OSI Layer 1 Security

Outline

• Access Control
  • Overview of Hardware Technologies
  • Overview of System Design
  • Common problems and Security Vulnerabilities

• CCTV
  • Overview of Hardware Technologies
  • Overview of System Design
  • Common problems and Security Vulnerabilities
OSI Layer 1 Security

Access Control

- Overview of Hardware Technologies
  - Proximity
  - Wiegand
  - Mag Stripe
  - Keypads
  - Biometrics
- Overview of System Design
  - Door Controllers
  - Small system design (<50 doors)
  - Large System design (>50 Doors)
  - Stand Alone Devices

- Common problems and Security Vulnerabilities
  - Improperly designed systems
  - Database Server Vulnerabilities
  - Easy duplication of credentials
  - Easily Circumvented Credentials
  - Defeating improperly installed locking devices
OSI Layer 1 Security
Access Control

Overview of Hardware Technologies

- Proximity
- Wiegand
- Magnetic Stripe
- Keypad
- Biometrics
OSI Layer 1 Security
Access Control
Proximity
The proximity technology reader constantly transmits a low level fixed RF signal that provides energy to the card. The most popular brand (HID) uses 125 kHz. When the card is held at a certain distance from the reader, the RF signal is absorbed by a small coil inside the card and powers the card's chip which contains a unique identification code. Once powered, the card transmits the code to the reader.

The whole process is completed in microseconds.
OSI Layer 1 Security

Access Control

Proximinity

**Pros:**
- Reader can be concealed in walls
- Card can be read through purse or wallet
- Cards are hard to duplicate
- Card rarely fail

**Cons:**
- Code can be stolen without contact
- Card can be used by unauthorized person
OSI Layer 1 Security
Access Control
Weigand
OSI Layer 1 Security
Access Control

Wiegand

Originally created to provide a permanently encoded card when magnetic stripe cards were so sensitive to magnetic fields. The Wiegand effect card is composed of a stream of bits of "Wiegand effect" wire inside the card. As the card is swiped through an electromagnetic field inside the reader, each bit of wire is charged momentarily until it gets to a read-head where it discharges itself and forms a data stream that will be used to identify the user. Wiegand was probably the most common technology in high security application before the advent of lower cost proximity technology.
OSI Layer 1 Security
Access Control

Wiegand

**Pros:**
- Cards are hard to duplicate
- Cards rarely fail

**Cons:**
- Expensive
- Must keep readers clean
- Card can be used by unauthorized person
OSI Layer 1 Security
Access Control
Magnetic Stripe
OSI Layer 1 Security

Access Control

Magnetic Stripe

Most people are familiar with this technology because of its wide spread use by bank and credit card operations. The card must be swiped or inserted in the reader so that the read head can pick-up the card's encoded data. The typical magnetic stripe accommodates 3 tracks. In banking and security applications, the standard is track 2.
OSI Layer 1 Security
Access Control
Magnetic Stripe

Pros:
• Inexpensive
• People are used to it from banks and hotels
• People can (in some cases) use their existing cards (credit card, bank card, library card, etc…)

Cons:
• Must keep readers clean
• High failure rate of cards
• High failure rate of readers
• Cards can be easily duplicated
• Card can be used by unauthorized person
OSI Layer 1 Security
Access Control
Keypads
Keypads are one of the most convenient, low cost, simple, and easy ways of doing access control. However they are also one of the least secure. Of any access control product keypads are the most commonly misused product. You can walk into almost any office building and find a keypad in the wrong place, installed improperly, and give a false sense of security. In my opinion the best use of a keypad today is as a secondary credential.
OSI Layer 1 Security

Access Control

Keypads

**Pros:**
- Inexpensive
- People are used to it from telephones
- People can make up their own pin codes
- Multiple people can use the same code
- The code is never “left home”

**Cons:**
- Code can be given away
- Code can be over seen
- Often installed improperly
- Code can be used by unauthorized person
OSI Layer 1 Security
Access Control
Biometrics
Biometrics refers to the automatic identification of a person based on his/her physiological or behavioral characteristics. This method of identification is preferred over traditional methods cards and PIN numbers for a few reasons, such as:

The person to is required to be physically present at the point-of-identification. (It’s very hard to let your friend borrow your finger)

Identification based on biometric techniques eliminates the need to remember a password or carry a card.

