Physical Security

- Physical protection and attacks;
- Authentication technologies;
- Direct attacks against computers
- Special-purpose machines
- Physical intrusion detection

Legal Notice

- Laws regarding lock picking vary significantly state-by-state
- In most states purchase and possession of dedicated lock picking tools is legal
  - Penalties are raised significantly if you get caught using them in the commission of a crime

Public domain image from http://commons.wikimedia.org/wiki/File:Madame_Restell_in_jail.jpg

What Is Physical Security?

- Any physical object that creates a barrier to unauthorized access
- This includes: locks, latches, safes, alarms, guards, guard dogs, doors, windows, walls, ceilings, floors, fences, door strikes, door frames and door closers

Is Physical Security An IT Concern?

- You have been working hard to secure your network from cyber attacks
  - Redundant layers of antivirus programs, firewalls and intrusion detection systems should protect against every possible electronic method of entry
- But what if an attacker gains access to the server room or network wiring closet ...
- Is you network still safe?

Destructive vs. Nondestructive Entry

- Destructive entry
  - Involves using force to defeat physical security
  - Methods involve crowbars, bolt cutters and sledge hammers
  - Negative impact on IT resources is apparent
  - Remediation steps also obvious
- Nondestructive entry
  - Compromises security without leaving signs of a breach
  - Defeats intrusion detection
  - Greater and long-term threat

Compromising Locks

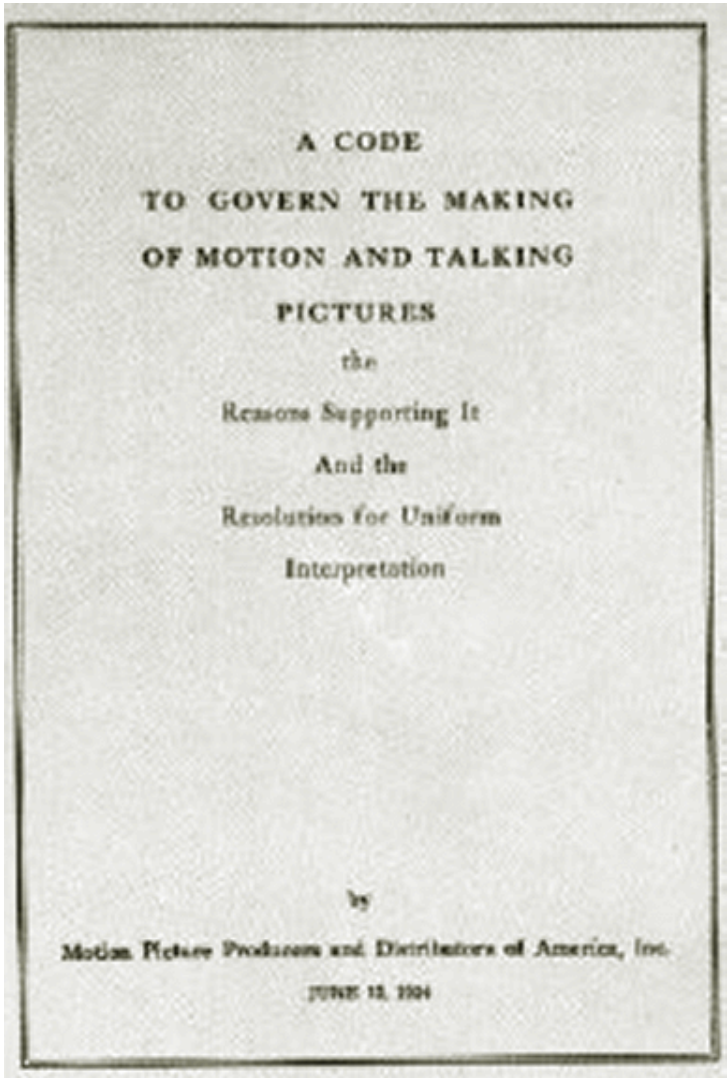
- For centuries, the lock has been one of the cornerstones of physical security
  - We rely on dozens of them every day to protect people and assets
- The trust most people place in locks is unwarranted
  - Most locks can be easily compromised with nondestructive methods
  - Sometimes within seconds and with readily available tools
- “Locks keep honest people honest”

Lock Picking

- Lock picking had been the exclusive art of locksmiths, professional thieves, spies and magicians for hundreds of years
- However, with the advent of the Internet, information about lock picking methods and tools has become readily available
  - E.g., YouTube has many lock picking videos

Lock Picking in Movies

- Genuine lock picking in movies used to be prohibited
- Before 1967, the Hays code (Motion Picture Production Code) required censorship of Hollywood movies
  - "All detailed (that is, imitable) depiction of crime must be removed, such as lock picking or mixing of chemicals to make explosives"


A CODE
TO GOVERN THE MAKING
OF MOTION AND TALKING
PICTURES
the
Reasons Supporting It
And the
Resolutions for Uniform
Interpretation
by
Motion Picture Producers and Distributors of America, Inc.
JUNE 13, 1934

Public domain image from http://commons.wikimedia.org/wiki/File:Motion_Picture_Production_Code.gif

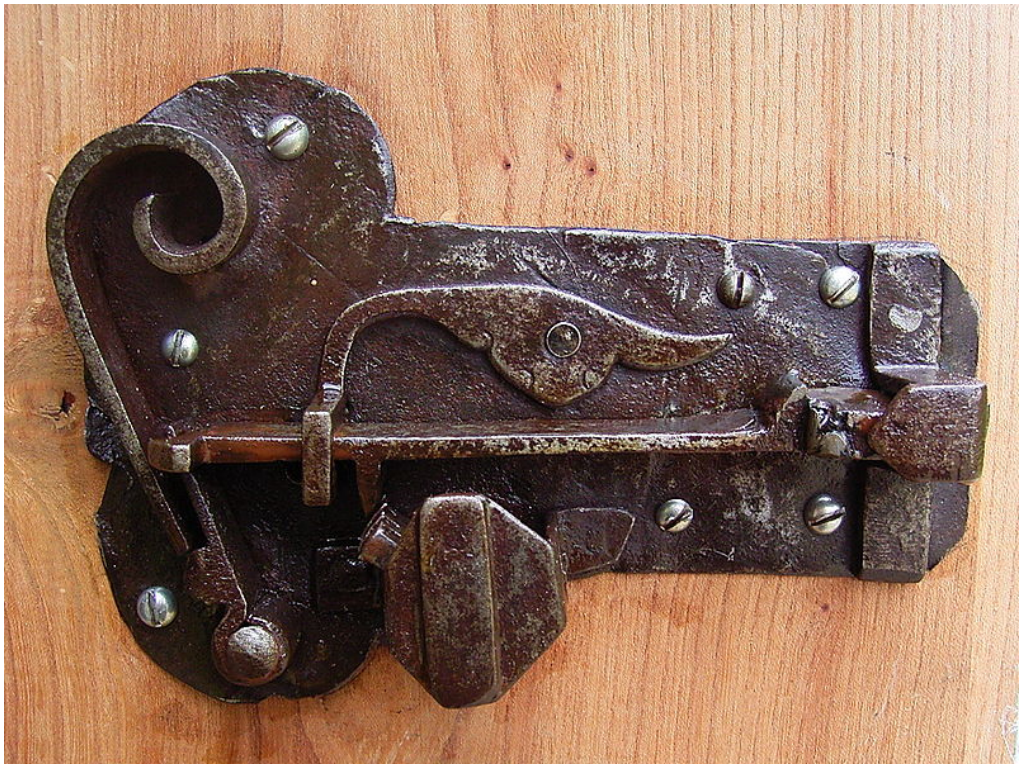


Image from http://commons.wikimedia.org/wiki/File:Ancient_warded_lock_open.jpg used with permission under Gnu Free Documentation License 1.2

