Chapter 2. Physical Security

CPSC 4620/5620

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?

Physical Security

- Is broadly defined as the use of physical measures to protect valuables, information or access to restricted resources.
  - Location protection: such as locks
  - Physical intrusion detection: detection of unauthorized access
  - Hardware attack: attack hard drives, network adapters, memory chips or microprocessors
  - Eavesdropping: attacks that monitor light, sound, radio, or other signals to detect communications or computations

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

2.2.1 Locks and safes

- Using a mechanical locking device to protect access to a building, vehicle, or container has been in use science ancient times.
- Used to protect the physical locations where computers and digital media are stored.

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

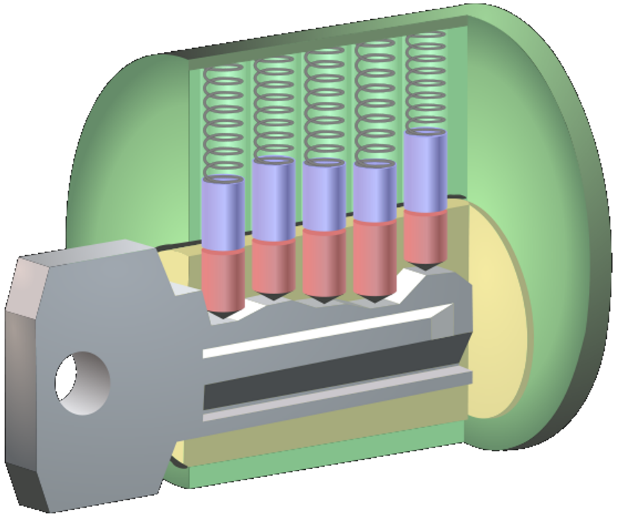
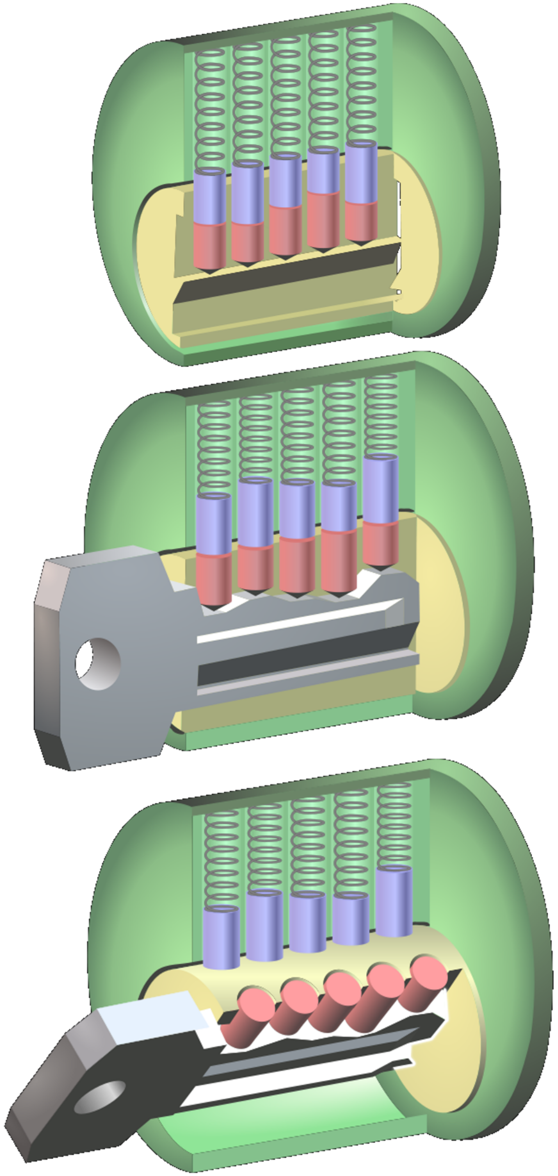


Image from http://en.wikipedia.org/wiki/File:Pin_tumbler_with_key.svg used with permission under Gnu Free Documentation License 1.2

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.



Images 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?