The credential is almost* impossible to duplicate.
OSI Layer 1 Security
Access Control

Biometrics

Pros:
• Higher Security than other methods
• The credential is never “left home”

Cons:
• Very Expensive
• Privacy issues with finger prints
• Most readers must be maintained
• Most readers are easily damaged
OSI Layer 1 Security
Access Control

Overview of System Design

Door Controllers

Small system design (<50 doors)

Large System design (>50 Doors)

Stand Alone Devices
OSI Layer 1 Security
Access Control
Door Controllers
In every access control system each door requires a door controller. In some systems many door controllers may be on the same circuit board. In others each may be individual. However all serve the same purpose and the majority have the same inputs and outputs.
## OSI Layer 1 Security

### Access Control

#### Door Controllers

**Inputs:**

1. Door Position Switch
2. Reader
3. Request To Exit (REX)
4. Auxiliary
5. Power
6. Communications

**Outputs:**

1. Main Door Relay
2. Auxiliary
3. Communications

Copyright 2003 Michael Glasser
OSI Layer 1 Security
Access Control

Small System Design
When dealing with systems of under 50 doors access control is, as a rule, kept very simple. Usually using either 2 or 4 door control panels mounted relatively close to the doors to be controlled. They have one cable daisy changed from the first to the next and eventually back to a computer for programming. Each panel can work on it's own without the help of the computer or any other panel.
OSI Layer 1 Security
Access Control
Small System Design

Basic Access Control System
OSI Layer 1 Security
Access Control

Large System Design
When dealing with systems of over 50 doors access control can get a bit more complicated. You are generally dealing with the same types of control panels, except more sophisticated. These are general TCP/IP enabled, and report to the computer constantly. One computer can control an access control system for hundreds of buildings at a time. The load on this computer can become very great.

For example:
Your access control system is controlling 20 turnstiles in a major Manhattan building. At the same time it is handling 15 more from the building across the street, 10 doors from the building down the block, 25 doors from the office upstairs, 120 doors from the Corporate headquarters in Florida, etc.…

Now make it 9:00am Monday morning. People are coming in everywhere at once. Each door controller is handling the load, but they are pumping log files into the computer so fast it starts to smoke! The computer crashes. You bring it back online and as soon as you do all the log files it had missed while being down suddenly start to get dumped into it again. The computer goes down. You start sweating and curse about how much you hate computers.
OSI Layer 1 Security
Access Control
Large System Design

You finally resolve this issue and now it’s 1:00pm. You’ve just given two new employees their ID cards and you are about to load them into the system. Unfortunately you can’t because the computer is now trying to handle the rush of the lunch crowd. Since it hasn’t downloaded yet when the new employees get to the turnstile, they can’t get through. The people behind them push, they lose their new jobs from being late to work on the first day, and everyone looks at you and asks why it didn’t work.
OSI Layer 1 Security
Access Control
Stand Alone Devices
OSI Layer 1 Security
Access Control
Stand Alone Systems

Sometimes you just can’t get a wire to a door. Sometimes you don’t need the audit trail from a door immediately. Sometimes you need a quick and simple solution that you can pop on a door and not worry about. That’s when stand alone systems come into play.

Any thing from a bathroom that you don’t want strangers using, to a utility closet that holds the mops, stand alone is a quick easy answer.

Hotels almost always use stand alone access control. Think about it! There aren’t any wires going to that lock, are there????
OSI Layer 1 Security
Access Control

Common problems and Security Vulnerabilities

Improperly designed systems

Database Server Vulnerabilities

Easy duplication of credentials

Easily Circumvented Credentials

Defeating improperly installed locking devices
OSI Layer 1 Security
Access Control

Improperly Designed Systems
OSI Layer 1 Security

Access Control

Improperly Designed Systems

This topic alone is worthy of a 2 hour discussion
Here are the worst offences.