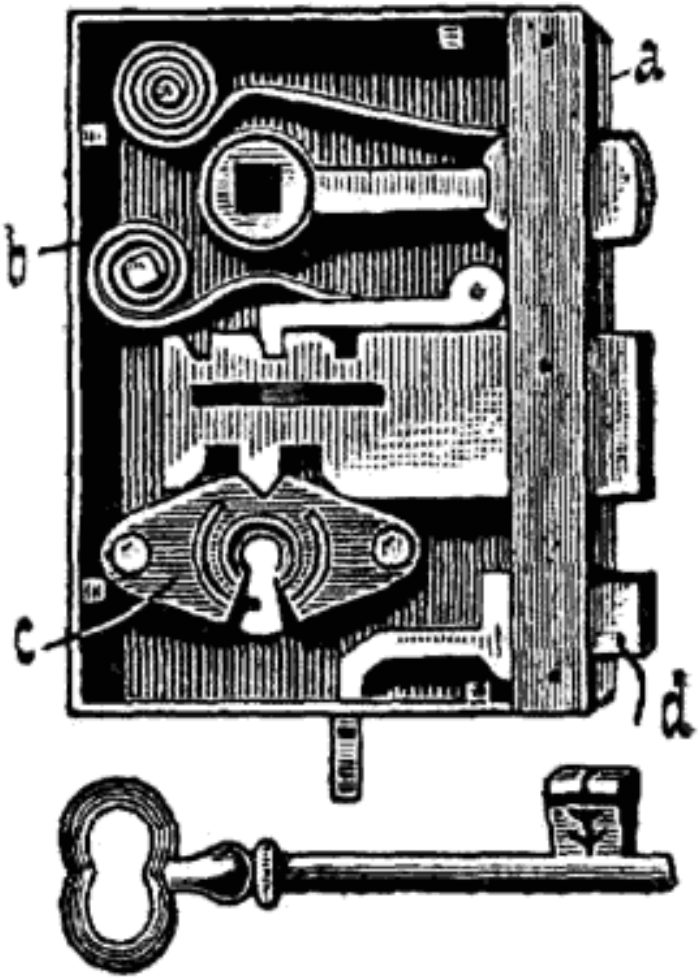
TSA Lock

- The U.S. government has established a set of rules for the inspection of baggage without the presence of passengers
- Special TSA-approved locks allow both inspection and protection against theft
- An important element is that the inspection must be easily verifiable by the user

Public domain government image

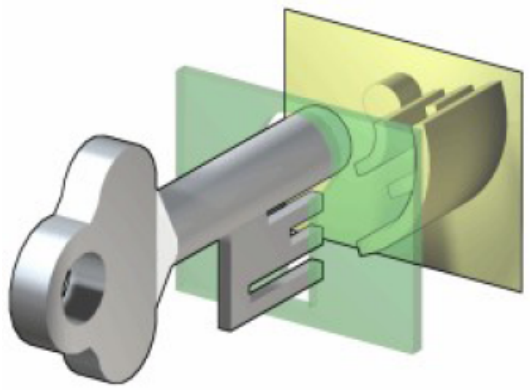
Warded Locks

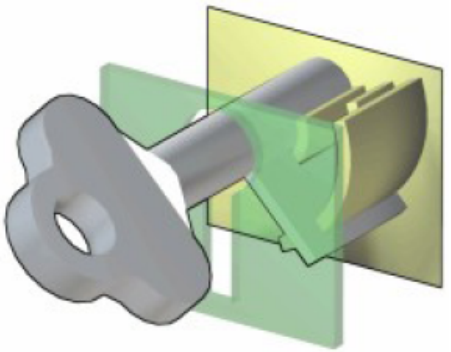
- Locks of this type were used in ancient times
- The key moves the bolt assisted by a support spring
- Security relies on the fact that not all keys pass through the key hole



Skeleton Key

- Usually in old style doors or desks
- Different concentric obstructions
- Easy to lock pick with Skeleton keys
- They come from ancient Rome





Pick vs. Bypass

Break open a lock in a nondestructive manner can be achieved either through:

- Pick: acting on the lock mechanism simulating the operation of the key
- Bypass: manipulation of the bolt without using the lock

1860: Yale Pin Tumbler Lock

Public domain image of Linus Yale, Jr.

- Modern version of the Egyptian single-pin design
- Utilizes two pins for locking
  - Double-detainer theory of locking
  - Created shear line

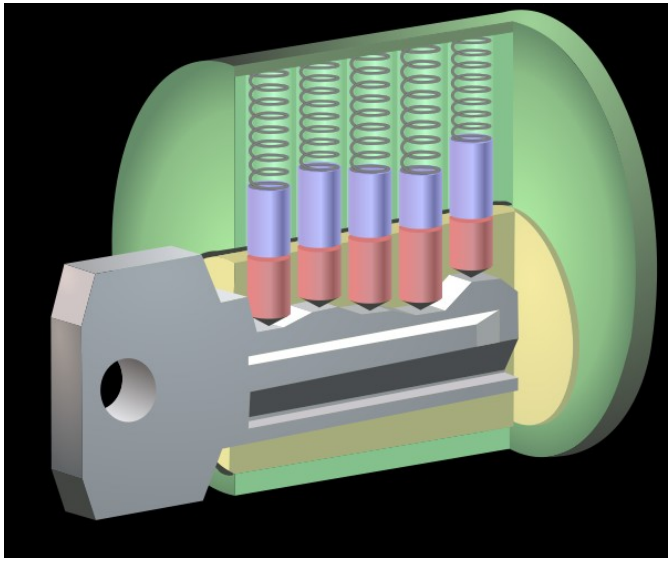
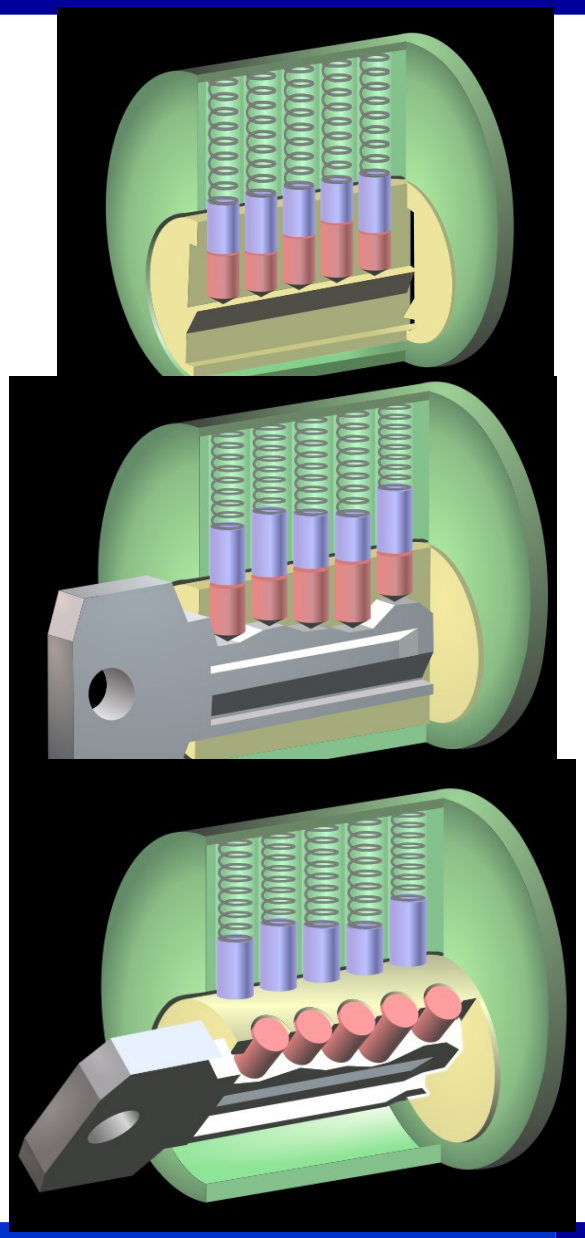