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

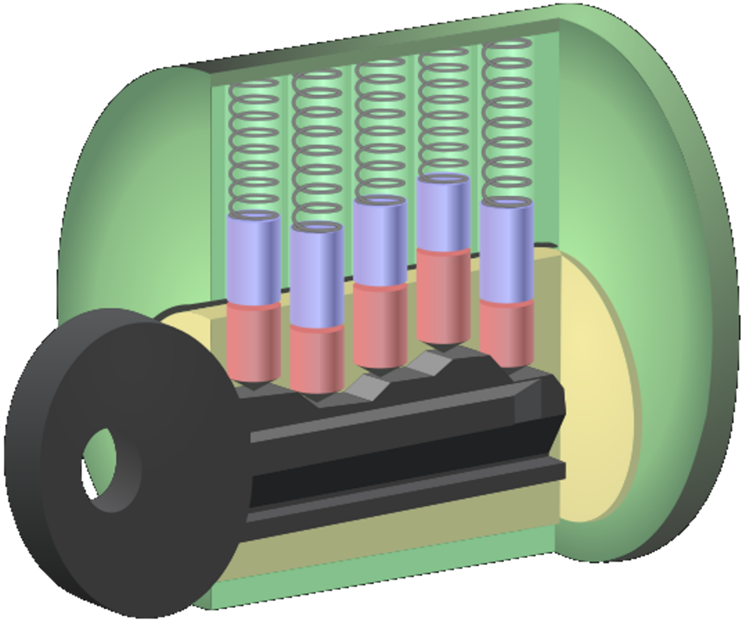
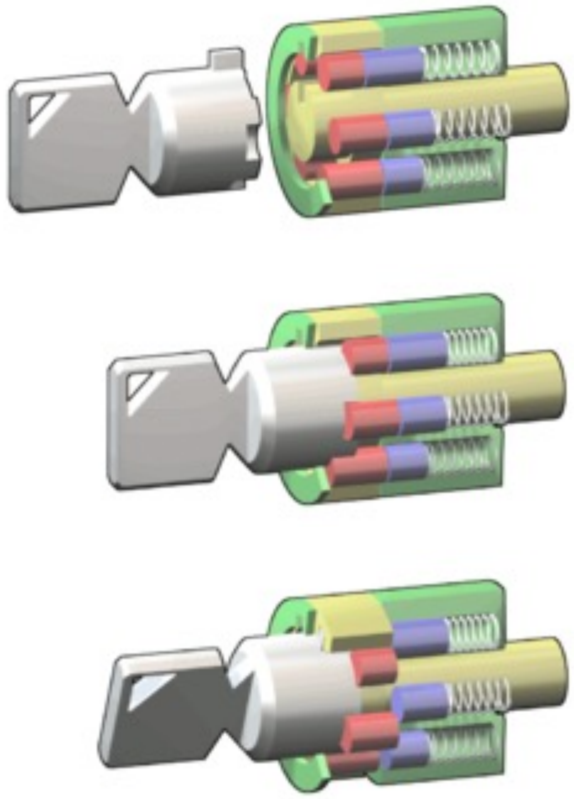


Image from http://en.wikipedia.org/wiki/File:Pin_tumbler_with_key.svg used with permission under Gnu Free Documentation License 1.2

Tubular lock

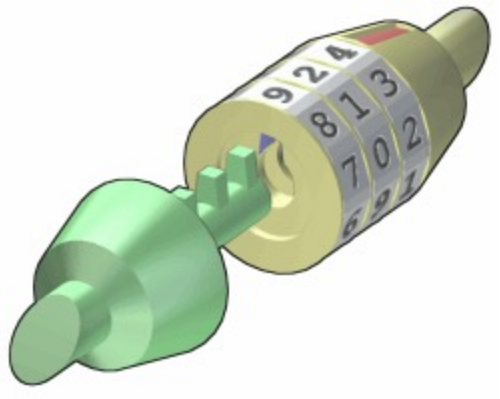
- Usually on car alarms or vending machines
- 6-8 pins
- Easy to pick with special tool
- The tool could become a new key



Images from http://en.wikipedia.org/wiki/File:Tubular_locked.png used with permission under Gnu Free Documentation License 1.2

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
  - 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

