CampusWide: Overview and Exploits

Acidus

(Acidus@resnet.gatech.edu)

www.yak.net/acidus/

Interz0ne Conference 9/27/2002

Presentation Overview

- Transaction systems 101
  - What they are
  - History
- System Specs
  - Overview
  - Server (AP/NP/Database)
  - Infrastructure
  - Cards
  - Readers

Overview Continued

- Simple Transaction
- Exploits
  - Reader to Device Exploits
  - Reader to Server Exploits
  - Card Based Exploits
- Securing an existing system
  - Photos of GT Worthless Security
  - How to really protect the system

Transaction Systems 101- What they are

- “One Card solutions”
  - Debt Card (Bookstore, food court)
  - Meal Plan
  - Library (Copy Machines, checking out books)
  - Building Access (Computer Labs, Offices, Labs)
  - Access to Sporting Events

Important! - Not just a debit card, it is the key to the whole school network

Transaction Systems 101 - History

- Special Teams (1984)
- Icollege (Envision)
- AT&T (CampusWide)
- Currently: BlackBoard Transaction System (Unix and NT)

Technology basically remains unchanged since 1984.

System Specs - Overview

- Simple System
  - Central Server with a database
  - Network interface
  - Hub spaced Network of data lines
  - Daisy-chained Readers

Server

- Applications Processor (AP)
  - Holds Database dbvista or Oracle
- Network Processor (NP)
  - Interface to all incoming data (RS-485, Ethernet, modem)
  - Convert to commands the AP can understand

Server - Specs

- HP9000, but any RISC processor will do
- Battery back-up
- 4 gig Tape drive for backups
- Normally Isolated from rest of network

Server - Interfacing

- Originally only from console, or 19,200 serial lines
- There are third party GUI’s to the database
- These change from school to school. No standard
- GT uses ?”Osiris”? For Door Entry

Infrastructure

- Uses RS-485
  - Doesn’t have protocol defined in standard
  - Used to control devices on factory assembly lines
  - Robust, has 2 data lines; uses difference between the 2
  - Short dist: 10 Mbit, Nearly a mile: 9600 baud. Repeaters extend range

Infrastructure continued

- IP Converters
  - Developed by Blackboard
  - Use existing Ethernet, ATT said this was bad idea (Any duplex network can work)
  - Hooks 16 devices to a box (Pentium w/ NIC), which encrypts, sends out TCP/IP
  - Keys can be updated remotely
  - Encryption unknown. High end: DES, Low end: XOR, key around 8 bytes

Infrastructure Continued still

- Merchant Dial-ups
  - Blackboard also created these
  - Low Cost, monthly fee
  - Before expensive lines needed to be run
  - Basically just a modem in a box
  - Lets you talk directly to the NP!

The Card

- Contains your standard ABA Track II.
- The card simply holds an account number which appears on the card
- These are printed on site using Polaroid card printers, just like at the DMV