• Putting the controller on the insecure side of the door
  • Protecting only one of many entrances
    • Not having a propped door alarm
  • Not instructing the employees of proper security protocols
OSI Layer 1 Security

Access Control

Database Server Vulnerabilities
OSI Layer 1 Security
Access Control
Network Access to Database Server

The access control database contains many things. The most important to someone who wishes to attack your company are the card numbers (if using cards), the pin numbers (if using keypads), and the log files of who is in the building, when they enter and leave, and where they are during that time. If they can’t get far enough to take the data, they may be able to destroy it. It is, unfortunately, common for me to get phone calls that the server crashed and they lost the database of all the users and system setup. Please, include this machine in your backups.
OSI Layer 1 Security
Access Control

Easy Duplication of Credentials
OSI Layer 1 Security

Access Control

Easy Duplication of Credentials

When using magnetic stripe for access control, duplication is a serious concern. The knowledge and technology needed to copy a magnetic stripe card is so easy and readily available, that you must assume that copies are being made.

When dealing with keypads, all it takes to make a copy of your code, is to tell someone.

Biometrics does very well to eliminate this problem.
OSI Layer 1 Security
Access Control

Easily Circumvented Credentials
OSI Layer 1 Security
Access Control
Easily Circumvented Credentials

In 80% percent of the access control systems today, regardless of what type of credential you are using there is a relatively easily exploited vulnerability.

A “Man in the Middle” attack used on the wire between the reader and the control panel will work every time. This will work against Proximity, magnetic stripe and even biometrics. Almost all of these systems simply send out a string of bits representing a user. The simplest way to attack this is to pull the reader off the wall and hide a small battery powered door controller attached to it. Every time an authorized user enters, the door controller that you’ve installed will record the ID number. Once you have the valid Id number you can go back and use a keypad to output that number.

The system can’t tell the difference.

The best way to be safe from this type of attack is to have all access points watched by a CCTV system.
OSI Layer 1 Security
Access Control
Easily Circumvented Credentials

The design of proximity cards let the ID number be read through bags and wallets. What’s to keep someone from reading that information while simply standing next to you?

For Example:

I walk into an elevator next to the president of ABC Corp. In my briefcase I have a small battery operated door controller and a long range proximity reader. While standing next to him the long range reader picks up his card number. Now I simply go in after hours with a keypad, disconnect the proximity reader off the wall, plug in the keypad and type in that number.
OSI Layer 1 Security
Access Control
Defeating Improperly Installed Locking Devices
OSI Layer 1 Security
Access Control
Defeating Improperly Installed Locking Devices

AN ACCESS CONTROL SYSTEM CAN ONLY WORK IF THE DOOR CLOSES AND STAYS CLOSED

Make sure all doors have door closers and that all doors properly close on a regular basis.

If a lock is installed improperly a credit card or a paper clip can defeat your access control system.
OSI Layer 1 Security

CCTV

• Overview of Hardware Technologies
  • Cameras
  • PTZ Cameras
  • Multiplexers
  • VTRs
  • DVRs

• Overview of System Design
  • 4 Camera VTR System
  • 4 Camera DVR System
  • 16 Camera Networked DVR System
  • Multisite DVR System

• Common problems and Security Vulnerabilities
  • Improperly designed systems
  • Recorder Vulnerabilities
  • Vandalized Cameras
  • Network Bandwidth
  • Covert Video
Keeping everything in proper perspective is the first and foremost step to a good CCTV system design. This means that you must remember that CCTV systems are meant to be “Visual Assessment” and/or “Visual Documentation” tools and nothing more! You should never allow yourself or a hired consultant to design your CCTV system with anything more or less in mind. Visual assessment refers to having visual information of a proper identifiable and/or descriptive nature during an incident. Visual Documentation refers to having visual information stored in a format that allows the study of and/or review of images in a sequential fashion. In addition, visual documentation will include various, in-bedded, authenticity, points ... i.e.; time / date stamp, character generation, etcetera.
OSI Layer 1 Security