2.2.2 Attacks - 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

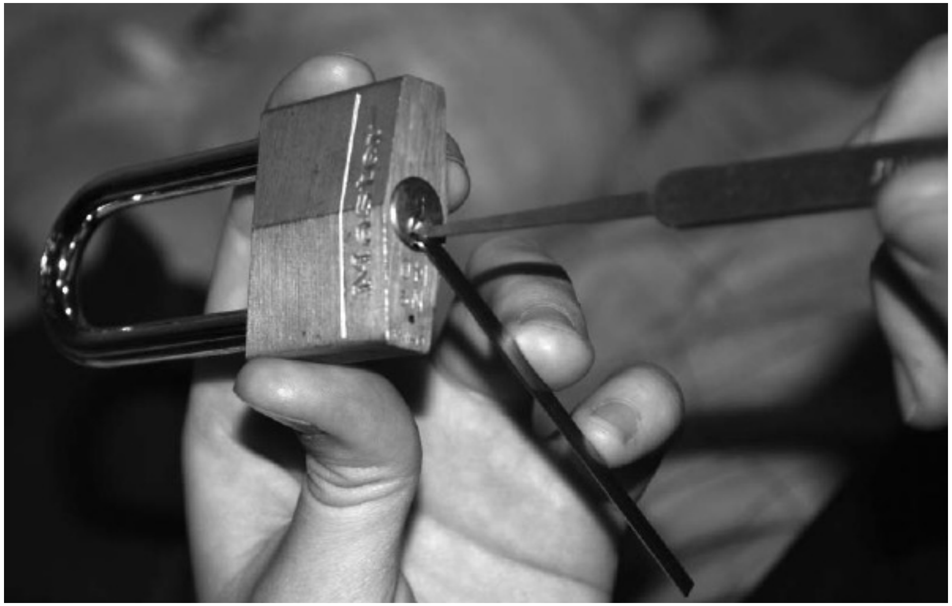


Photo by Dan Rosenberg included with permission.

LOCK PICKING

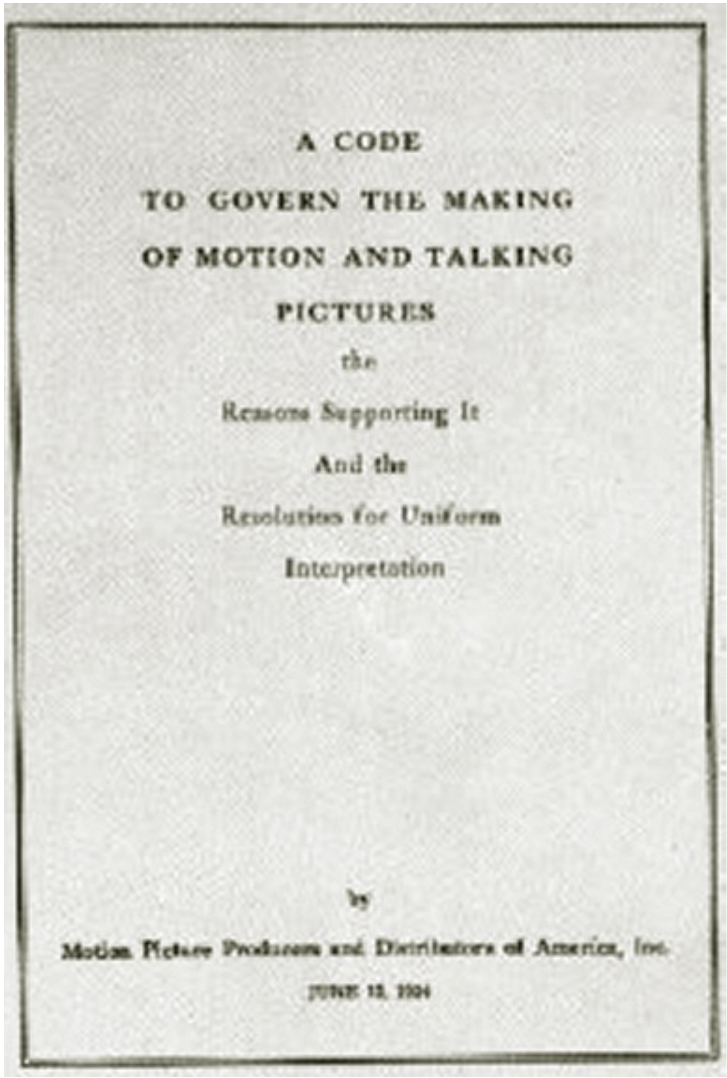
Legal Notice

- 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

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
Resolution 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