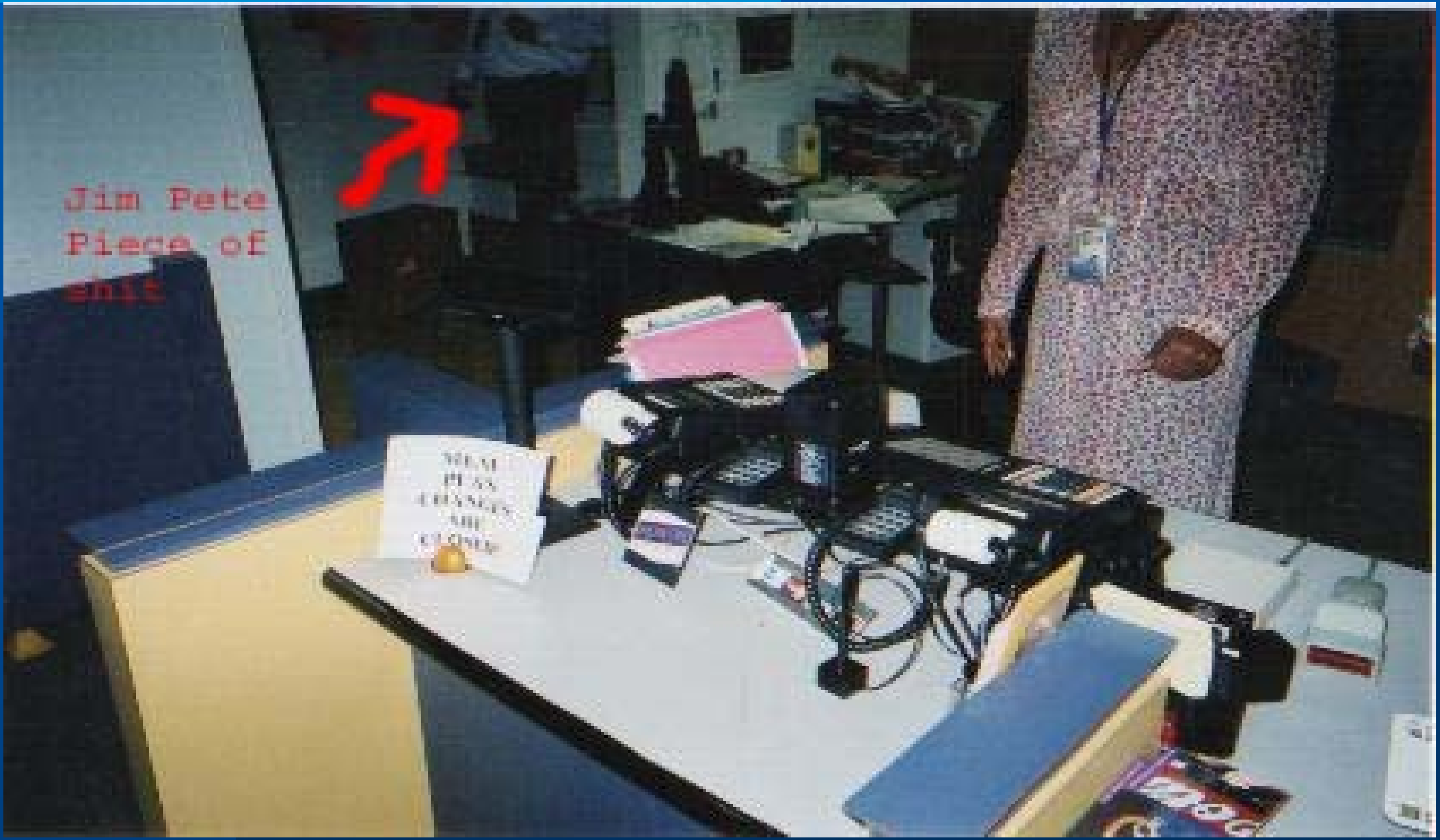
The Card - GT Buzzcard Center

The Card - GT Buzzcard Center

Purchase with a Temporary BuzzCard
Check your BuzzCard Account

The Card - GT Buzzcard Center

The Card - GT Buzzcard Center



Readers

- 3 types
  - Self-Vending readers (The bulk of them)
  - Door entry readers
  - Point of Sale (POS)

Readers - Overview

- Small, Black with either the ATT or Blackboard Logo
- Made of metal or plastic
- All data out of a reader is in RS-485, so it is backward compatible
- Transmits at 9600 baud
- I/O: 2x16 LCD with 16 key keyboard and activation LED's