Image from http://en.wikipedia.org/wiki/File:Pin_tumbler_with_key.svg used with permission under Gnu Free Documentation License 1.2

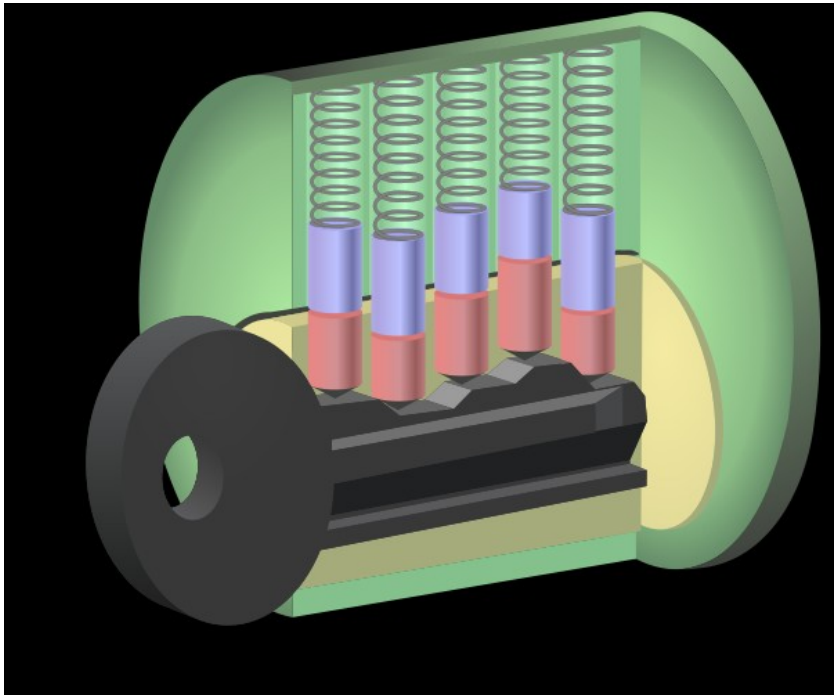
How Does a Pin Tumbler Lock Work?

1. When a key is not present, the pin stacks are pushed down by the springs so that the driver (top) pins span the plug and the outer casing, preventing the plug from rotating.
2. When the correct key is inserted, the ridges of the key push up the pin stacks so that the cuts of the pin stacks are aligned with the shear line.
3. The alignment of the cuts with the shear line allows the plug to be rotated.



How Does a Pin Tumbler Lock Work?

- If an inappropriate key is insered, then the pins do not align along the shear line and the lock does not turn.



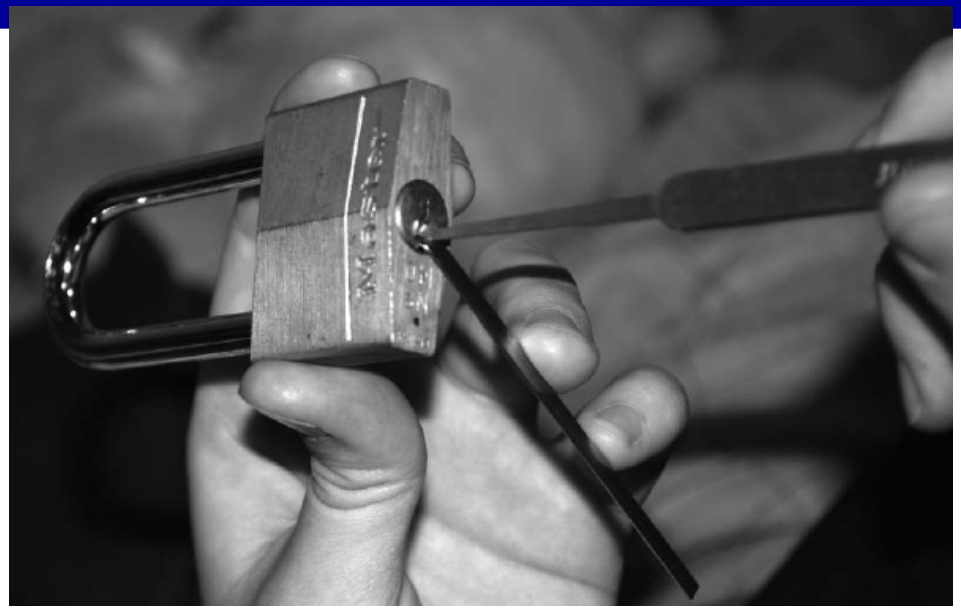


Photo by Dan Rosenberg included with permission.

Terminology

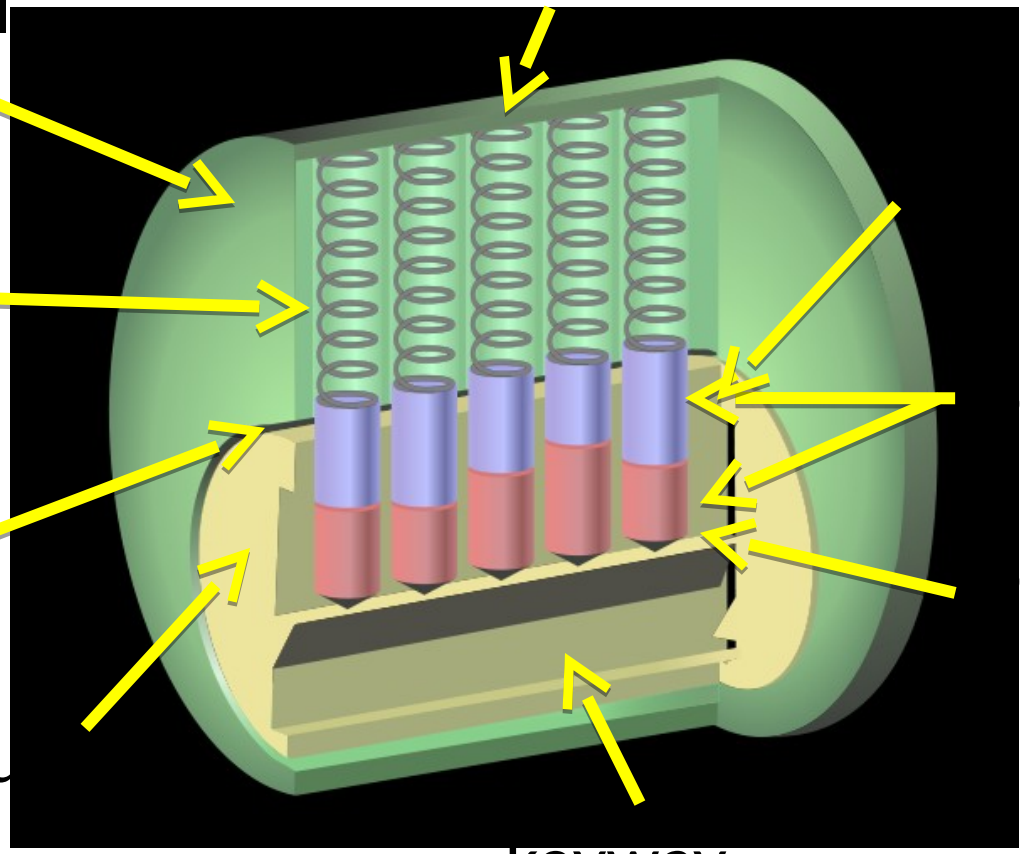


Image from http://en.wikipedia.org/wiki/File:Pin_tumbler_with_key.svg used with permission under Gnu Free Documentation License 1.2

Lockpicking Tools

- Feelers
- Scrubbers
- Tension tools

Photo by Jennie Rogers included with permission.

