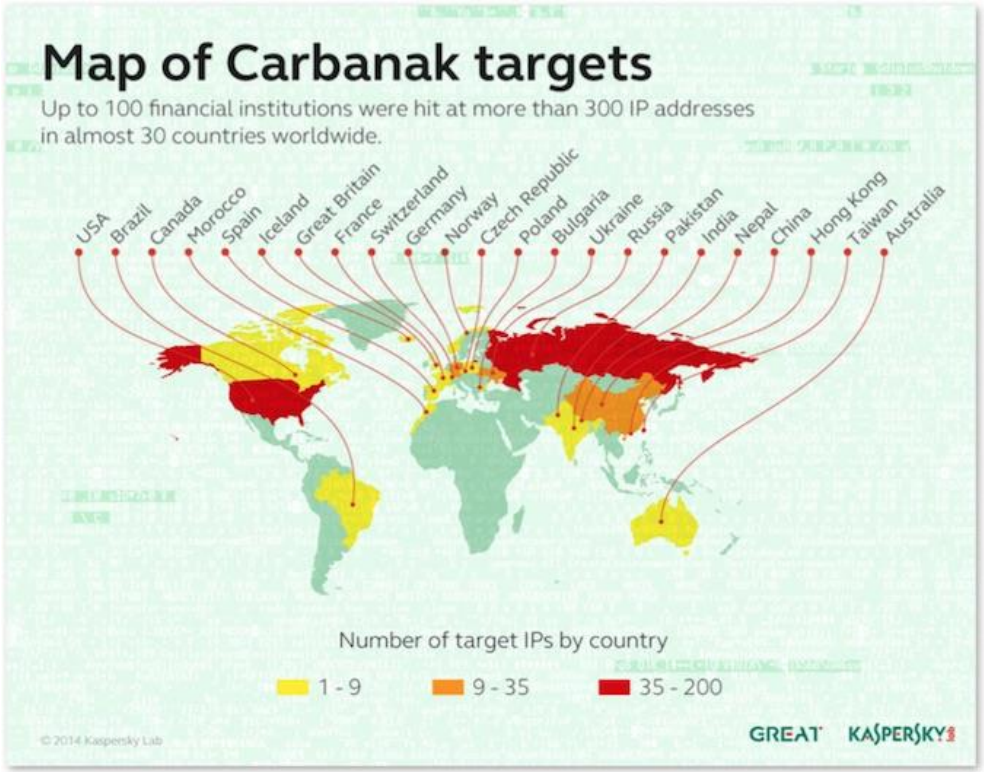
Demo

https://youtu.be/4TXnIcjn1xc

True Story #3

Hijacking ATM Control/Processing Host

- Carbanac – 2015
- MitM – 2015



Hack in Paris

5th edition

Possible connections to processing center

- VPN (Hardware/Software)
- SSL
- MAC-authentication
- Firewall
- IDS

ATMs In Internet

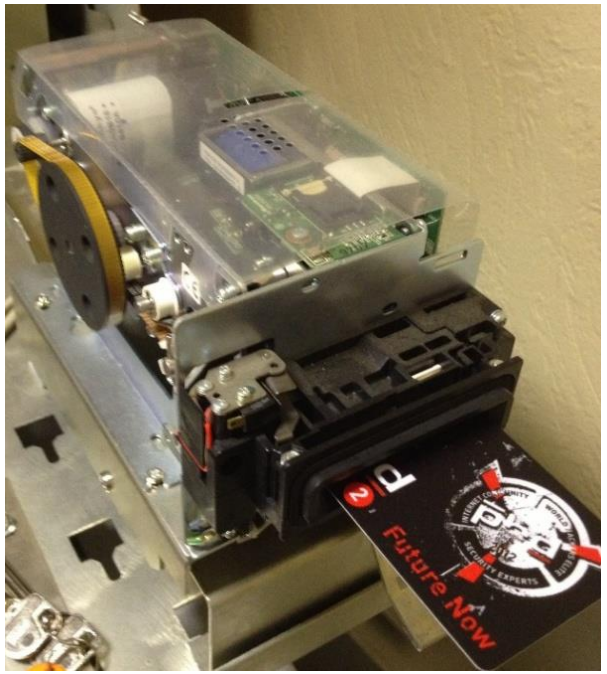
Pakistan	1458
Russia	571
Venezuela	28
Tajikistan	20
Ukraine	16
Armenia	11
Brazil	1
Zambia	1
Sierra-Leone	1
Thailand	1

Hack in Paris

5th edition

Who Cares

Card Reader/ Writer/ Skimmer



Sensitive data disclosure, e.g. track data in plaintext, is possible with reading command sending to COM/USB port directly. This attack is possible with ATM's computer or with any external device, which is connected to the card reader's COM/USB port.