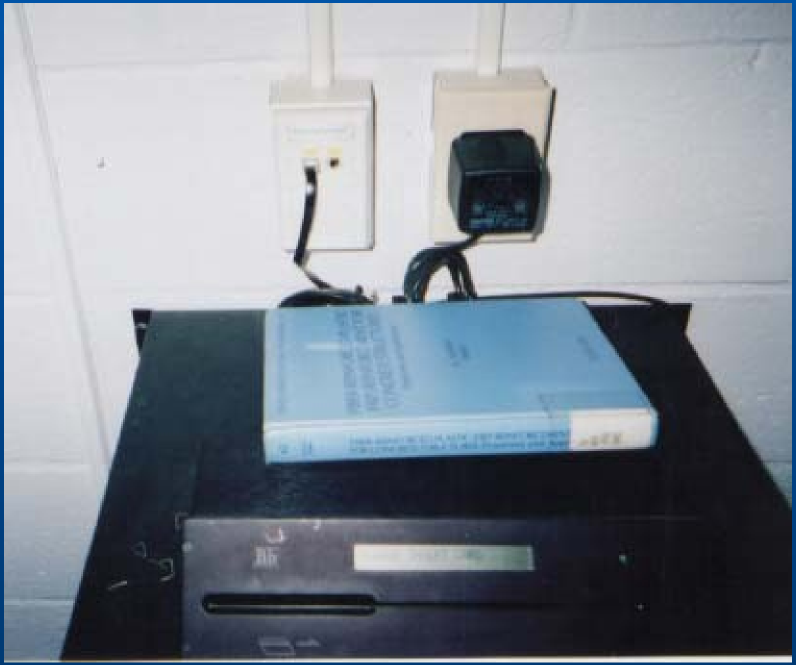
Readers - Overview continued

- Can store offline transactions in NVRAM
- Code is in boot ROM and Flashable RAM
- Boot very quickly, normally under 15 seconds

Readers - Self Vending

- Most common reader and most varied
- Laundry, Vending, Copy machines
- Easiest to hack because they are isolated
- All work basically the same. Talk to NP, confirm or deny transaction, then send signals to device.
- Can tell if Offline

