Strengths and Weaknesses of Access Control Systems

Eric Schmiedl and Mike Spindel
Choosing a System

- Error rate
- Environment
- Cost
- Physical Vulnerability
- Additional Constraints
Error Rate

- False Reject Rate (Type I error)
- False Accept Rate (Type II error)
- Equal Error Rate
Environment

- Does it have to handle inclement weather?
- Vandals?
- Extreme temperatures?
Cost

• You’re on a budget.
Physical Vulnerability

- Decreased resistance to forced and covert entry
  - Electromagnets can be bypassed with packing tape
  - Electric strikes can disable anti-loiding features on locksets
    - "Loiding": from the celluloid strips originally used to slip latches. Credit cards can also be used.
  - Request to exit sensors can be defeated with balloons, long pieces of plastic, etc.
Additional Constraints

- What load does the system need to handle? How fast does it have to process users?
- Do you need different levels of access for different users? An audit trail?
- Does the system have to talk to a separate alarm system?
- Will it detect or resist physical attacks?
How to improve the security of any access control system
Stacking

What you have + What you know + What you are

• Improve either FAR or FRR (in the most common configuration)

• Can reduce security

• e.g. mechanical key bypass
Centralized systems

- Terminals
- Communication lines
- Servers
Categories of Systems

- Guard
- Token
- Knowledge
- Biometric
Guard Checks Photo ID

• Good:
  • Simple
  • Low initial cost
  • Fast
  • Not affected by the environment.
Guard Checks Photo ID

• Bad:
  • Easy to counterfeit ID cards
  • Cards can be stolen
  • People get complacent
  • Guards have salaries, not a one-time purchase cost.
Guard Checks Photo ID

Source: www.african-safari-pictures.com
Guard Checks Photo ID

- Ugly:
Guard Checks Photo ID

- Ugly:
  - 32.6% error overall
Guard Checks Photo ID

- **Ugly:**
  - 32.6% error overall
  - Paranoid: 3/6 cashiers rejected a recent, accurate photo at least once

Source: www.african-safari-pictures.com
Guard Checks Photo ID

- **Ugly:**
  - 32.6% error overall
  - Paranoid: 3/6 cashiers rejected a recent, accurate photo at least once
  - 34.09% of the time a blatantly wrong photo was accepted

Source: www.african-safari-pictures.com
Guard Checks Photo ID

• Ugly:
  • 32.6% error overall
  • Paranoid: 3/6 cashiers rejected a recent, accurate photo at least once
  • 34.09% of the time a blatantly wrong photo was accepted
  • 50% false accept rate

Source: www.african-safari-pictures.com
Guard Checks Photo ID

• Ugly:
  • 32.6% error overall
  • Paranoid: 3/6 cashiers rejected a recent, accurate photo at least once
  • 34.09% of the time a blatantly wrong photo was accepted
  • 50% false accept rate
  • 63.64% FAR for a similar-looking photo

Source: www.african-safari-pictures.com
Tokens

- Mechanical key locks
- Magnetic cards
- Barcodes
- Proximity / RFID
- Smart cards / CPU tokens
- BFV and Wiegand Wire
- VingCard
Mechanical key locks

• Very reliable and need no power supply
• No audit trail
• Lots of security issues
  • Picking
  • Bumping
  • Decoding
• Attacking the master key
• Many different mechanical lock technologies
VingCard

- Mechanical keycards
- Quick to rekey
- Easy to copy
  - Hotel thieves example
- Electronic lock decoding
- Low security
Magnetic Stripe cards

- Low vs. High Coercivity
- Reliable (as long as there’s no magnet around)
- Audit trail limited by back-end
- Cheap
- Trivial to read, duplicate, and potentially modify
Barrium Ferrite Cards

- Preceded HiCo magstripe standard
- Embedded layer of Barium Ferrite
- Tough:
  - Weather-resistant
  - High Coercivity
- Easy to decode
- Last seen in an automated parking system
Wiegand Wire

- Processed magnetic alloy
- Single apparent domain wall
- Low coercivity core
- High coercivity shell

Image adapted from Switching Behavior of Stressed Vicalloy Wire, IEEE Transactions on Magnetics, 1979
Wiegand
Wiegand Wire

- First attack published in 1996 on cypherpunks list:
  - Cut wires out of a card and rearrange

- Vulnerable to emulation style attacks
Barcodes

- Cheap, low security
- 1D and 2D versions
- Easy to duplicate
- Invisible barcodes
Prox / RFID