Feeler Picking

- Apply light tension
- Lift one pin at a time
  - Identify binding pin
- Lift binding pin until it reaches the shear line
- Setting the binding pin will rotate the lock slightly
- Find next pin and repeat the process

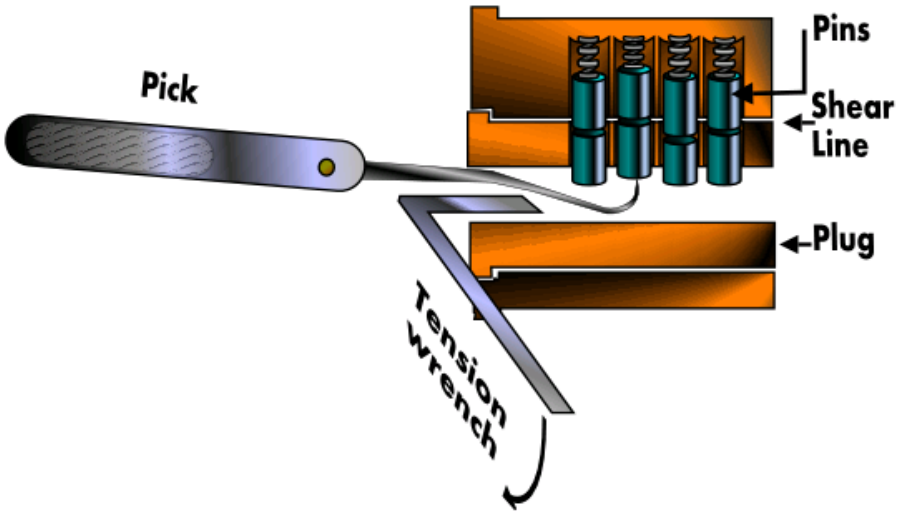


Image from http://commons.wikimedia.org/wiki/File:Pin_and_tumbler_lock_picking.PNG used with permission under Gnu Free Documentation License 1.2

Scrubbing / Raking

- Apply light tension
- Work over pins back to front in a circular motion
  - attempting to pop them into the shear line with the combination of tension
- Good for beginners
- Usually employ snake pick or half diamond

Photo by Jennie Rogers included with permission.

The Math of Lock Picking

- Suppose we have
  - 40 different kinds of key blanks
  - 7 pin positions
  - 8 different possible pin heights
- Then the total number of possible locks is
  - $40 \times 8^7 = 83{,}886{,}080$
- Not all these are possible, however, as it is difficult to put long teeth next to small teeth.

Rights Amplification in Master Keyed Systems

Reverse engineer master key from change key

Each lock has P pins, with D potential cut heights

Create D-1 test keys for each pin position *p*

Cut all pin positions except *p* as known change key

Published by Matt Blaze at Penn

Rights Amplification (continued)

Query the lock until you find each pin position

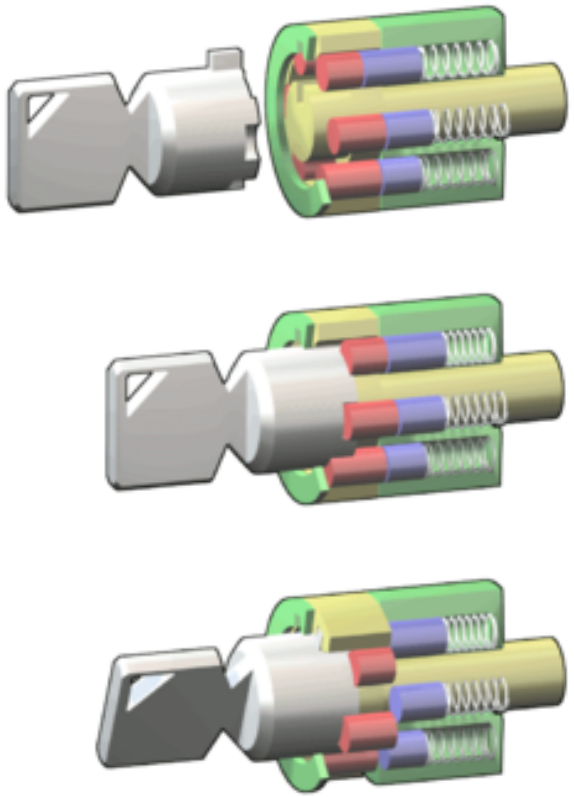
- i.e. To determine first key cut depth insert each of the D-1 test keys and determine which one does not bind to the pin
- Repeat for each pin

Rights Amplification Statistics

- Consumes P(D-1) blanks
- Can reduce to P blanks and file down on the fly
  - But this looks suspicious
- Search space is practically pruned by manufacturer specs
  - Maximum distance limit in legal adjacent cuts
  - Older installations sometimes require MKs to be higher on the pin stack

Tubular lock

- Usually on car alarms or vending machines
- 6-8 pins
- Easy to pick with special tool
- The tool could become a new key

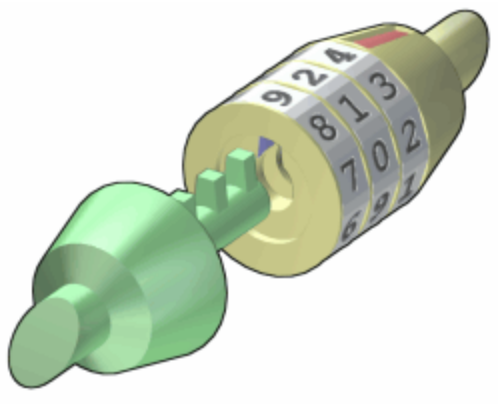


Statistics

- 4-6 pins, 4-10 levels
- $10^6 = 1{,}000{,}000$ possible keys!
- The angular positions of the cylinders allow to obtain about 180 different positions $(180 \cdot 10)^6 = 3.4012224 \times 10^{19}$
- (Un) fortunately there is a need for some tolerance in locks

Combination Locks

- There are locks that do not require a physical key to be opened but a code
- Number of combinations is
  - Number of digits
    times
  - Length of combination



Images from http://en.wikipedia.org/wiki/File:Combination_unlocked.png and http://commons.wikimedia.org/wiki/File:Electronic_lock_yl88.jpg used with permission under Gnu Free Documentation License 1.2

Combination Locks

- Inexpensive combination padlocks allow attacks based on reducing the space of possible combinations to try
  - The gears have a higher tolerance of the external disk combination
  - Nominal number of combinations is $40^3 = 64{,}000$
  - Possibilities can be reduced to about 80 by detecting critical gear points

Public domain image from http://commons.wikimedia.org/wiki/File:Lock.JPG

E.g., see http://www.wikihow.com/Crack-a-%22Master-Lock%22-Combination-Lock

Bumping

- A different way of picking locks
- Virtually all traditional Yale and similar locks can be opened by bumping
- What lock pickers say about bumping:
  - RELIABLE
  - REPEATABLE
  - SIMPLE TO LEARN

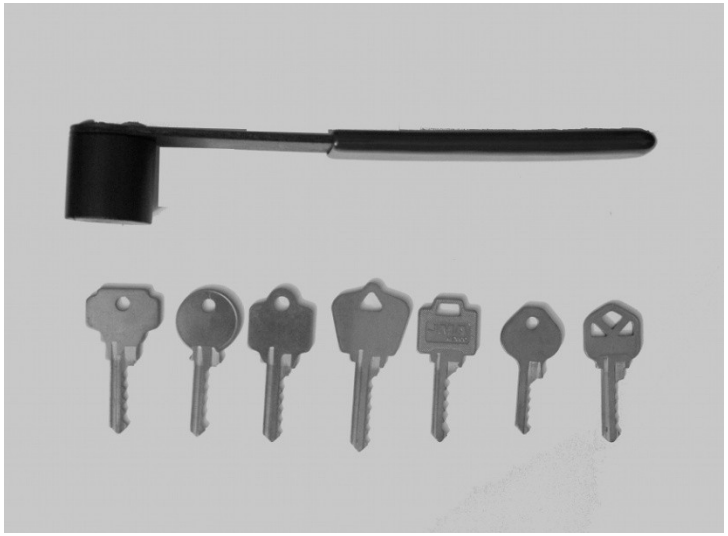


Photo by Jennie Rogers included with permission.

