Robbing Banks: Easier Done Than Said
Table of Contents

❖ Introduction
❖ Bank Robberies by Any Mean
❖ ATM Attacks
❖ Network Attacks
❖ Direct Application Attacks
❖ Value Added Partner Services’ Attacks
❖ Insider Accomplice Attacks
❖ Conclusion
Introduction

❖ Foreword: we are NOT criminals
   ✦ Attack always performed with full documented contract

❖ Goal of attacks: know if the financial institution is affected
   ✦ Risk gets analyzed and fixed if necessary

❖ Goals of this presentation
   ✦ Increase awareness of typical vulnerabilities
   ✦ Most of it backed-up with real stats
   ✦ Provide concrete solutions
   ✦ Rant about some old technologies
Bank Robberies
By Any Mean

❖ Why banks?

✦ They have money to steal... lots of it!
✦ We’ve all seen enough bank robberies movies...
✦ ...or “hack the bank” movies

❖ What’s new?

✦ The variety of means to attack
✦ The lack of knowledge about these potential attacks
Bank Robberies
By Any Mean

❖ Physical bank robberies
  ✦ Either rob the bank coffers or the fund transfer truck
    ⚫ Dangerous
      ✷ you could get shot
      ✷ you could get recognized
    ✫ Money may be “marked”
    ✫ Money may be “tracked”
    ✫ Difficult to walk around with a million dollar discretely...
Bank Robberies
By Any Mean

❖ ATM Attacks
   ✦ Attack the bank-side ATM processor
   ✦ Attack the ATM OS
   ✦ Card duplication

❖ Network Attacks
   ✦ Hack into the bank’s network

❖ Direct Application Attack
   ✦ Hack into the bank’s applications
Bank Robberies
By Any Mean

❖ Value added Partner Services’ Attacks
   ✦ Attack loan sales agent
   ✦ Attack bill payment portals
   ✦ Attack payment gateway applications
   ✦ more...

❖ Insider Accomplice Attacks
   ✦ helps an attacker gain enough information to perform online attacks
Bank Robberies
By Any Mean

❖ Banks used to have a simple closed environment

❖ As payment services grew, banks had to open-up
  ○ ATM
  ○ Credit Card, international networks (VISA, MasterCard, Plus, Cyrus, Maestro, etc...)
  ○ SWIFT
  ○ Intra-country bank debit network (e.g.: NETS/ATM5 in Singapore, CB in France, JETCO/UnionPay in HK)
  ○ Phone banking
  ○ Centralised cheques processing
  ○ Internet Banking
  ○ Mobile Banking

❖ Now the environment is extremely complex!!

→ all these services create new avenues for frauds
Bank Robberies
By Any Mean

❖ The foundation of a bank is its “host”, its mainframe
❖ It is the one that perform all the actual money movements
❖ All services need direct or indirect access to the host
❖ Attackers no longer need to point a gun to perform a robbery
   ➡️ robbers just need to use the services in “unusual” ways
Bank Robberies
By Any Mean

Robbing Banks: Easier Done Than Said

Diagram of a bank's network infrastructure, including web server clusters, database server clusters, firewalls, and various connections such as Internet, mobile banking, ATM connections, and phone banking.
ATM Attacks

Robbing Banks: Easier Done Than Said

MiniBank
Fabrice A. Marie
A/C: 913275-033-023

ATM vsat connection
POTS dial-up
WiFi connection

Host
ATM Processor

vsat connection
POTS
dial-up
WiFi
cconnection
ATM Attacks

❖ An ATM performs money transactions for a client
  ✦ Uses a unique ATM card and the user’s PIN for authentication

❖ ATM cards are simply magnetic cards
  ✦ An attacker needs a $5 magnetic card reader to copy the card

⇒ **ALL magnetic ATM cards can be copied**

- Some banks use an invalid CRC so some advanced card reader fail
- However, cheap card readers will read the card, and copy it with the very same CRC error
- Cheaper hardware is better!
ATM Attacks
Card Duplication

❖ A lot of ATM frauds recently in the APAC region
❖ Probably other regions as well
❖ Full fraudsters syndicates

❖ The fraudster installs a thin card reader in front of the real ATM’s card reader
❖ And a pin-hole camera above the PIN pad

⇒ Fraudster get all the ATM and credit card numbers and their respective PINs.
ATM Attacks