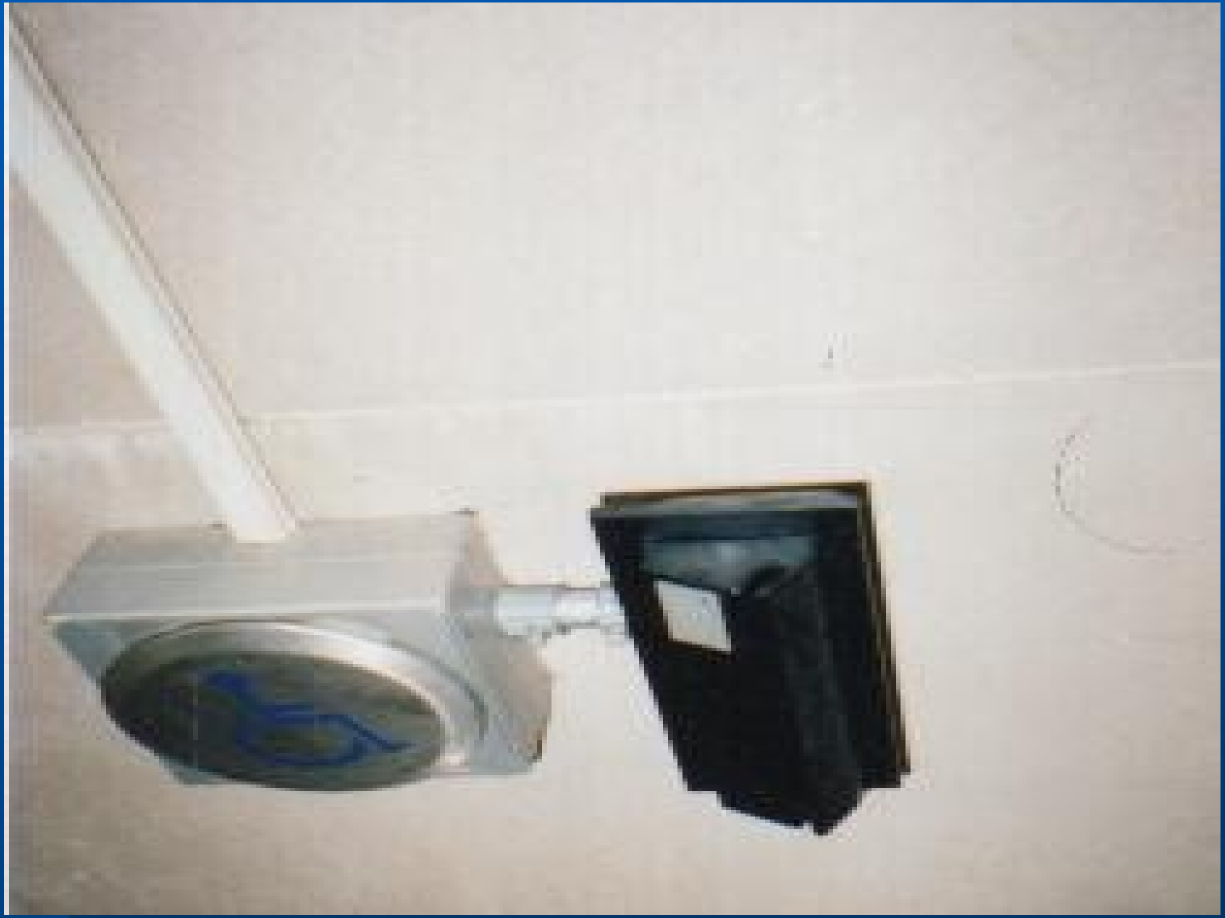
Readers - Self Vending



Readers - Door Entry

- Small and tricky
- Can’t tell they are offline
- Can hold a local database of 4000-16000 card numbers in NVRAM
- Uses this if it can’t reach NP
- Works just like vending, when confirmation received from NP, tell the magnetic door lock to release

Readers - Door Entry

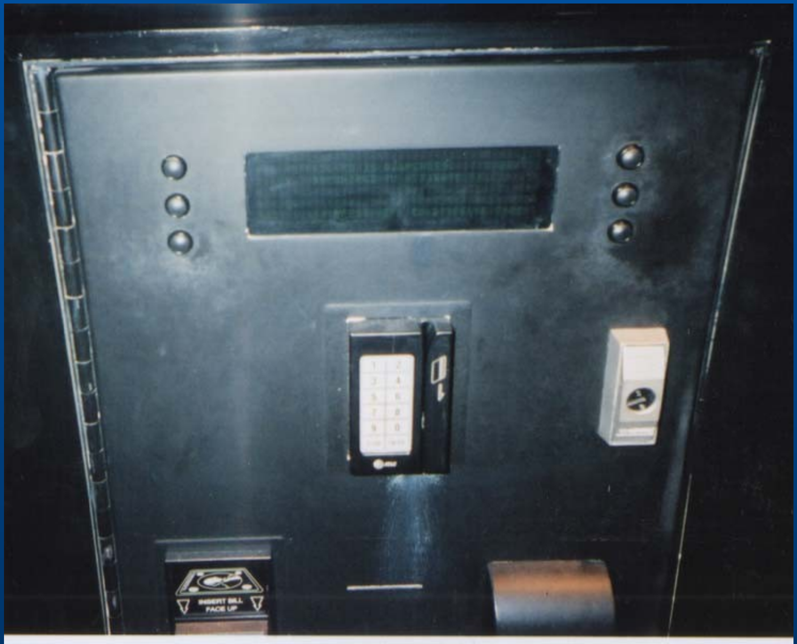


Readers - POS

- Most complex and large
- Rare compared to others
- Access will normally be restricted since they are almost always manned

Readers- Value Transfer Station

- The "Holy Grail"



Readers - Value Transfer Station

- Lets you deposit money on card
- Feed in all of your dollar bills, then it sends the signal
- Also allow temp cards (very bad)

A Simple Transaction

- **Want to buy a load of wash**
- **Select washer on laundry reader then swipe card**
- **Reader takes account number off card and sends along with reader ID to the NP through RS-485 lines**
- **IP Converter may be in between reader and NP, but it doesn’t know and doesn’t care.**