Bump Keys

- Driver pins “jump” higher than the cylinder just for an instant
- If a light rotational force is applied, the cylinder will turn
- Lock bumping is a very fast method for opening the lock
- The lock is not damaged in any way
- Few key-pin locks cannot be bumped

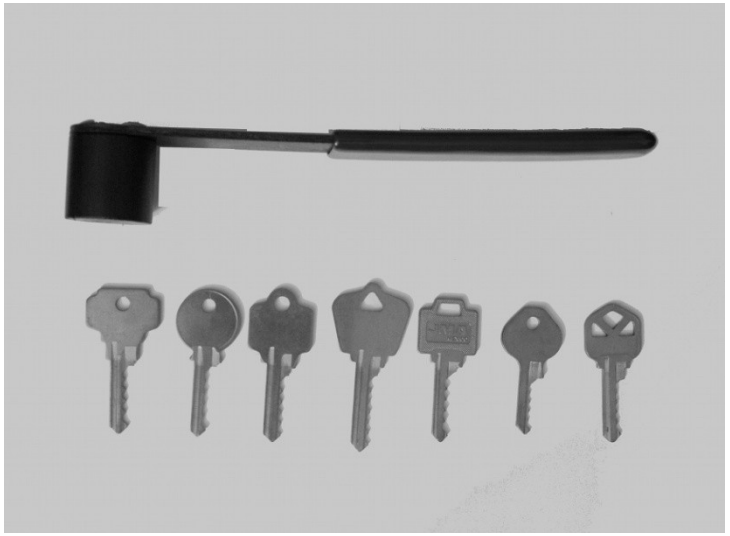


Photo by Jennie Rogers included with permission.

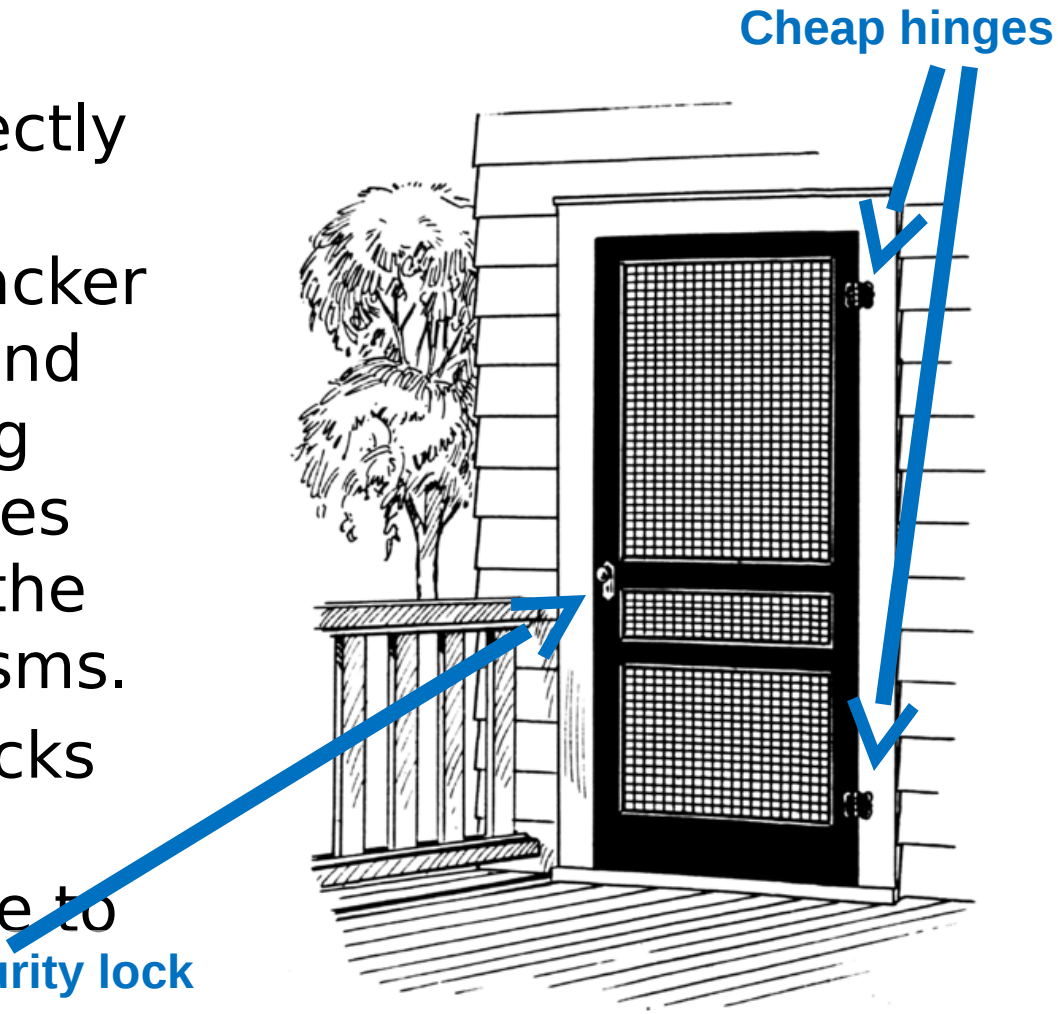
Pick Gun

- Manual and electronic pick guns are a popular method for quick and easy ways of opening up doors
- The pick gun is used in a similar way but usually has a trigger that creates an upward movement that must be repeated rapidly to open the lock

Public domain image from http://en.wikipedia.org/wiki/File:IDET2007_lock_picking_device.jpg

Side Channel Attacks

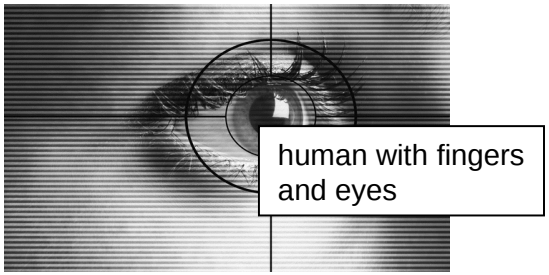
- Rather than attempting to directly bypass security measures, an attacker instead goes around them by exploiting other vulnerabilities not protected by the security mechanisms.
- Side channel attacks are sometimes surprisingly simple to perform.



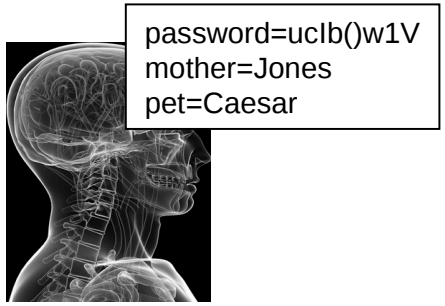
Public domain image by Pearson Scott Foresman from http://en.wikipedia.org/wiki/File:Screen2_%28PSF%29.png

Authentication

- The determination of **identity**, usually based on a combination of
  - something the person has (like a smart card or a radio key fob storing secret keys),
  - something the person knows (like a password),
  - something the person is (like a human with a fingerprint).



Something you are



Something you know

Something you have

Barcodes

- Developed in the 20th century to improve efficiency in grocery checkout.
- First-generation barcodes represent data as a series of **variable-width, vertical lines** of ink, which is essentially a one-dimensional encoding scheme.
- Some more recent barcodes are rendered as **two-dimensional patterns** using dots, squares, or other symbols that can be read by specialized optical scanners, which translate a specific type of barcode into its encoded information.