Card Duplication

❖ Most banks protect their ATM against this kind of attacks
  ✦ Camera can record the face of the fraudster who installs the equipment
  ✦ Special card reader slot that make attaching an additional card-reader before the real card reader physically impossible

❖ What about other machines not owned by the bank?
  ✦ Overseas ATMs
  ✦ Merchants’ card readers
  ✦ Automated machines (ticketing, bill payment, etc…)
  ✦ …
ATM Attacks

“Network” Attacks

❖ ATMs have to be connected to the bank in real-time to perform the transactions

✦ Verify balance
✦ Deduce money when fund transfer performed
✦ Deduce money when money withdrawn

❖ Connection technology depends on a lot of factors

✦ Cost
✦ Location
✦ Legislation and compliance
✦ Bank’s head-office usual way / preference
ATM Attacks

"Network" Attacks (cont’d)

❖ ATMs use various connection types
   ✦ POTS dial-up
   ✦ Leased lines
   ✦ vsat connection
   ✦ WiFi connection
   ✦ Ethernet connection

❖ ATMs use various communication protocols
   ✦ SNA over SDLC
   ✦ TC500 over Async
   ✦ X.25
   ✦ TCP/IP over Ethernet

❖ The message format is generally a home-brewed version of ISO 8582.
ATM Attacks

“Network” Attacks (cont’d)

❖ Typical problems with ATM connections?
  ✦ Lack of encryption / Weak encryption
  ✦ Lack of authentication / Weak authentication
  ✦ Connection not physically secure

❖ Typical problems with ATM protocols?
  ✦ Complex doesn’t mean an attacker won’t know it
    ◦ Still a lot of X25 experts (in France/Italy for example)
    ◦ The complete SNA network stack on Linux was written by a 21 year old teenager in USA in 2001
  ✦ Protocols not properly implemented
    ◦ Recommended security settings
      ◦ ignored / misunderstood / badly implemented
ATM Attacks

“Network” Attacks

❖ An attacker plants a device between the ATM and the network
  ✦ Phone connector
  ✦ X.25 pad
  ✦ Ethernet mini-hub
  ✦ vsat and WiFi direct association

❖ Then he can start wiretapping the traffic
  ✦ Hopefully encrypted
  ✦ Most of the time weak encryption ➔ record all transactions

๏ Replay attack almost never works
  ‣ However, direct modification of the request sometimes work
    ✭ When the home-brewed ISO 8582 message does not follow the security recommendations
ATM Attacks

“Network” Attacks (cont’d)

❖ Once physically on the same network as the ATM, the attacker can try to hack into the ATM

✧ It’s a networked computer after all.
✧ Most are running EXTREMELY old version of windows these days
  ○ Plant a Trojan onto the ATM itself
  ○ Trojan could record ATM/Credit Card information including PIN
  ○ Trojan could arbitrarily dispense money
    ‣ Dispense less?
    ‣ Dispense more?
    ‣ Not dispense and still decrease balance?
    ‣ Retain the card?
    ‣ Overwrite the card with the previous client card’s content?
    ‣ more fun stuff…
ATM Attacks

"Network" Attacks (cont’d)

❖ Once physically on the same network as the ATM, the attacker can try to hack into the ATM Processor (bank-side)
  ✦ It’s a networked computer after all.
  ✦ Most are running archaic operating systems that are seldom patched-up

❖ ATMs often share the same key to authenticate to the bank
  ✦ Either steal the key using the trojan method above
  ✦ Or physically steal the ATM machine
    ◎ Needs 2 strong gangsters, and a pick-up truck.

❖ Then you can pretend to be an ATM when talking to the ATM processor of the bank, and perform valid arbitrary transactions.
ATM Attacks

“Network” Attacks (cont’d)

❖ Maybe your bank is protected against this kind of attacks ...
   ✦ ... or so you think... !!!

❖ What about other...
   ✦ Banks
   ✦ Bank networks
   ✦ Point of sales
   ✦ Automated machines
ATM Attacks
“Network” Attacks (cont’d)

Real Life Example 1:

❖ A leading bank in Bangkok, Thailand
    ✦ ATM in the shopping center...
    ✦ Is plugged to the UPS
    ✦ And to the X25 modem
    ✦ Without any temper-proof cover!!
    ✦ No security camera either
      ☐ Attacker could unplug the ATM and plug his laptop to the X.25 pad, then wiretap the traffic
      ☐ Attacker can modify the traffic on the fly
      ☐ Attacker can attack both sides of the connection (ATM / ATM processor bank-side)
ATM Attacks
“Network” Attacks (cont’d)