CCTV

Overview of Hardware Technologies

Cameras

Multiplexers

VTRs

DVRs
OSI Layer 1 Security

CCTV

CAMERAS
The camera that you choose to use will be determined by its sensitivity first, its resolution second, and its features third. Sensitivity refers to the amount of actual visible or Infrared light necessary to produce a quality image. Resolution defines the image quality from a detail or reproduction perspective. The camera’s features are those things that give one camera an advantage over another. Therefore the camera type or model that you will use is always decided upon prior to the lens selection. It is also very common and possible to have multiple or different models of cameras within the same system. It is not recommended however, to have or use cameras from multiple manufacturers within the same system. This is due to simple and subtle differences within the timing circuits of the cameras. Each manufacturer, although working within limits of the NTSC or PAL standards, has a slight difference as to how they produce an image. Therefore phasing or sequencing problems may arise when using cameras from multiple manufacturers within the same system.
OSI Layer 1 Security
CCTV CAMERAS

Resolution standards for Color camera’s are:

“Low Resolution” 300-330TVL

“Medium Resolution” 380-420TVL

“High Resolution” 470-500TVL
OSI Layer 1 Security
CCTV

Multiplexers
The early multiplexers were basically video switchers that could mark each camera with a unique number in the vertical interval. This required the cameras to be v-phased so the VCR would see a continuously composite sync signal so it would not lose servo lock on the switched incoming video signals. The playback mechanism merely switched to the correct camera only during its active period on the tape while switching to a flat field (usually a solid gray picture) for the rest of the time. This caused severe flicker but produced a viewable single camera image and was effective.

Later digital memory was used to save the active camera until a new picture was displayed. Early v-phasing was poor and cameras drifted causing the VCR to record garbage, therefore resulting in poor playback regardless of digital memory or not. Next a two field digital memory was used to time base correct the incoming signal to guarantee continuous composite video to the VCR. The main benefit of this technology was that this device guaranteed continuous composite sync to the VCR regardless of the video quality. A side benefit was that when non-v-phased any camera could be used. This method is still the preferred method used among multiplexer manufacturers.
OSI Layer 1 Security
CCTV

VTRs
VTRs

A VTR (video time-lapse recorder) is virtually the same as a VCR. The main difference is that VTRs record using a “time-lapse” mode. Real time recording uses a full 30 frames per second recording. Time lapse is anywhere below that. The advantage of using time lapse over real time is longer recording times. The main disadvantage is the longer the record time, the more information is missing. (960 hour recording takes a frame every 8 seconds) It’s like walking in a strobe light. You miss information while the light is off. In VTRs you miss information between frames.
OSI Layer 1 Security

CCTV

DVRs
DVRs

DVRs (Digital Video Recorders) are the newest and hottest thing in CCTV. Most DVRs are an off the shelf computer with a multi channel video input card installed. There are about 6 Korean companies that make the majority of those video input cards and yet there are over 200 DVR manufacturers in the USA.

The differences are easy to see if you look for them!!!
Important factors to consider when evaluating a DVR:

1. Frame Rate (How many frames per second can the recorder handle?)
2. Resolution (How will the pictures look at that frame rate?)
3. Compression (Will you fill your hard drive in 1 day of recording?)
4. Hard Drive Space (How long can you record for?)
5. Features (Can this recorder do what you need it to do?)
OSI Layer 1 Security

CCTV

Overview of System Design

4 Camera VTR System

4 Camera DVR System

4+ Camera Networked DVR System
OSI Layer 1 Security
CCTV

4 Camera VTR System
OSI Layer 1 Security

CCTV

4 Camera VTR System
OSI Layer 1 Security
CCTV

4 Camera DVR System
OSI Layer 1 Security
CCTV
4 Camera DVR System
OSI Layer 1 Security
CCTV

4+ Camera Networked DVR System
OSI Layer 1 Security
CCTV
4+ Camera Networked DVR System
OSI Layer 1 Security

CCTV

Common problems and Security Vulnerabilities

- Improperly designed systems
- Recorder Vulnerabilities
- Vandalized Cameras
- Network Bandwidth
- Covert Video
OSI Layer 1 Security
CCTV

Improperly Designed Systems
What good is a CCTV if it’s watching the wrong things, or even worse if it’s watching the right things but has been set up wrong?