Hack in Paris

5th edition

What Big Vendors Think

The vulnerabilities are essentially normal specifications of the card readers and not unexpected. As long as the ATM is running within normal parameters, these problems cannot possibly occur.(c)

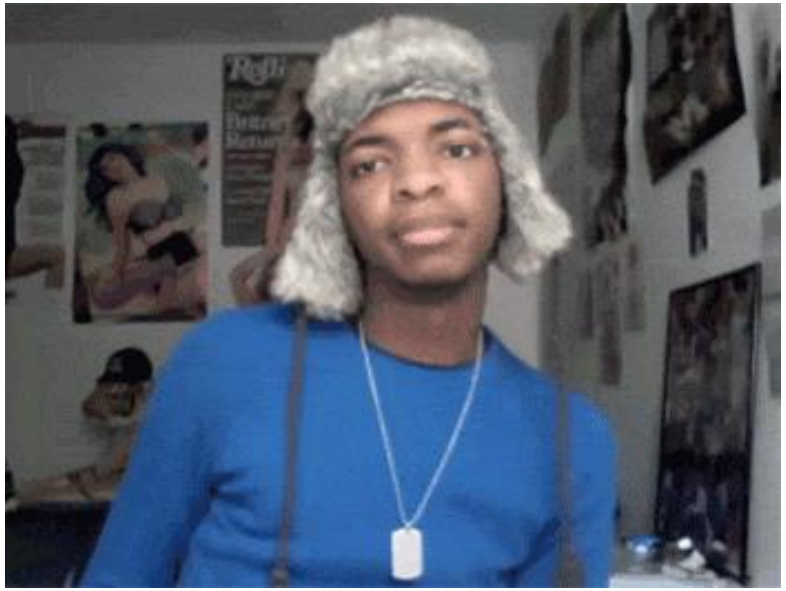
However this vulnerability is inherent in the USB technology and is expected be mitigated by the use of appropriate physical controls on access to the ATM top box.(c)

Quick Cash And Full Control

Control cash dispenser module by unauthorized application or user. An attacker has possibility to control cash dispenser by sending command to COM/USB port directly, including dispensing and presenting commands. This attack is possible with ATM's computer or with any external device, which is connected to the dispenser's COM/USB port.

What Big Vendors Think

"We regret informing you that we had decided to stop producing this model more than 3 years ago and warranties for our distributors been expired."



Hack in Paris

5th edition

What About Cryptography

Dispenser **“Half”** Security Level:
Any use of cryptography – is NOT equal to good use of cryptography

Achievement Unlocked

Dispenser **High** Security Level: Dispenser Upgrade Pack is released and available from the vendor_name download center, and it will be included as standard in the next release of XFS.(c)

Hack in Paris

5th edition

No More SSL

- OpenSSL in ATM/POS software
- Misconfiguration
- PCI/PA DSS v.3.1

SSL >> TLS

Hack in Paris

5th edition

How Live With All This

Conclusions

- Current vulnerabilities in ATMs are low hanging fruits, that are ready for criminals
- Vendors are not that interested in fixing. Increase cost, decrease profit
- Banks are not that competent to know what to do

Proposals

- Implement mutual authentication both for ATM computer and it's devices
- Make peer review of XFS standard/communication protocols
- Authenticated dispense from processing center
- Trust environment is not about ATMs
- Implement regular security assessments and pentest of ATMs

Kudos

Alexander Tlyapov, @_Rigmar_

And all other guys worth mentioning

Questions?

Alexey Osipov
@GiftsUngiven, GiftsUngiv3n@gmail.com
Olga Kochetova
@_Endless_Quest_, Olga.v.Kochetova@gmail.com