Real Life Example 2:

❖ A few leading banks in Bali, Indonesia
  ♦ ATM nearby the beach…
  ♦ Is connecting to the near-by branch of the bank using WiFi without encryption
  ♦ Another one is using vsat to connect to Jakarta (probably without encryption)
    ○ Attacker can peer with the network in both cases and wiretap the traffic
    ○ Attacker can modify the traffic on the fly
    ○ Attacker can attack both sides of the connection (ATM / ATM processor bank-side)
Real Life Example 3:

❖ A leading bank in Singapore

✦ ATM is securely protected in a hard-shell with security camera
✦ 3 meters away (far from the camera viewpoint) is the phone cable connecting ATM ↔ ATM processor bank-side

๏ Attacker can peer with the network in both cases and wiretap the traffic
๏ Attacker can modify the traffic on the fly
๏ Attacker can attack both sides of the connection (ATM / ATM processor bank-side)
ATM Attacks
“Standalone” Attack

Real Life Example 4:

❖ A bank in Taipei, Taiwan

❖ Withdraw $100 from the ATM
❖ Take 80
❖ Leave 20 (the ATM will take it back)
❖ The ATM will refund your account $100
❖ You just stole $80
ATM Attacks
Solution (short)
❖ Solution is technologically simple
❖ But costly
✦ Need to update all EFTPOS in the operating country
✦ Need to update all automated machines that support the card
❖ Problem:
✦ Security of ATM is as weak as its weakest link
๏ If card works overseas, then the card has to accept lower standards so it can be used there
ATM Attacks
Solution (long)

❖ Use smart-card technology + strong encryption
  ✦ Latest revisions are unbreakable so far
    ○ Impossible to copy
    ○ Impossible to operate without the card / brute-force

❖ Use strong encryption for privacy and authentication
  ✦ Each ATM terminal its own key

❖ Harden your machines
  ✦ Secure the ATMs OS like you would do with any other machine
  ✦ Secure the ATM Processor OS like you would do with any other machine
ATM Attacks
Solution (long)

❖ Use 2-factor authentication for big transactions
  ✦ 2nd factor can be a hardware token, sms, private question etc...

❖ Give a phone call for even bigger transactions

❖ Enforce geo-location conflicts
  ✦ If user just withdrew in Singapore he can’t be in Hong Kong five minutes later to withdraw again.
Credit Card Frauds

❖ Credit card is an old and INSECURE technology

❖ Some new secure standards

✦ BUT still compatible with the insecure old standard

➡ Stealing the card and forging the card’s signature works until today

➡ Or worse, buying an item by phone and giving someone else’s card information works too

❖ Credit cards have the same problems as ATM

❖ … plus their own! (ATM is therefore more secure)

❖ plenty of attacks, we will just see one
Credit Card Frauds
Simplest Attack Ever

Easiest attack

❖ Relies on the fact that merchants are ... careless
❖ Counterfeiting signature is trivial

Especially...

... when the merchant does not check the signature !!!

✦ Just use your credit card (no mistake... not debit card!)
✦ Buy dinner to a few friends
✦ And sign something totally unrelated (or let your friend sign...)
✦ Refuse to pay the bank!
✦ Bank will check, the signature will not match yours, the bank will reverse the transaction and the merchant will lose money!!!
Credit Card Frauds

Solution

❖ Enforce higher standards of security

✦ ... internationally

✦ Not going to happen tomorrow

❖ Use standards like in France for example

✦ Credit card is a smart-card

✦ PIN always necessary while in France

✦ Overseas the lower level of security applies

๏ Magnetic stripe

๏ Signature

๏ So even French cards can be used for frauds

❖ Hence the need to drop the support for lower level of security...

❖ And create ONE new SECURE international standard
Robbing Banks: Easier Done Than Said

Network Attacks

Diagram showing a network architecture with Web Server Cluster, Firewall and proxy, Application Server Cluster, Firewall, Database Server Cluster, Internet, telecom, Mobile banking, Other banks, X.25 network, LAN & other internal apps, Host.
Network Attacks

❖ Are complex
❖ Used to be very difficult the last 5 years
❖ But as banks offer more services…
  ✦ …they need to open up their network!!
❖ Anything goes
  ✦ Penetrate into the DMZ, and plant a sniffer
  ✦ Penetrate into the LAN though a VPN/Dial-up
    ๏ and do everything from there
  ✦ Penetrate a partner that has privileged access to bank network
  ✦ …
Network Attacks

