1 Overview of Targets
2 Physical/Local Attacks
3 Inside Attacks
4 Protocol Attacks
5 Demos
Overview of Targets

Devices

- ATM Systems
- Typical Point of Sale Implementations
- Grocery Checkout Devices
- Kiosks
- Anything That Gives “Cash Back”
Overview of Targets

Infrastructure

- Processing Servers
- Device Management Infrastructure
- Active Directory
Overview of Targets

Network

• Paths from POS/ATM to processing
• Paths from Processing to Acquiring Bank
• Management Protocols
Physical/Local Attacks

1 Non-Invasive
   • Screen manipulation
   • Skimmers

2 Moderately Invasive
   • Device Manipulation

3 Very Invasive
   • Alternate Boot
Physical/Local Attacks

Screen Manipulation

- Kiosk/ATM frequently have touchscreen display
- You can’t usually ctrl+alt+del on that
- What happens when the device reboots?
- Win the race, and what do you get?
Physical/Local Attacks

Skimmers

- Oldie but goodie
- We still find these in the field
- Fit over current card slot or integrated into POS
- Frequently Coupled with something to capture PIN
  - Video
  - Keypad Mod
- Device is either recovered or transmits
Physical/Local Attacks

Device Manipulation

- What’s in an ATM?
  - Safe
  - Monitor
  - One or more computers
- It’s behind a lock
- USB ports are frequently active
- What happens when a keyboard is attached?
Demo: Physical Device Slideshow
Physical/Local Attacks

Device Manipulation

- Get past active application
- You may find you’re logged in as:
Physical/Local Attacks

Alternate Boot

- Some of these devices are using DHCP/BootP/PXE
- Try rebooting with malicious DHCP Server
- If you have bypassed the lock, try USB boot
- If USB is disabled, take the drive out
- Broken device management is difficult with all these disabled
Inside Attacks

1. Hardware Attacks
2. OS Attacks
3. Software Attacks
4. Infrastructure Attacks
Hardware Attacks

Talking Directly to the Money

- Things that automatically give cash back typically have a Serial or USB interface that goes from the computer to the dispenser.
- It goes through an init step, has the ability to report cash, dispense cash, and more.
- Through the last step, it may be possible to determine what to send the devices to get them into the proper stage.
- From there, either replay init/dispense messages or create your own.
- Harder to execute, but most logs live on the PC side, not the dispenser side.
OS Attacks

• Look Familiar?
OS Attacks

• Previously, many ATM/Kiosk devices were running embedded OS
• More of them have upgraded!
  – To XP
  – So they can be joined to the domain?
  – And use Domain Credentials to manage via Telnet?
• How long ago was MS08-067?
Software Attacks

Reverse Engineering

• Who will ever see this?
• It’s easier to debug software if you:
  – Add no anti-debug protection
  – Include Debug Symbols
  – Create verbose logs
    • Full track data is always helpful for troubleshooting
  – Have descriptive configuration files with no integrity checking
• This insight is equally helpful for your attacker
Software Attacks

Modifying Software Behavior

- Through DLL Injection/Detours code paths can be modified
- Information can be either changed or dumped
- Unmasking masked receipts
- This would allow for changing dispense amounts/bill amounts etc
- But also may give insight into how devices interact with hardware
Infrastructure Attacks

• Processing Server
  – In retail environments, cards go here for authorization
  – If you can reach this server, you’ve likely won
  – Memory dumping processes is still effective
    • Bad guys are doing it
    • So we do it too
  – Network capture is still effective
    • SSL is hard (it doesn’t Google itself)
    • More on this later
Infrastructure Attacks

- Device Management Servers
  - ATM and Kiosk management systems frequently have centralized management
  - These devices have the ability to query logs, push software, interrogate system status, and more
  - These devices are frequently joined to the domain
  - They are also frequently accessible from the corporate network
  - If you own it, you own ALL the target devices
  - Multiple un-documented management protocols, few of them encrypted
Defense Review

- Good Locks
- Alarms and MONITORING
- Cameras
- Harden the internals
- Encrypt the Network Traffic
- Cable Protection
- Host based Defense
- Patching Vigilance
Protocol Attacks

1. POS/Kiosk Attacks
2. ATM Attacks
3. Demo
Protocol Attacks

POS/Kiosk Attacks

- Many are communicating using ISO8583
- Predominantly Fixed Width Messages
- Can be implemented independently or using frameworks like jPOS
- Protocol dates back to ~1987
- Some updates, but many improvements have been done in fields that are specific to individual banks
- Two options for figuring that out:
  - Ask the Bank
  - Break out favorite pcap tool/scripting language and find proper markers and go from there
Protocol Attacks

POS/Kiosk Attacks

- So what are you looking for?
- One of 3 groupings of Fields
  - Track 1 Data (Bitmap 45)
    - Has PAN
    - Expiration Date
    - CVV
  - Track 2 Data (Bitmap 35)
    - Has PAN
    - Expiration Date
    - CVV
  - PAN (Bitmap 2)/Exp (Bitmap 14)
Protocol Attacks

POS/Kiosk Attacks

• With this knowledge, and the ISO spec, you can do a few interesting things
  – Steal PAN + Exp
  – Grab Track Data
  – Modify amounts
Protocol Attacks

POS/Kiosk Attacks

- So What’s the big deal, you still get charged?
  - Take a Prepaid Debit Card
  - Take Ettercap
  - Ask for 200$ cash back
  - Turn it into 20$ on the wire
  - Bank says authorized
  - You’re up 180$
- Some system have additional fields to verify amounts
- Newer systems may also have additional checksums or even SSL!
- POS/Kiosk talking to the local server frequently don’t have these, even if bank sees them higher up
Protocol Attacks

ATM Attacks

- ATMs work off a number of different protocol depending on version
- Ones seen recently use Diebold 91x, NDC, or XML
- Most transactions look like this:
  - Track data sent for auth with amount
  - Server responds back with service charge
  - Charge accepted
  - Server responds back with OK and one of two things:
    - Dispense 80$
    - Dispense 4 20s
Protocol Attacks

ATM Attacks

• So what do you do with this knowledge?
• Use Ettercap
  – Modify requests going out to downgrade dollar amount
  – Incoming requests to ATM raise the dollar amount
  – Result: Request 80, charge 20, 80 Approved
• Use Ettercap
  – Request whatever you want
  – Dispense 50 100$ bills
Protocol Attacks

ATM Attacks

- Many ATM PIN Blocks are encrypted with 3DES
- With a static key
- What does that mean?
- Use Ettercap
  - Capture one transaction
  - Create fake card
  - Rewrite pin block outgoing to already captured one
  - Charge 20$
  - Dispense 5000$
  - Make it rain
Demo

1. 8583 Client/Server communication
2. Capturing encoded data on the wire
3. Modifying amounts on the wire
Contact Information

Twitter/Email

- Twitter: @sussurro
- Email: Rlinn@trustwave.com

- Twitter @tilver
- Email: jhoopes@trustwave.com

- Thanks for coming
THANK YOU