A Simple Transaction Continued

- NP receives signal (be it IP or RS-485) and converts it to a query for the AP.
- AP looks in account, deducts $1, sends back a confirmation and new balance to NP
- NP sends this info back to reader
- Reader displays new balance

A Simple Transaction Continued

- Reader talks to device. This is device specific. The Device has no idea it is attached to a network.
- For Laundry, Reader sends coin pulses to board in washer where coin validation normally attaches
- Laundry machine thinks 4 quarters dropped in and gives you a load of wash

Exploits - Overview

- System is relatively secure provided that the data lines are protected
- But, dial-up could be hacked or phone number social engineered out of stupid pizza boy.
- IP Converter releases packets into the wild. Careful analysis of traffic could show their IP addresses.

Exploits - Reader to Device

- Device is stupid, doesn’t know its on a network, so reader must simulate what that device is used for (in this case, quarter pulses)
- To compromise, simply access lines from reader to device, and then simulate quarter pulses yourself
- No way for machine to know the difference

Exploits - Reader to Device

- Pros
  - Very low risk: By their nature these are isolated
  - Very easy to hack: Most devices attached to these are coin based.
  - Communication is always 1 way from reader to device so there’s no complex handshaking to spoof

Exploits - Reader to Device

- Cons
  - Many be difficult/impossible to get at date lines between reader and device (ex: coke reader is mounted inside coke machine)
  - Leaves physical evidence in the way of stripped wire, etc

Exploits - Reader to Server

- Readers are stupid and can be fooled Ex:
  - Attach laptop to back to coke machine, grab all raw data after swiping card
  - Plug laptop to wall, send data to NP, record all that comes back
  - Attach laptop to coke machine, play NP’s response, get a coke
  - Replay NP’s response, get another coke

Exploits - Reader to Server

- RS-485 doesn’t define standard, but who cares? Signal may be encrypted, but again, who cares?
- If you get the raw data, that doesn’t matter
- VTS comes in here. It doesn’t send the “x $ was deposited onto y account” until you tell it to

Exploits - Reader to Server

- The Buzzcard Director confirmed that this can be done
- Would require analysis of packet, but, by depositing known $ on known account, it could easily be done

Exploits - Reader to Server

- Pros
  - Very low risk: By their nature these are isolated
  - RS-485 to RS-232 adapters relatively cheap ($50-$100)
  - No physical evidence: Most readers contain plugs into RS-485 networks, so no cut wires
  - Faster than Reader to Device spoofing
  - Only way to spoof coke machines

Exploits - Reader to Server

- Cons
  - Though confirmed, have not personally tested.
  - Reader could be smart, and wonder why it got a reply from server when none was sent. (Note: Even this is easily remedied. Swipe card, have you laptop ignore all data it receives from the reader, wait a second, and then send confirm)

Exploits - Reader to Server

- Cons continued
  - Data dumps from NP to reader would most likely only work on that reader, since packet most likely contains reader ID
- IP Converter Spoofing
  - IP address could be found by monitoring buildings.

Exploits - Reader to Server

- IP Converter Spoofing continued
  - Data in normal packets as well as swiping the multiple machines (up to 16) that the converter is on would allow the IP Packet Structure to be deciphered
  - Packets could then be sent from anywhere, making machines vend.
  - Tell all coke machines in library to all spit out a coke!