Authentication via Barcodes

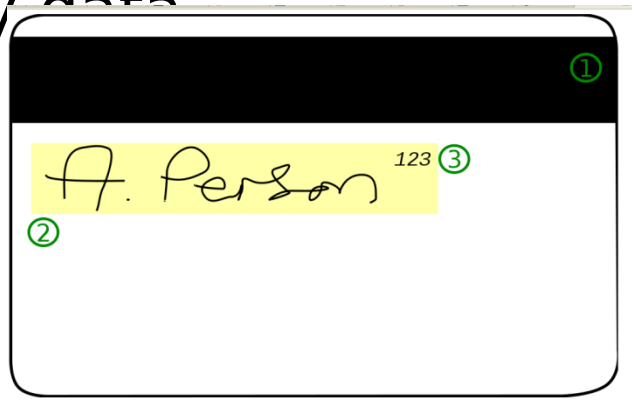
- Since 2005, the airline industry has been incorporating two-dimensional barcodes into boarding passes, which are created at flight check-in and scanned before boarding.
- In most cases, the barcode is encoded with an internal unique identifier that allows airport security to look up the corresponding passenger's record with that airline.
- Staff then verifies that the boarding pass was in fact purchased in that person's name (using the airline's database), and that the person can provide photo identification.
- In most other applications, however, barcodes provide convenience but not security. Since barcodes are simply images, they ar

Two-dimensional barcode

Public domain image from http://commons.wikimedia.org/wiki/File:Bpass.jpg

Magnetic Stripe Cards

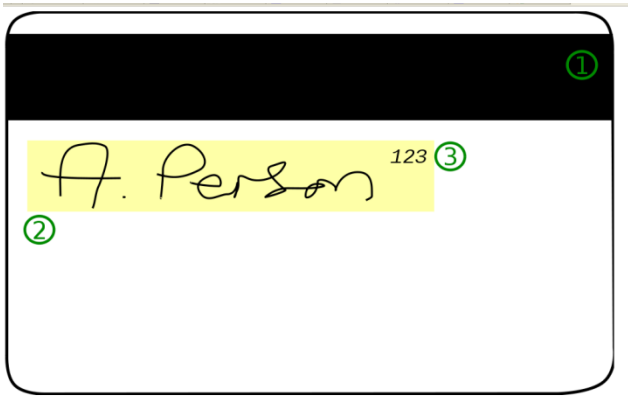
- Plastic card with a magnetic stripe containing personalized information about the card holder.
- The first track of a magnetic stripe card contains the cardholder's full name in addition to an account number, format information, and other data.
- The second track may contain the account number, expiration date, information about the issuing bank, data specifying the exact format of the track, and other discretionary data.



Public domain image by *Alexander Jones* from http://commons.wikimedia.org/wiki/File:CCardBack.svg

Magnetic Stripe Card Security

- One vulnerability of the magnetic stripe medium is that it is easy to read and reproduce.
- Magnetic stripe readers can be purchased at relatively low cost, allowing attackers to read information off cards.
- When coupled with a magnetic stripe writer, which is only a little more expensive, an attacker can easily clone existing cards.
- So, many uses require card holders to enter a PIN to use their cards (e.g., as in ATM and debit cards in the U.S.).



Public domain image by *Alexander Jones* from http://commons.wikimedia.org/wiki/File:CCardBack.svg

Smart Cards

- **Smart cards** incorporate an integrated circuit, optionally with an on-board microprocessor, which microprocessor features reading and writing capabilities, allowing the data on the card to be both accessed and altered.
- Smart card technology can provide secure authentication mechanisms that protect the information of the owner and are extremely difficult to duplicate.

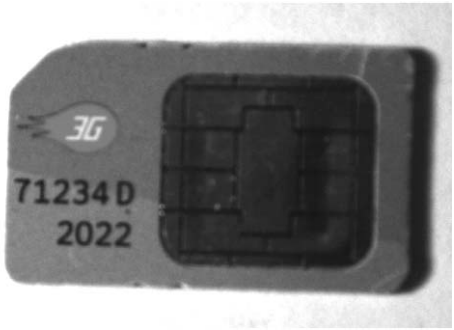
Public domain image from http://en.wikipedia.org/wiki/File:Carte_vitale_anonyme.jpg

Smart Card Authentication

- They are commonly employed by large companies and organizations as a means of strong authentication using cryptography.
- Smart cards may also be used as a sort of “electronic wallet,” containing funds that can be used for a variety of services, including parking fees, public transport, and other small retail transactions.

SIM Cards

- Many mobile phones use a special smart card called a **subscriber identity module card (SIM card).**
- A SIM card is issued by a network provider. It maintains personal and contact information for a user and allows the user to authenticate to the cellular network of the provider.

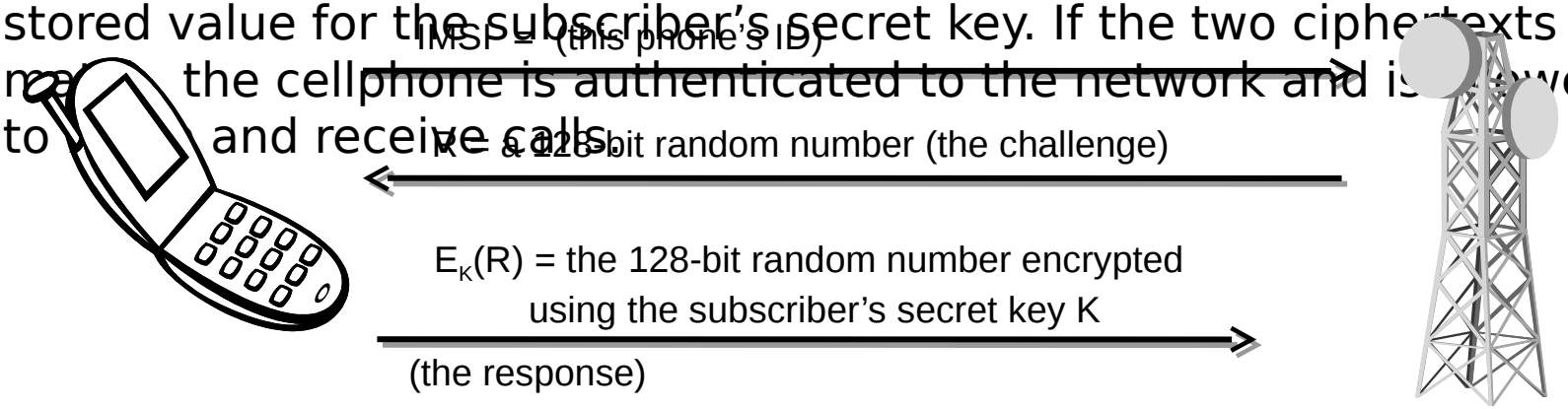


SIM Card Security

- SIM cards contain several pieces of information that are used to identify the owner and authenticate to the appropriate cell network.
- Each SIM card corresponds to a record in the database of subscribers maintained by the network provider.
- A SIM card features an **integrated circuit card ID (ICCID),**
- which is a unique 18-digit number used for hardware identification.
- Next, a SIM card contains a unique **international mobile subscriber identity** (**IMSI),** which identifies the owner's country, network, and personal identity.
- SIM cards also contain a 128-bit **secret key.** This key is used for authenticating a phone to a mobile network.
- As an additional security mechanism, many SIM cards require a PIN before allowing any access to information on the card.