❖ DMZ attacks are very unlikely
   ✦ virtually the best protected place in the bank

❖ LAN attacks are easier
   ✦ VPN attacks are the most straight forward
   ✦ Even better with a dial-up or a rogue WiFi
   ✦ Social engineering
     ☐ Courier a trojan on an “interesting” CD to an IT guy in the bank
     ☐ He will DEFINITELY open the CD in his desktop
     ☐ Trojan will connect to attacker launch pad and await commands
     ☐ Even better, malware/virus detectors will not detect it
       ❖ because it’s carefully custom made
Network Attacks

❖ While banks network are secure...
❖ ... their partners are not necessarily
❖ Attack the partners!
   ✦ stock brokers
   ✦ bank loan sales agencies
   ✦ sometimes even insurance companies
❖ Bank connected via global X.25 network?
   ✦ even better
Network Attacks Solution

❖ Secure your bank network like you secure your DMZ
❖ Prevent staff from installing rogue WiFi
❖ Prevent staff from installing rogue dial-up
❖ Don’t use X.25
  ✦ Internet or VPNs are cheaper and better understood
❖ Don’t trust your partners in terms of security
  ✦ separate yourself from them with a very strict firewall
❖ Secure ALL passwords on the VPN
❖ Segregate your internal network in smaller areas
  ✦ enforce internal policies with internal firewall with strict rules
Direct Application Attacks

❖ Banks have a lot of internet facing applications
  ✦ Consumer Internet Banking
  ✦ Enterprise Internet Banking
  ✦ Mobile banking
  ✦ Reward program
  ✦ Stock investment

❖ Each and every of them is an avenue for frauds
Direct Application Attacks

❖ Bank Applications attacks are generally simple
  ✦ If not simple, then the network equivalent attack would be worse!

❖ Lack of skills in the application arena
  ✦ Developers/Architects/Programmers are under-skilled
  ✦ Lack of funds for the application
  ✦ Lack of funds for the application security testing

❖ You have control over your network, but not over your application
  ✦ Network uses standard components
  ✦ Application is a monolithic peace of software
Direct Application Attacks

❖ Requirements for attack?

✦ Become a customer of your bank
✦ Username and password given to the attacker/customer

❖ Tools?

✦ Various interactive web proxies
  ✧ Burp
  ✧ WebScarab
  ✧ Paros, etc…
✦ Decompilers for .Net & Java
✦ Decoders and encoders

All free and easy to download
Direct Application Attacks

❖ Basic Concept:
   ✦ Fill in the form
   ✦ Intercept the request
   ✦ Modify the request without limitation

❖ Sometimes attacks are hard
   ✦ Lots of things to modify
   ✦ 6th sense / previous knowledge helps
   ✦ Complex interlinked data structures makes it harder
      ☐ The developer gets lucky sometimes

❖ Hard means a dedicated knowledgeable attacker will still manage, albeit in a longer time!!!

❖ Sometimes it’s super easy
   ✦ Change one field and enjoy!!
Direct Application Attacks (cont’d)

Logic Flaws

❖ “Using an existing functionality in an unauthorized or malicious manner in order to get what we want”

❖ Attackers want money so…

❖ Impact:
  ✦ … they’ll help the attacker rob the bank
  ✦ … or the bank customers
  ✦ Loss of confidentiality
  ✦ Usually outright frauds in general

❖ When it comes to stealing money
  ✦ they perform better than SQL Injections and other conventional web application attacks
Frauds we commonly find on internet banking applications:

- read other customer’s bill payments
- read other customer’s personal information
  - very useful as the base for more advanced attacks
    - identity theft
- stealing money using various transfer functionalities
- direct bank transfers among others
- buy shares at a discounted price
- avoid transaction fees
- various payment gateway systems replay attacks
- destruction of transaction records
- modification of other customer personal details
  - very useful as the base for more advanced attacks
    - user impersonation
Robbing Banks: Easier Done Than Said

Direct Application Attacks

Internet Banking Applications
Breakdown of vulnerabilities by category

- Sql Injection: 25%
- Cross Site Scripting: 11%
- Denial of Service: 11%
- Stolen money: 11%
- Loss of confidentiality: 9%
- System information disclosure: 9%
- Cryptography: 5%
- Session related: 3%
- The rest: 1%

Last 17 internet banking applications we audited (in 2005)