This is a very common problem and should not be over looked. Cameras in parking lots are one of the best examples. I have seen people spend thousands of dollars on recorders and cameras to properly protect their workers on their way home at the end of the day, only to realize that the cameras were no good in the dark!

Many people believe in having 1 PTZ (pan-tilt-zoom moving camera) camera to watch a warehouse. In most cases it would be more cost effective and get much better coverage buying 5 or more fixed cameras then 1 PTZ. PTZ’s are meant so that a guard on site can focus their attention on a situation. When a PTZ is left to scan side to side you have a very good chance of missing the critical piece of information when you need it most.
OSI Layer 1 Security
CCTV

Recorder Vulnerabilities
OsI Layer 1 Security

CCTV

Recorder Vulnerabilities

The first thing all good burglars do when they rob a convenience store is demand to know where the video recorder is. They then take the tape.

WHAT GOOD IS A RECORDER WITHOUT THE RECORDING???

The first step to protecting yourself with a CCTV system is protecting your recorder. Make sure it is in a secure locked box and that all the current tapes are locked up. If you are using a digital recorder make sure it is locked as well.

When using digital recorders that are hooked up to the network you must be careful to protect them the same way as you would any other server. They are susceptible to the same types of attacks. For example, on a very popular brand of recorder if you simply start requesting that it opens remote sessions to quickly, it’s recording frame rate can drop from 30 frames a second down to less the 1. If you hit other brands the same way, they will simply crash.
OSI Layer 1 Security
CCTV
Recorder Vulnerabilities

Most of the DVRs are either Windows based or Linux based.

Can YOU guess how many of the amateur manufactures properly set up windows security and file sharing???

I’ll let you find out for yourselves.

If someone deletes all the video recorded on the DVR who’s fault is it that it wasn’t protected???

Protect the DVRs because no one else will!
OSI Layer 1 Security

CCTV

Vandalized Cameras
OSI Layer 1 Security

CCTV

Vandalized Cameras

I haven’t met a camera yet that a can of spray paint can’t defeat. (and yes I’ve seen the ones with window wipers)

• Make sure that cameras are mounted high and out of peoples range.
• Cameras are expensive, if someone can get to it, they will steal it!
  • Make sure the wires are concealed or in protective conduit
• Install vandal resistant cameras outdoors (people throw rocks!)
OSI Layer 1 Security
CCTV

Network Bandwidth
How much bandwidth do you think 16 cameras showing real time video takes up?

I come up against this every day. For example:

I am a guard for ABC Corp. I am sitting at my desk doing my job and decide to take a look at all the different sites my company owns. I start opening up windows to every site, just like I always do, but today I keep them open instead of closing them one at a time. I now have 64 real time streaming video signals on my screen and I feel like I am doing a good job.

And then the network administrator kills me.

Get involved from day one. When you hear they are installing security ask about the network, and don’t trust the salesman do your own bench tests.
OSI Layer 1 Security
CCTV

Covert Video
OSI Layer 1 Security
CCTV
Covert Video

What’s legal? What’s not?
A good rule of thumb is this.

*If you would show somewhere to a guy delivering pizza to your office you can most likely put a video camera there.*

Can you put a camera in a bathroom? MAYBE, but I wouldn’t suggest it. I have come across this where schools have aimed them at the doors only to catch who was going in to smoke.

Can you put a camera in a private office? Yes
Can you put it under the desk? No
OSI Layer 1 Security

Conclusion

Thanks to:

http://www.corporatedefense.com  Security Consultant
http://www.surveillance-video.com/  Retail CCTV Equipment
http://www.plm-group.com  New York Rep Group
http://www.logica-group.com  Security Manufacturer
http://www.synergisticsinc.com  Access Control Manufacturer
http://www.generalsolutions.net  DVR Manufacturer
http://www.kaba-ilco.com  Access Control Manufacturer
http://www.multiplexertechnology.com/  CCTV Manufacturer
http://biometrics.cse.msu.edu/info.html  Biometrics Info
http://winn.com/bs/disclaimer.html  Disclaimer
http://www.kantech.com/  Access Control Manufacturer
http://www.hidcorp.com/  Access Control Manufacturer

Copyright 2003 Michael Glasser