A history of ATM violence

From blowing up safes over jackpotting to all-round malware

Erik Van Buggenhout & Daan Raman
OWASP Chapter Meeting - May 2014
Who are we?

Penetration testers

Certification lovers

Instructor
SEC 560 & 542

NVISO ApkScan
Topics for tonight

- Introduction
- Attacking the ATM
- Common ATM system design
- Assessing a sample ATM
- Conclusion
Topics for tonight

- 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 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 than 2.2 million ATM’s worldwide.
ATM?

The ATM is a “stupid” device, part of the bank’s overall architecture.
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 computer
2. (Touch)screen
3. Card-reader
4. PIN pad
5. Cash dispenser
6. Cash cassettes
ATM?

1. ATM computer
2. Touchscreen
3. Card reader
4. PIN pad
5. Cash dispenser
6. Cash cassettes
ATM?

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

- Disk bays
- CD / DVD
- Auxiliary ports
- USB
Topics for tonight

- 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
- 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...
How to attack the ATM?

Blow up the safe

Copy cards & steal PIN codes

Steal the entire thing...
How to attack the ATM?

Copy cards & steal PIN codes

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.

Skimming off the top
Why America has such a high rate of payment-card fraud
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

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

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

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 the OS

- Attack back-end communication
- Access "operator" mode

---

**ATM malware Ploutus updated with English-language version**

Adam Greenberg, Reporter

October 28, 2013

---

**Texting ATMs for Cash Shows Cybercriminals’ Increasing Sophistication**


---

**Cash machines raided with infected USB sticks**

By Chris Vallance

BBC Radio 4
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?

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 on the Internet
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

CCC 2013
"Electronic bank robberies"
Boot ATMs from USB
Topics for tonight

- Introduction
- Attacking the ATM
- Common ATM system design
- Assessing a sample ATM
- Conclusion
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 (eXtensions for Financial Services) provides a standard set of APIs that can be used by Windows applications to operate the ATM peripherals.
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)

- We will only change from Windows XP when we absolutely have to change. 23%
- We will need to begin migrating to Windows 7 or 8 now or within the next two years. 30%
- We would like to have the choice of running a non-Microsoft operating system (e.g., Linux). 9%
- No opinion 18%
- Other 1%
Topics for tonight

- Introduction
- Attacking the ATM
- Common ATM system design
- Assessing a sample ATM
- Conclusion
Where to start?

Big Time Deals!
Big Time Savings!

FEBRUARY PACKAGE
G2505
View more details

ALWAYS THE MONEY

BUY NOW >

THE ATM STORE

OPEN 24 HOURS
Where to start?
ATM delivery 101
ATM delivery 101
Let’s get started
Physical access?
Physical access?
Physical access?
Physical access?
Physical access?
Physical access?
Running the ATM

- AMIBIOS
  - Version: 08.00.15
  - Build Date: 05/18/09
  - ID: 0ABKJ056

- Processor
  - Intel(R) Core(TM)2 Duo CPU E6400 @ 2.13GHz
  - Speed: 2133MHz
  - Count: 1

- System Memory
  - Size: 2824MB

- System Time
  - [20:59:22]

- System Date
  - [Wed 01/22/2014]

- Operating System not found
Running the ATM

Operating System not found

Attack failed
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

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
Software engineering 101

C:\Documents and Settings\User\Desktop>ATMDispenser.exe

ATM Dispenser v0.1 by Erik Van Buggenhout

------------------------------------------------------------------------
This PoC executable will use the XFS standard to perform an ATM cash-out in EUR.

Usage: <TOTALAMOUNT> <CASSETTE1-NOTES> <CASSETTE2-NOTES>

Totalamount: Total amount to be dispensed (e.g. 150)
Cassette1-Notes: Number of notes from cassette 1 (loaded with 10 EUR)
Cassette2-Notes: Number of notes from cassette 2 (loaded with 50 EUR)

Dispense will only succeed if the denomination is correct (e.g. 150 EUR = 5x10 EUR and 2x50 EUR).

C:\Documents and Settings\User\Desktop>
Software engineering 101

DEMONSTRATION
Topics for tonight

- Introduction
- Attacking the ATM
- Common ATM system design
- Developing ATM “malware”
- Conclusion
Modern ATMs are **standard**, **Windows-based**, computers full of money.

Developing ATM “malware” is a piece of cake.

Highly interesting target, protection is required!

- Patch management (No WIN XP)
- Application whitelisting
- Network segmentation
- Disk encryption
- Protect the BIOS