Lockpicking Tools

- Feelers
- Scrubbers
- Tension tools

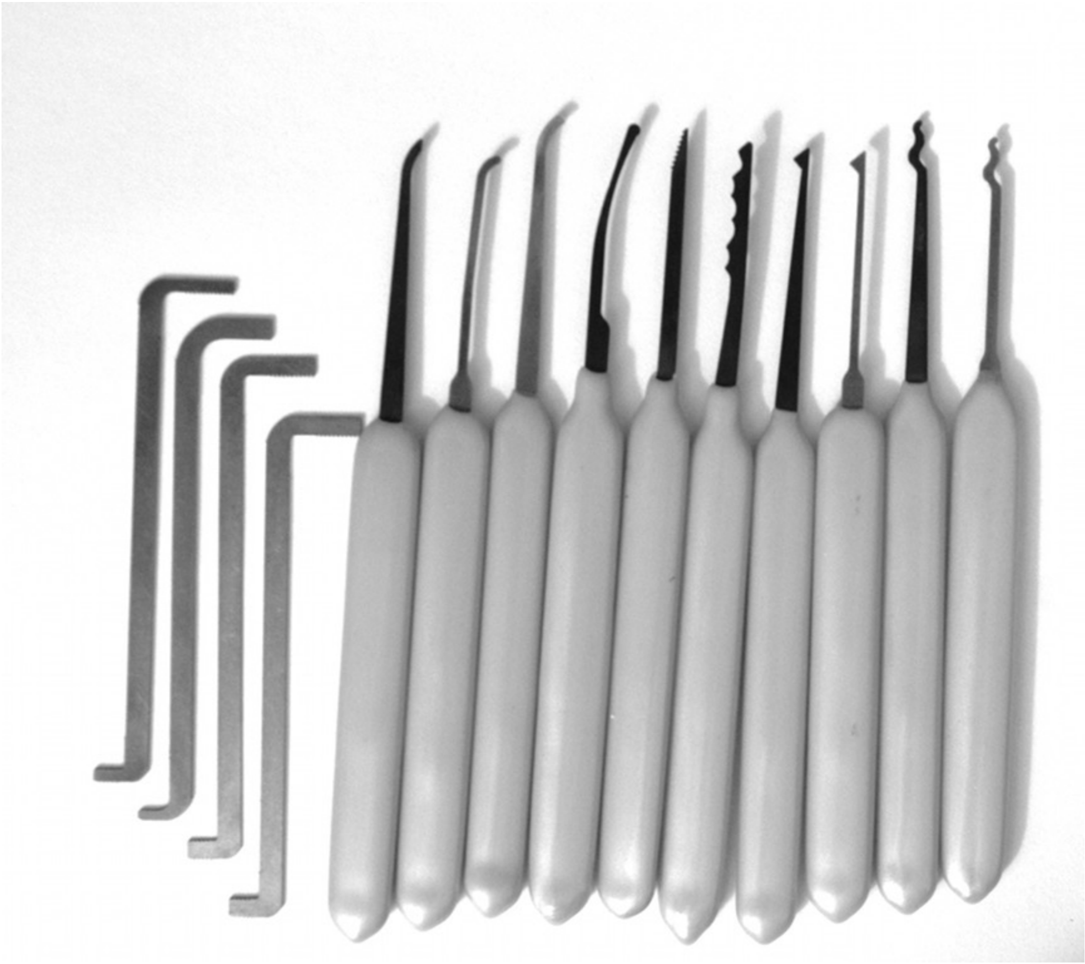


Photo by Jennie Rogers included with permission.

2.2.3 Protecting against brute-force attacks

- 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.