Exploits - Card based

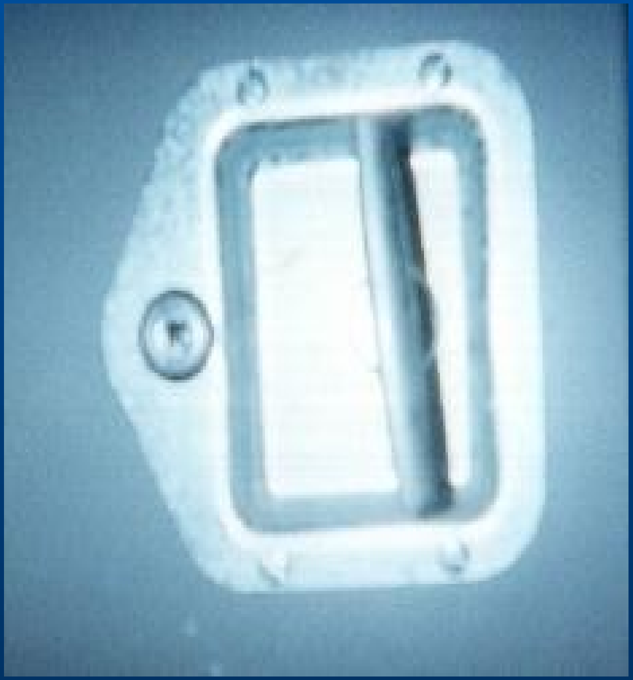
- Cards are ABA Standard, normal card capture tool will capture them
- Card contains basically just a number, which can be cloned
- This number could also be obtained by building a monitoring device on a RS-485 line, and let it harvest
- Clone card would work everywhere normal card would

Security - GT Style!

- If Data lines from server to reader and from reader to device are so important, they must be really protected right?
- …
- Well, not at Georgia Tech! Metal conduit protecting lines commonly stops at hanging ceiling

Security - MW/MHWMENC

- Panels containing equipment normally held on by flat head screws



Security - MW/MHWMENC

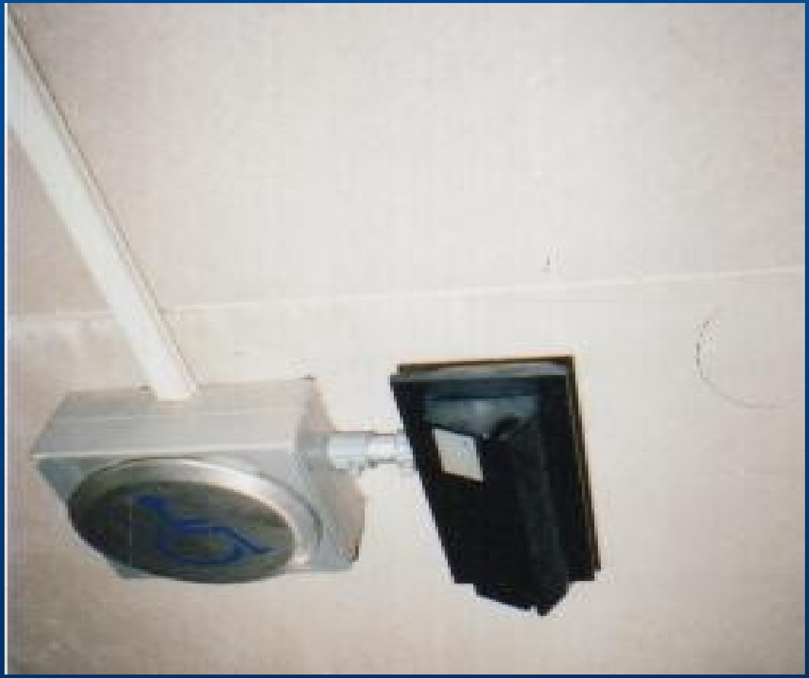
- What’s inside
  - Repeaters to boost Signals
  - Multiplexes to talk to all the Laundry machines