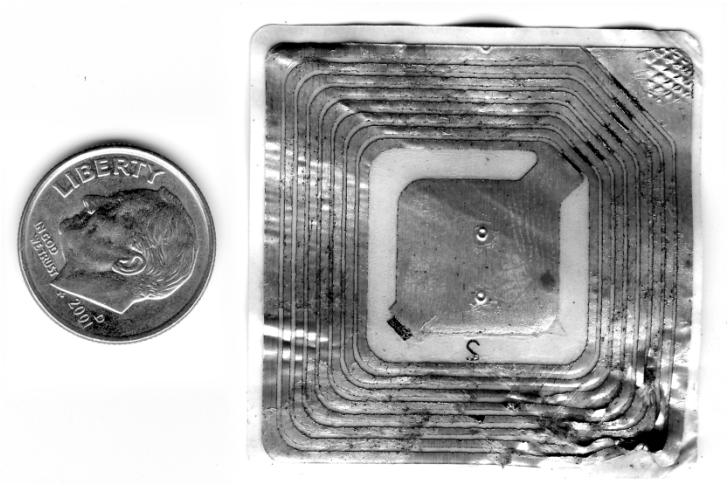
GSM Challenge-Response Protocol

1. When a cellphone wishes to join a cellular network it connects to a local **base station** owned by the network provider and transmits its IMSI.
2. If the IMSI matches a subscriber's record in the network provider's database, the base station transmits a 128-bit random number to the cellphone.
3. This random number is then encoded by the cellphone with the subscriber's secret key stored in the SIM card using a proprietary encryption algorithm known as **A3,** resulting in a ciphertext that is sent back to the base station**.**
4. The base station then performs the same computation, using its stored value for the subscriber's secret key. If the two ciphertexts match, the cellphone is authenticated to the network and is allowed to [illegible] and receive calls.



RFIDs

- **Radio frequency identification, or RFID,** is a rapidly emerging technology that relies on small transponders to transmit identification information via radio waves.
- RFID chips feature an integrated circuit for storing information, and a coiled antenna to transmit and receive a radio signal.



RFID Technology

- RFID tags must be used in conjunction with a separate reader or writer.
- While some RFID tags require a battery, many are passive and do not.
- The effective range of RFID varies from a few centimeters to several meters, but in most cases, since data is transmitted via radio waves, it is not necessary for a tag to be in the line of sight of the reader.

RFID Technology

- This technology is being deployed in a wide variety of applications.
- Many vendors are incorporating RFID for consumer-product tracking.
- Car key fobs.
- Electronic toll transponders.

Passports

- Modern passports of several countries, including the United States, feature an embedded RFID chip that contains information about the owner, including a digital facial photograph that allows airport officials to compare the passport's owner to the person who is carrying the passport.

Passport Security

- In order to protect the sensitive information on a passport, all RFID communications are encrypted with a **secret key.**
- In many instances, however, this secret key is merely the passport number, the holder's date of birth, and the expiration date, in that order.
  - All of this information is printed on the card, either in text or using a barcode or other optical storage method.
  - While this secret key is intended to be only accessible to those with physical access to the passport, an attacker with information on the owner, including when their passport was issued, may be able to easily reconstruct this key, especially since passport numbers are typically issued sequentially.

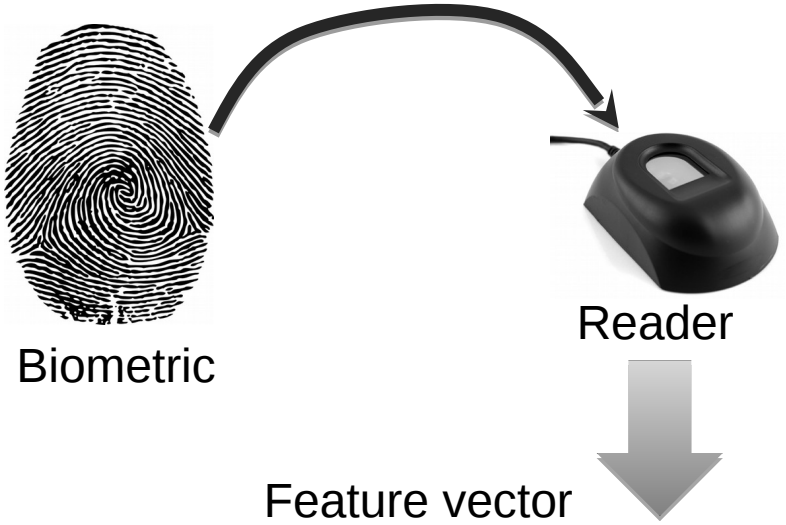
Biometrics

- **Biometric** refers to any measure used to uniquely identify a person based on biological or physiological traits.
- Generally, biometric systems incorporate some sort of sensor or scanner to read in biometric information and then compare this information to stored templates of accepted users before granting access.

Requirements for Biometric

- **Universality.** Almost every person should have this characteristic.
- **Distinctiveness.** Each person should have noticeable differences in the characteristic.
- **Permanence.** The characteristic should not change significantly over time.
- **Collectability.** The characteristic should have the ability to be effectively determined and quantified.

Biometric Identification



Candidates for Biometric IDs

- Fingerprints
- Retinal/iris scans
- DNA
- “Blue-ink” signature
- Voice recognition
- Face recognition
- Gait recognition
- Let us consider how each of these scores in terms of universality, distinctiveness, permanence, and collectability…

Public domain image from
http://commons.wikimedia.org/wiki/File:Fingerprint_Arch.jpg

Public domain image from
http://commons.wikimedia.org/wiki/File:Retinal_scan_securimetrics.jpg

Public domain image from
http://commons.wikimedia.org/wiki/File:CBP_chemist_reads_a_DNA_profile.jpg

Direct Attacks on Computational Devices

Environmental Attacks

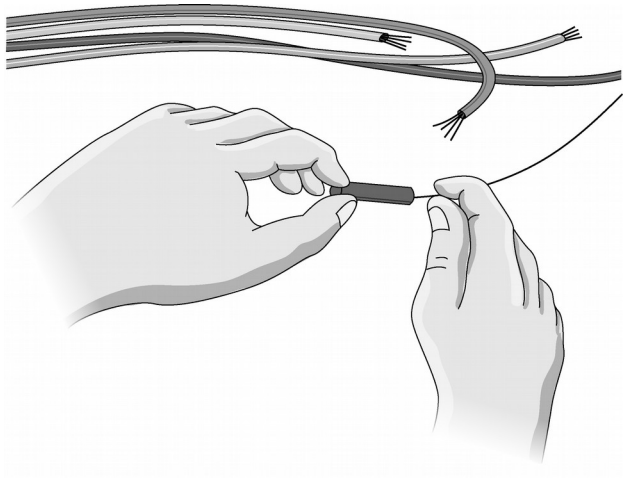
- **Electricity.** Computing equipment requires electricity to function; hence, it is vital that such equipment has a steady uninterrupted power supply.
- **Temperature.** Computer chips have a natural operating temperature and exceeding that temperature significantly can severely damage them.
- **Limited conductance.** Because computing equipment is electronic, it relies on there being limited conductance in its environment. If random parts of a computer are connected electronically, then that equipment could be damaged by a short circuit (e.g., in a flood).

Eavesdropping

- **Eavesdropping** is the process of secretly listening in on another person's conversation.
- Protection of sensitive information must go beyond computer security and extend to the **environment** in which this information is entered and read.
- Simple eavesdropping techniques include
  - Using social engineering to allow the attacker to read information over the victim's shoulder
  - Installing small cameras to capture the information as it is being read
  - Using binoculars to view a victim's monitor through an open window.
- These direct observation techniques are commonly referred to as **shoulder surfing.**

Wiretapping

- Many communication networks employ the use of inexpensive coaxial copper cables, where information is transmitted via electrical impulses that travel through the cables.
- Relatively inexpensive means exist that measure these impulses and can reconstruct the data being transferred through a tapped cable, allowing an attacker to eavesdrop on network traffic.
- These **wiretapping attacks** are passive, in that there is no alteration of the signal being transferred, making them extremely difficult to detect.