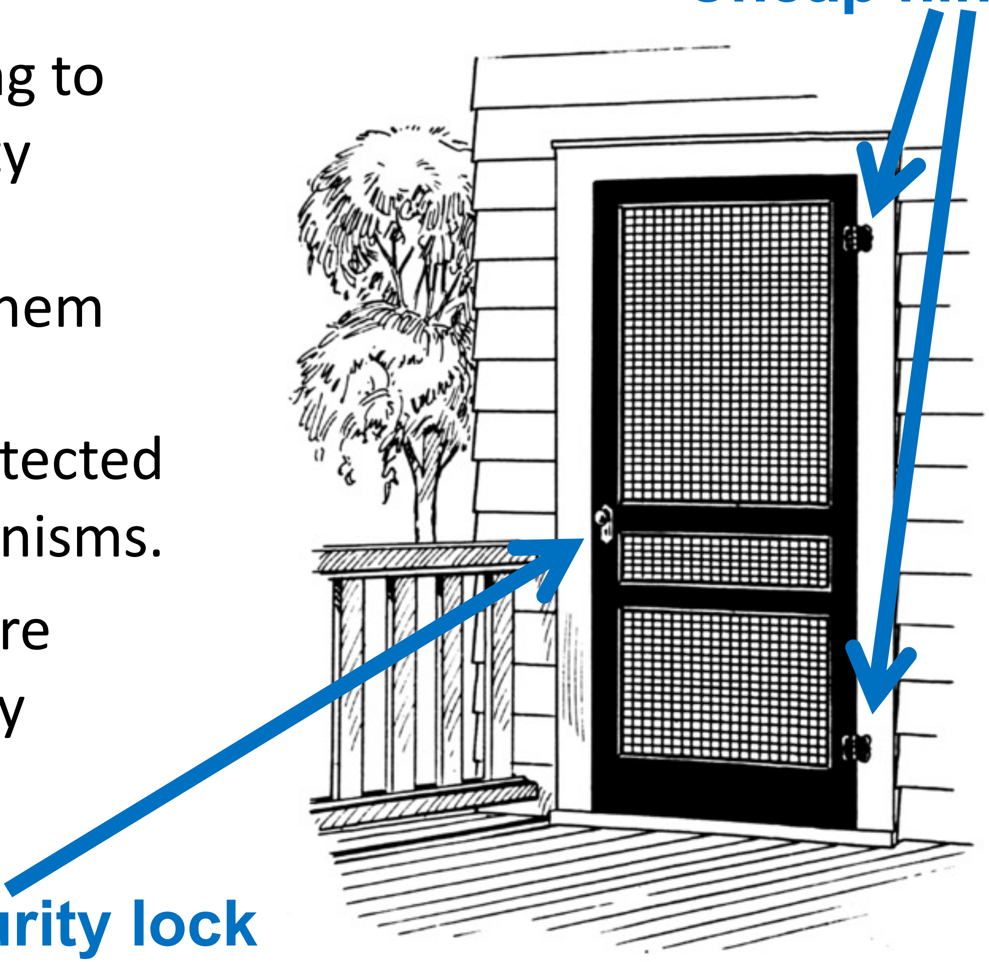
Pick vs. Bypass

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

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.



Cheap hinges

High security lock

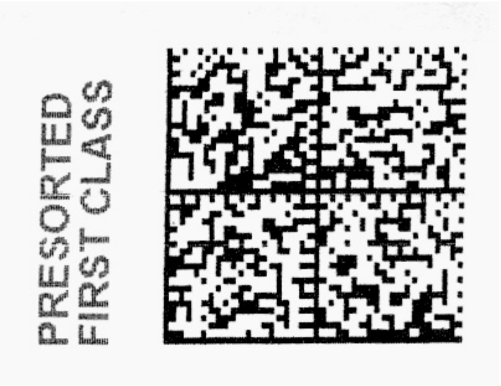
Public domain image by Pearson Scott Foresman from http://en.wikipedia.org/wiki/File:Screen2_%28PSF%29.png

2.3 Authentication

- The determination of **identity**, usually based on a combination of something the person has, something the person knows, and something the person is.
  - Barcodes
  - Magnetic stripe cards
  - Smart cards
  - RFIDs
  - biometrics

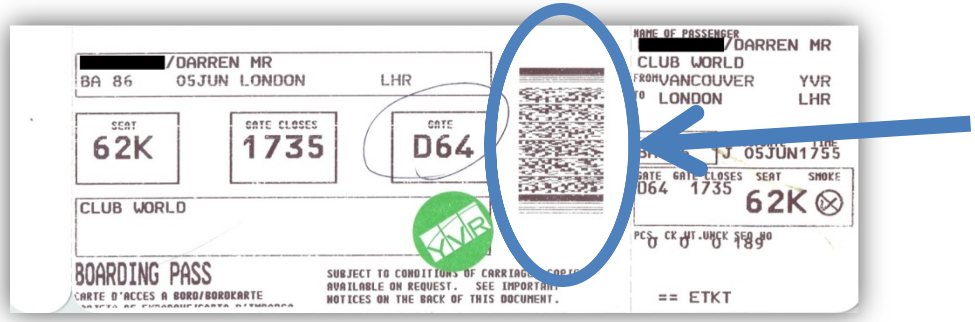
Barcodes

- 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

- Airlines use barcodes in boarding passes for flight check-in and boarding since 2005.
- Barcode is encoded as an internal unique identifier to look up passenger's record. 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.
- Provides more convenience than security because duplication is easy.



[redacted]/DARREN MR
BA 86 05JUN LONDON LHR

SEAT 62K
GATE CLOSES 1735
GATE D64

CLUB WORLD

BOARDING PASS
CARTE D'ACCES A BORD/BORDKARTE

SUBJECT TO CONDITIONS OF CARRIAGE
AVAILABLE ON REQUEST. SEE IMPORTANT
NOTICES ON THE BACK OF THIS DOCUMENT.