Security - Laundry Machines

- **Coils protecting data lines, attached with flat head screws**

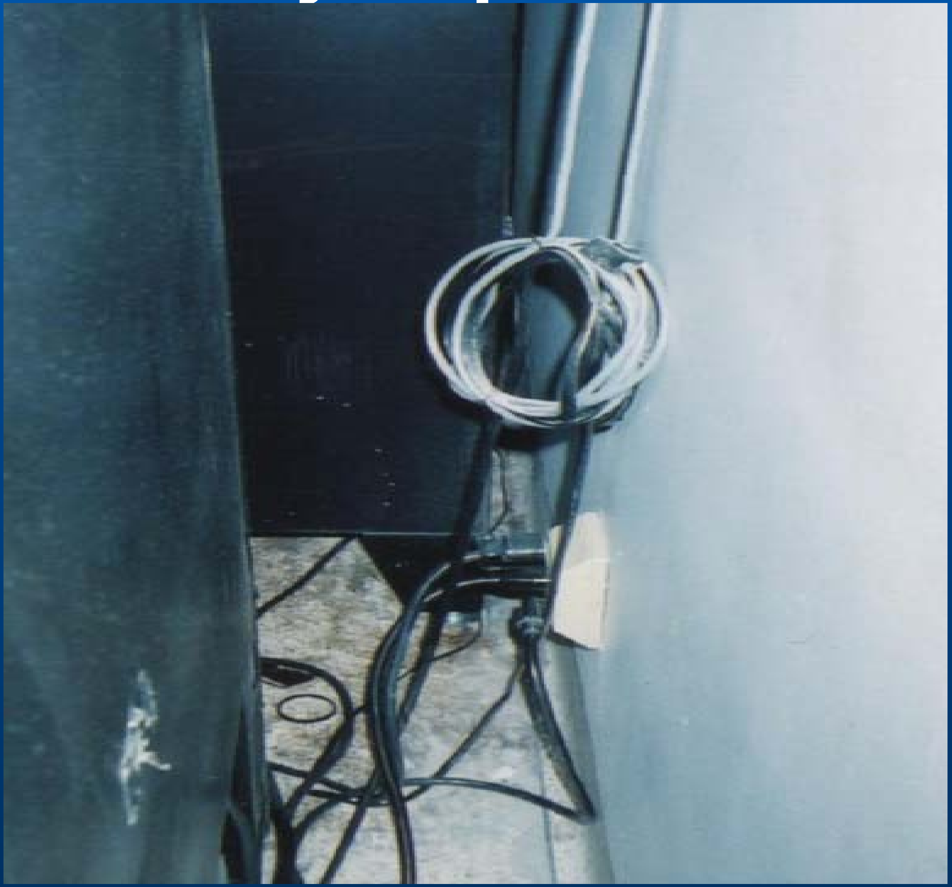
Security - Door Readers

- Lines for the door readers held on by flat head screws



Security - Coke Machines

- **RS485 totally unprotected**



Security - Coke Machines

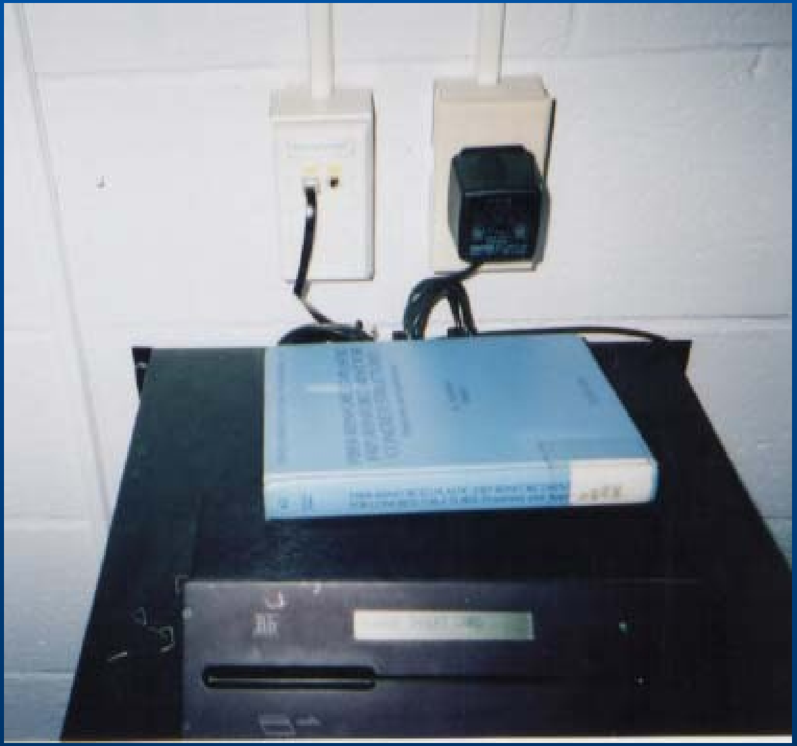
- With Convenient plugs no less!