- Many well-known issues
- Cloning
- Hybrid RFID / Magstripe systems

Richard M. Stallman’s Office Key
CPU Tokens

- Smart cards, iButtons
- It’s easy to make a ‘virtual’ token
- Cryptographic authentication is necessary for real security
- DirecTV vs. Hackers
Knowledge

- Mechanical combination locks
- Electronic keypads
- Safe-type electronic locks
Mechanical combination locks
Mechanical combination locks

- **Good:**
  - Simple, reliable, and no power necessary
Mechanical combination locks

• **Good:**
  - Simple, reliable, and no power necessary

• **Bad:**
  - No audit trail
  - Can be manipulated (usually)
  - Brute force attack

• [http://www.cs.berkeley.edu/~bh/v3ch2/math.html](http://www.cs.berkeley.edu/~bh/v3ch2/math.html)
Simplex operation
Opening Procedure
Which tumbler is binding?

binding
not binding
Push 1. Is a new tumbler binding?
Advance tumbler 1 by pushing a “throwaway” button -- here, number 5 -- and check if another tumbler is binding.

This tumbler is advanced by 1 when I push this one.
Try pushing another throwaway button -- 4 -- and check for binding
Reset, and try the combination 152
Check if any new tumblers are binding now.
Reset, and try the combination 125
Check if any new tumblers are binding now
Reset and try the combination 123
Electronic keypads
Electronic keypads

- Attacks
Electronic keypads

- Attacks
- The UV powder trick
  - Attacker needs to enter very many combinations
  - So use a highlighter
Electronic keypads

- Attacks
- The UV powder trick
  - Attacker needs to enter very many combinations
  - So use a highlighter
- Shoulder surfing and hidden cameras
Electronic keypads
Electronic keypads
Electronic keypads

- Dynamically changing “scramble-key” high-security keypads fix most of these problems
Electronic keypads

- Dynamically changing "scramble-key" high-security keypads fix most of these problems
- Users can still distribute the combination
Safe-type electronic locks
Safe-type electronic locks
Safe-type electronic locks

- Very secure
Safe-type electronic locks

- Very secure

- Audit trail usually available
  - LaGard Navigator
    - Web-based lock designed for ATMs, extensive audit trail
    - User connects smart phone or PDA loaded with client software that allows the lock to communicate with the server
Safe-type electronic locks

- Very secure
- Audit trail usually available
  - LaGard Navigator
    - Web-based lock designed for ATMs, extensive audit trail
    - User connects smart phone or PDA loaded with client software that allows the lock to communicate with the server
- Some are vulnerable to spiking and other safe-technician tricks
Biometrics

- Voice
- Face
- Fingerprints
- Hand geometry
- Retina scan
- Iris scan
- Signature
Voice pattern recognition

- Reliability
  - Time, stress, illness
- Easy to defeat
Face recognition

Hold up a photo or a laptop
Fingerprints
Fingerprints

• Guess what your fingers leave behind on the sensor?

  • Use gummi bears, breath, water-filled bag (condom)
Fingerprints

• Guess what your fingers leave behind on the sensor?
  • Use gummi bears, breath, water-filled bag (condom)

• Environment around the sensor has fingerprints too
Fingerprints

- Guess what your fingers leave behind on the sensor?
  - Use gummi bears, breath, water-filled bag (condom)
- Environment around the sensor has fingerprints too
- Supervision by trained guards
Multispectral imaging

- The manufacturer claims that it:
  - Does not require contact between the finger and reader
  - Is capable of reading when the reader is immersed in water
  - Inherently differentiates between a live finger and any prosthetic
Multispectral imaging

http://www.lumidigm.com
Hand geometry

- Hands are not unique
- Privacy
- Dummy hands
Retina scan

- Nobody in the public literature has yet falsified a retina.
- Invasive
Iris scan
Iris scan

- Effectively zero error rate
- 1 in 1 million Equal Error Rate
- For FRR of 0.0001%, an FAR of 1 in a trillion (1x10^{-12}%)
Iris scan

• Effectively zero error rate
  • 1 in 1 million Equal Error Rate
  • For FRR of 0.0001%, an FAR of 1 in a trillion (1x10^{-12}%)

• Defeating iris scan
  • Magazine covers
  • Printing on contact lenses
• Measure pressure and velocity

• 1% ERR

• Banks demand 1% FAR and 0.01% FRR

• Forging signatures is easy to learn
Further reading

- Ross Anderson’s *Security Engineering*
- Ross, et al. *Handbook of Multibiometrics*