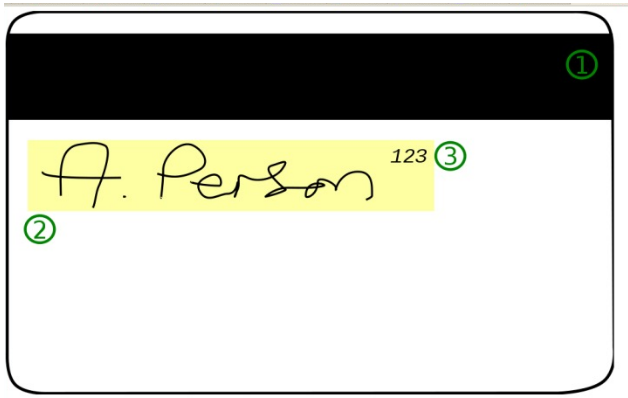
NAME OF PASSENGER
[redacted]/DARREN MR
CLUB WORLD
FROM VANCOUVER YVR
TO LONDON LHR
J 05JUN1755
GATE D64 GATE CLOSES 1735 SEAT 62K SMOKE ⊗
PCS 0 CK WT. 0 UNCK 0 SEQ NO 189
== ETKT

Two-dimensional barcode

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

Magnetic Stripe Cards

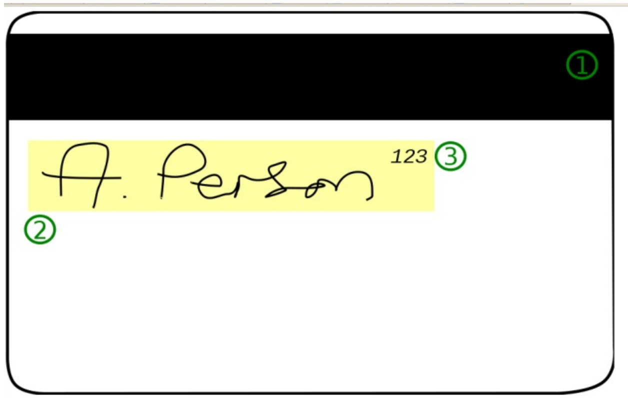
- Plastic card with a magnetic stripe containing personalized information about the card holder.
- The first track of a magnetic stripe card contains the cardholder's full name in addition to an account number, format information, and other data.
- The second track may contain the account number, expiration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

Circuit interface

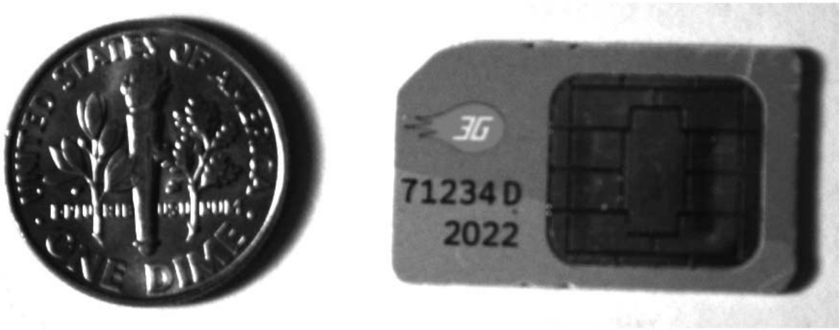
Public domain image from http://en.wikipedia.org/wiki/File:Carte_vitale_anonyme.jpg

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.