Applications we could steal money from: 100%
Applications we could steal personal information from: 100%

275 vulnerabilities
429 beta scripts
341 unnecessary files

average: 16 vulnerabilities per application
Direct Application Attacks
(cont’d)

❖ Application Security Testing CANNOT be automated
  ✦ Automated tools will only find generic attacks
  ✦ Automated tools will not know about logic flaws
    ○ and logic flaws are the most dangerous ones
  ✦ Automated tools may assist an experienced pen-tester
  ✦ but will never replace a professional
Direct Application Attacks

Service Oriented Architecture
❖ Buzz word for a central WebServices server
❖ Which is another buzz word...
   ✦ Basically a central, insecure, SOAP server
❖ Usually uses weak authorization
   ✦ several application use one username / passwords
   ✦ therefore a credit application could potentially
     ☑ transfer money
     ☑ instead of approving a credit
❖ SOAP makes the attack way easier for a network based attacker that would otherwise have to craft the transaction by hand
Value Added Partner Services’ Attack

❖ Large banks have a few partners
  ✦ stock brokers to invest shares
  ✦ loan sales agencies to sell bank loans
  ✦ pawn shops to secure loans
  ✦ car dealers to sell bank loans
  ✦ payment gateway processors
  ✦ bill payment service companies
Value Added Partner Services’ Attack

❖ Partners have to have access to the bank
❖ Either to dedicated specialized bank applications
  ✦ open only with VPN
  ✦ or firewall ACL
❖ Or to the bank SOA
  ✦ open only with VPN
  ✦ or firewall ACL
Value Added Partner Services’ Attack

❖ However partners have less stringent security rules
❖ Their applications are more insecure
❖ Their network are more insecure
❖ Yet they have a trusted access to the bank

❖ Trivial to use a partner as a launch-pad to defraud money from the bank or its customers
Value Added Partner Services’ Attack

✧ Visa is already forcing their partners to secure-up
  ✧ good, but is it enough?

✧ Some banks are forcing some of their partners to secure-up
  ✧ seldom happens. Yet if it does, is it enough?

✧ Banks should force ALL their partners to secure-up
Insider Accomplice Attack

- The threat always come from inside
- Bank LANs are never encrypted
- Internal networks are seldom properly segregated
  - even when they are since they are not encrypted...
    - ... an internal attacker can easily recover usernames / passwords
      - and masquerade as an admin / authorized user to fraud
      - and sell them to organized crime
Insider Accomplice Attack
(cont’d)

❖ Banks run a LOT of applications for internal use only
  ✦ Credit management applications
  ✦ Investment applications
  ✦ Identity management applications
  ✦ Payroll applications

❖ The list is unbelievable
  ✦ Most of them are weaker than the internet facing ones
  ✦ Which were already quite weak
  ✦ All the usual attacks apply (SQL injection, command execution, and the whole lot)
Insider Accomplice Attack
(cont’d)

❖ By getting a few relevant usernames / passwords
  ✦ using very basic sniffing techniques

❖ And insider attacker could
  ✦ authorized without authorization a loan an attacker requested
  ✦ spy on investments and provide “insider trading” information to an attacker
  ✦ increase an attacker credit limit
  ✦ wipe an attacker audit-trails or errors logged
  ✦ perform all sorts of interesting, undetectable frauds
    ○ they will be detected too late
    ○ the wrong person will be blamed
Pre-Conclusion

❖ If you are a bank and organized crime really wants your money
  ✦ they will recruit good hackers
  ✦ they will pay the right insider
  ✦ and they will definitely succeed

❖ That would be entertaining for the rest of us
  ✦ could be turned into a “real story” movie after that
Conclusion

❖ You protect your human tellers
  ✦ so protect equally your ATMs machines and network

❖ You put heavy firewalls and money in network security review
  ✦ So put strong controls in your applications
  ✦ and test them adequately as well

❖ Use strong encryption at EVERY level

❖ Force your partners to secure up to your level

❖ When organized crime will realize their “opportunity cost” they will definitely turn to cyber-robberies
  ✦ by then you better be ready
 Links

❖ Hacking Internet Banking Applications
   ✦ HITB 2005
   ✦ Available here:
     ○ http://www.packetstormsecurity.org/hitb05/BT-Fabrice-Marie-
       Hacking-Internet-Banking-Applications.pdf

❖ Application based Intrusion Prevention Systems
   ✦ HITB 2006
   ✦ Available here:
QUESTIONS?