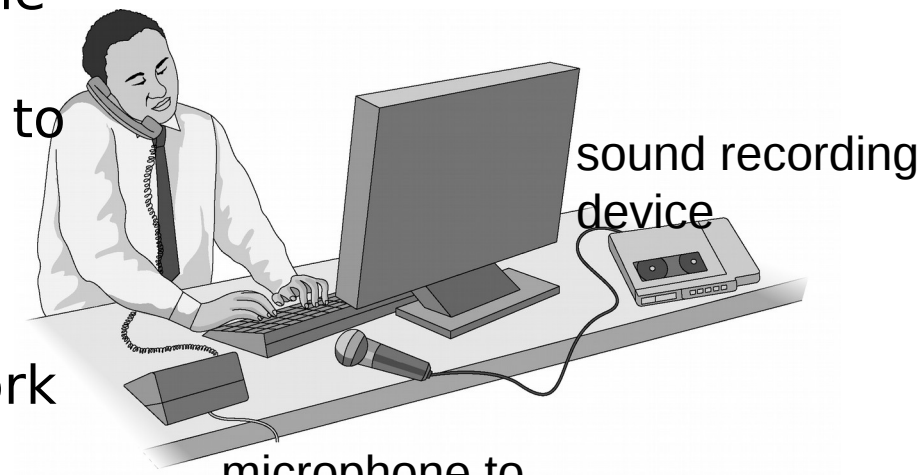


Signal Eminations

- Computer screens emit **radio frequencies** that can be used to detect what is being displayed.
- **Visible light** reflections can also be used to reconstruct a display from its reflection on a wall, coffee mug, or eyeglasses.
- Both of these require the attacker to have a receiver close enough to detect the signal.

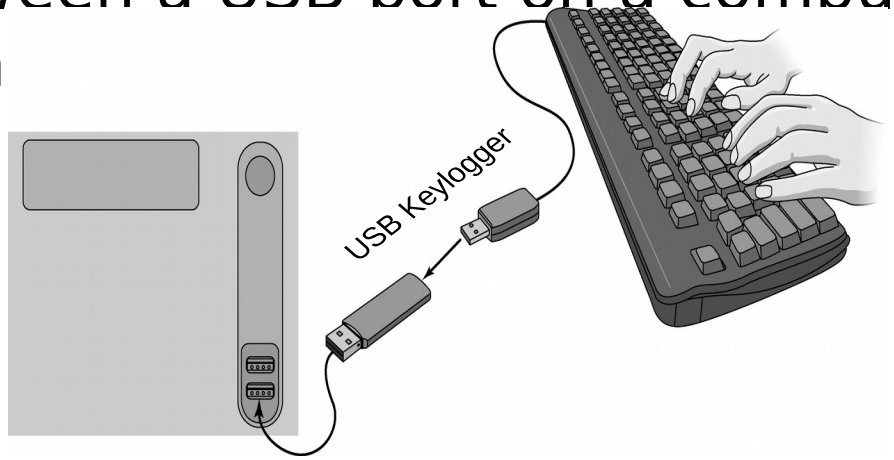
Acoustic Emissions

- Dmitri Asonov and Rakesh Agrawal published a paper in 2004 detailing how an attacker could use an audio recording of a user typing on a keyboard to reconstruct what was typed.
  - Each keystroke has minute differences in the sound it produces, and certain keys are known to be pressed more often than others.
  - After training an advanced neural network to recognize individual keys, their software recognized an average 79% of all keystrokes



Hardware Keyloggers

- A keylogger is any means of recording a victim's keystrokes, typically used to eavesdrop passwords or other sensitive information.
- Hardware keyloggers are typically small connectors that are installed between a keyboard and a computer.
- For example, a USB keylogger is a device containing male and female USB connectors, which allow it to be placed between a USB port on a computer and a USB cable com



TEMPEST

- **TEMPEST** is a U.S. government code word for a set of standards for limiting information-carrying electromagnetic emanations from computing equipment.
- TEMPEST establishes three zones or levels of protection:
  1. An attacker has almost direct contact with the equipment, such as in an adjacent room or within a meter of the device in the same room.
  2. An attacker can get no closer than 20 meters to the equipment or is blocked by a building to have an equivalent amount of attenuation.
  3. An attacker can get no closer than 100 meters to the equipment or is blocked by a building to have an equivalent amount of attenuation.

Emanation Blockage

- To block visible light emanations, we can enclose sensitive equipment in a windowless room.
- To block acoustic emanations, we can enclose sensitive equipment in a room lined with sound-dampening materials.
- To block electromagnetic emanations in the electrical cords and cables, we can make sure every such cord and cable is well grounded and insulated.

Faraday Cages

- To block electromagnetic emanations in the air, we can surround sensitive equipment with metallic conductive shielding or a mesh of such material, where the holes in the mesh are smaller than the wavelengths of the electromagnetic radiation we wish to block.
- Such an enclosure is

Computer Forensics

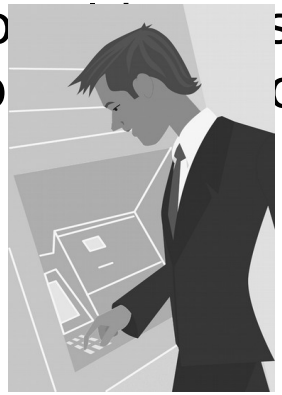
- **Computer forensics** is the practice of obtaining information contained on an electronic medium, such as computer systems, hard drives, and optical disks, usually for gathering evidence to be used in legal proceedings.
- Unfortunately, many of the advanced techniques used by forensic investigators for legal proceedings can also be employed by attackers to uncover sensitive information.

Computer Forensics

- Forensic analysis typically involves the physical inspection of the components of a computer, sometimes at the microscopic level, but it can also involve electronic inspection of a computer's parts as well.

ATMs

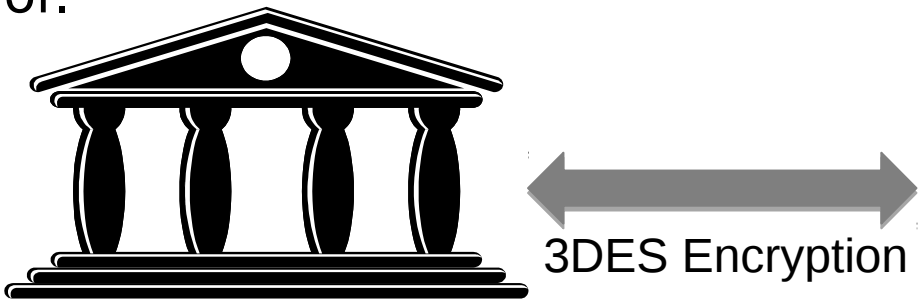
- An **automatic teller machine (ATM)** is any device that allows customers of financial institutions to complete withdrawal and deposit transactions without human assistance.
- Typically, customers insert a magnetic stripe credit or debit card, enter a PIN, and then deposit or withdraw cash from their account.
- The ATM has an internal cryptographic processor that encrypts the entered PIN and compares it to an encrypted PIN stored on the card (only fo stems that are not connected to a network) o ote database.



ATM

ATMs

- To ensure the confidentiality of customer transactions, each ATM has a cryptographic processor that encrypts all incoming and outgoing information, starting the moment a customer enters their PIN.
- The current industry standard for ATM transactions is the **Triple DES (3DES) cryptosystem,** a legacy symmetric cryptosystem with up to 112 bits of security.
- The 3DES secret keys installed on an ATM are either loaded on-site by technicians or downloaded remotely from the ATM vendor.



Bank

ATM

Attacks on ATMs

- **Lebanese loop:** A perpetrator inserts this sleeve into the card slot of an ATM. When a customer attempts to make a transaction and inserts their credit card, it sits in the sleeve, out of sight from the customer, who thinks that the machine has malfunctioned. After the customer leaves, the perpetrator can then remove the sleeve with the victim's card.
- **Skimmer:** a device that reads and stores magnetic stripe information when a card is swiped. An attacker can install a skimmer over the card slot of an ATM and store customers' credit information without their knowledge. Later, this information can be retrieved and used to make duplicates of the original cards.
- **Fake ATMs:** capture both credit/debit cards and PINs at the same time.