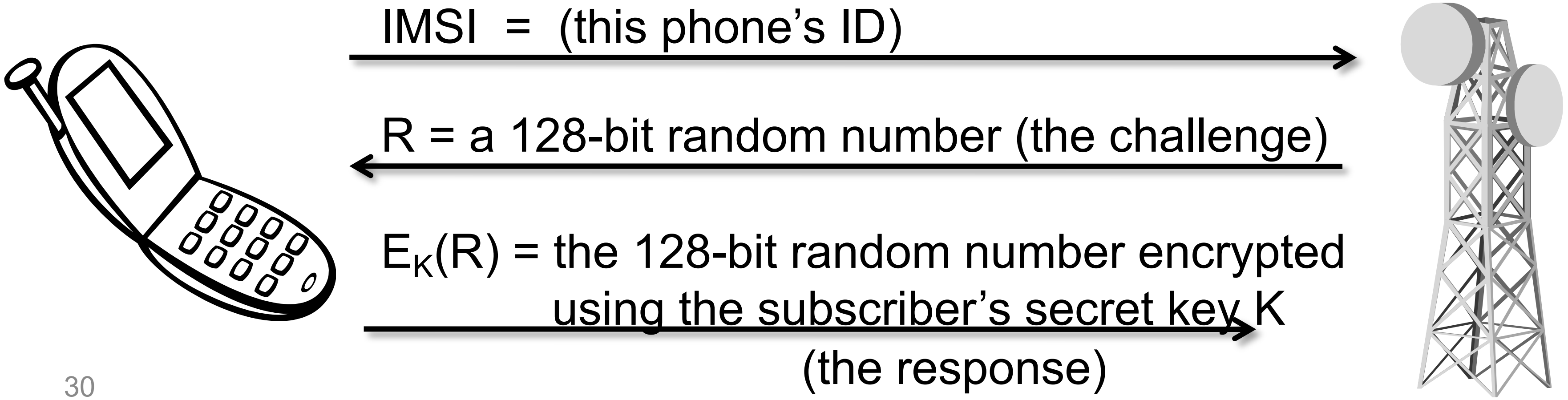


SIM Card Security

- 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 make and receive calls.



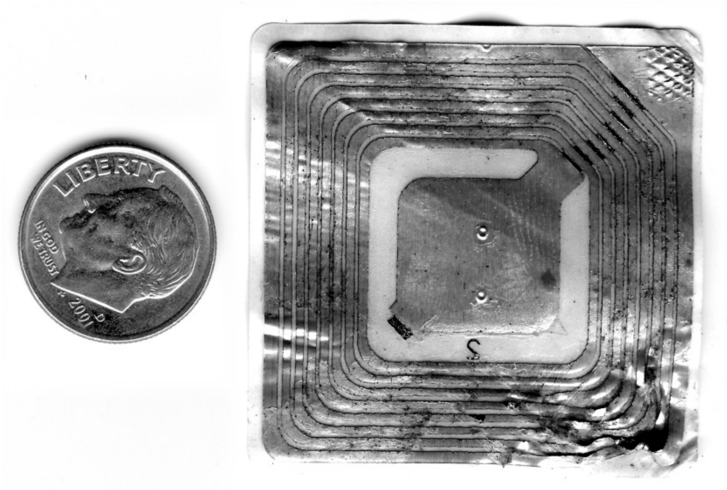
IMSI = (this phone's ID)

R = a 128-bit random number (the challenge)

$E_K(R)$ = the 128-bit random number encrypted using the subscriber's secret key K (the response)

2.3.4 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

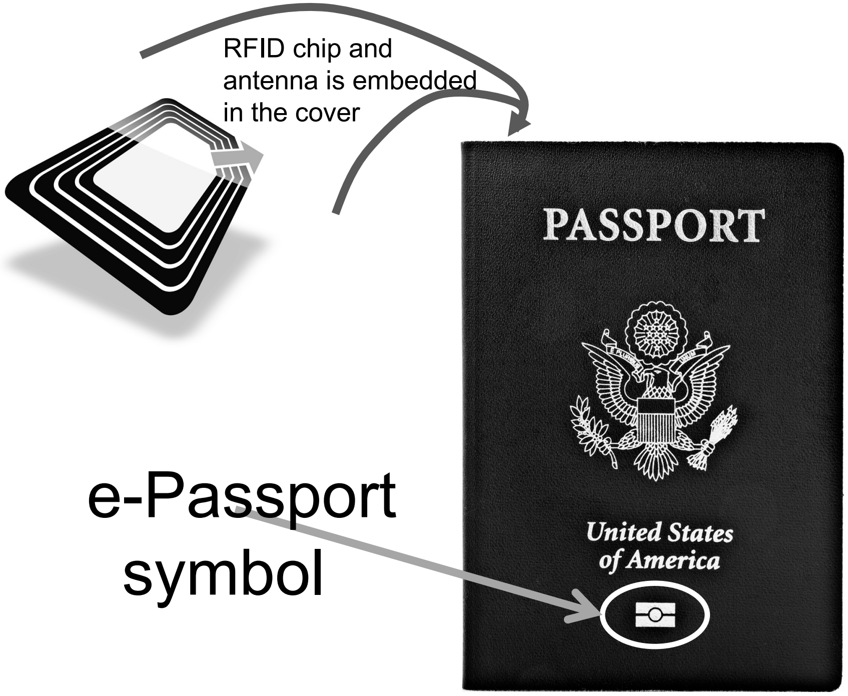
- RFID tags must be used in conjunction with a separate reader or writer.
- While some RFID tags require a battery, many are passive and do not.
- The effective range of RFID varies from a few centimeters to several meters, but in most cases, since data is transmitted via radio waves, it is not necessary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



RFID chip and antenna is embedded in the cover

e-Passport symbol

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.