Security - Coke Machines

- Which plugs into a hub inside that box, which has no lock

Security - Copy Machine

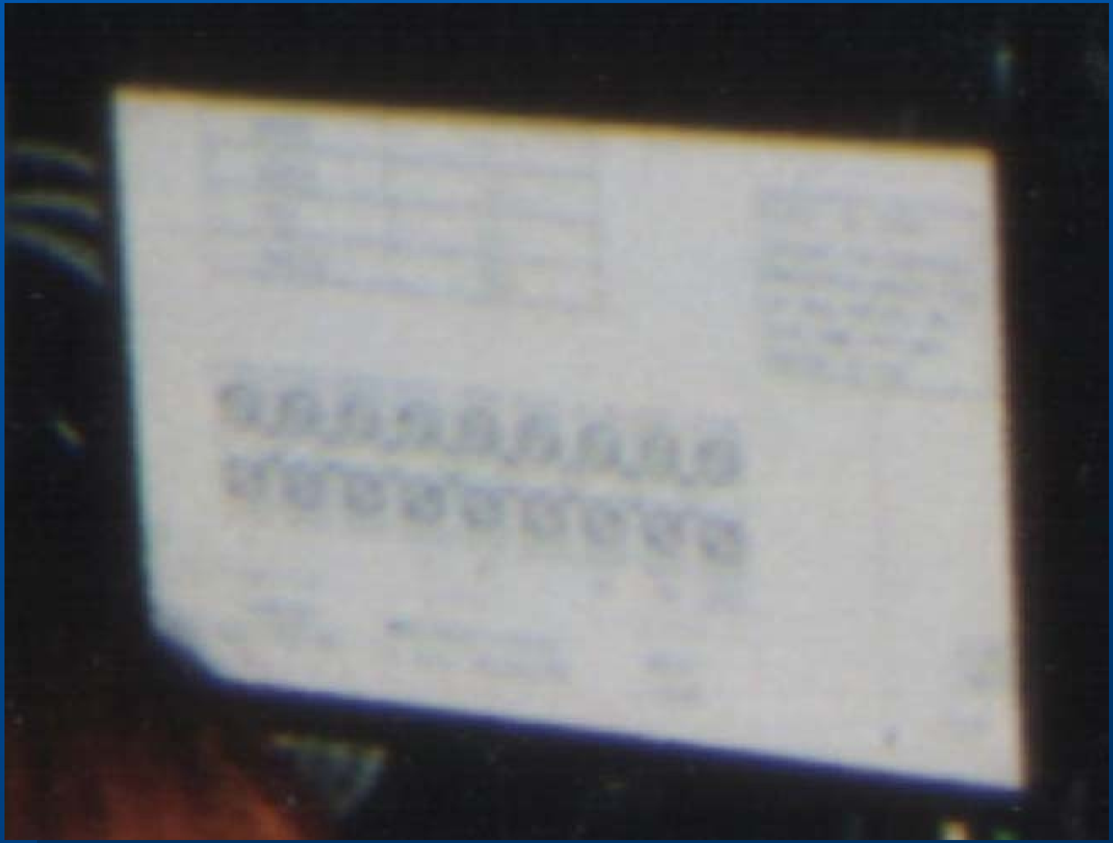
- They didn’t even try with this one!
- And the reader is attached to the shelf with… That’s Right! FLAT HEAD SCREWS!



Security - VTS

Security - VTS

- A Close up of the letters



Security - Really securing the system

- Secure the data lines.
- Get rid of IP Converters
- For god sakes, you take $9000 from me a year, buy some god damn Torx Screws!

QUESTIONS?

Closing

- Check www.yak.net/acidus
- For much more technical info:
- See me for copies of slides or the 2600 Article
- Tell your school about how insecure the system is
- Make them change it