2.3.5 Biometrics

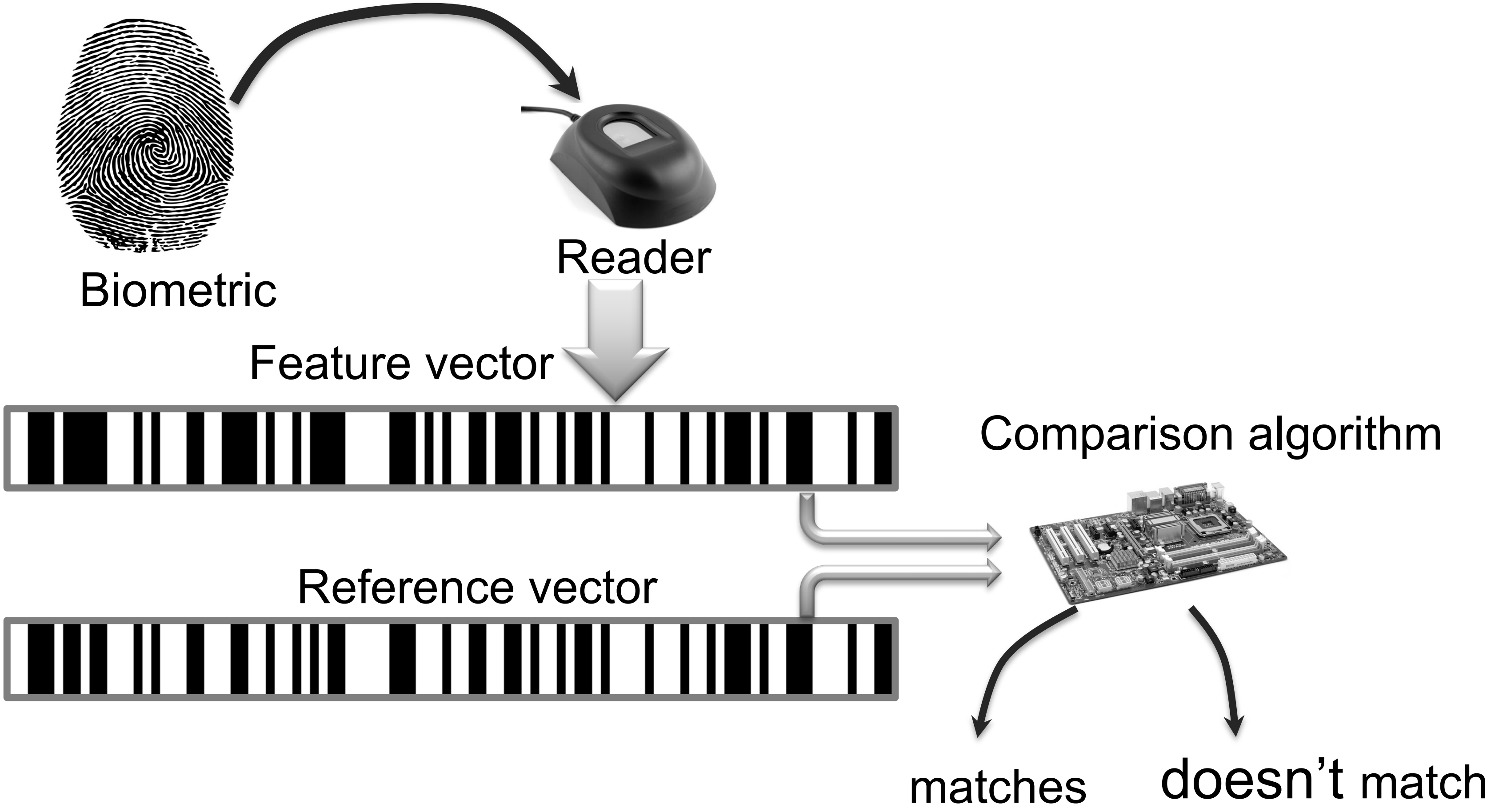
- **Biometric** refers to any measure used to uniquely identify a person based on biological or physiological traits.
- Generally, biometric systems incorporate some sort of sensor or scanner to read in biometric information and then compare this information to stored templates of accepted users before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

Image from http://commons.wikimedia.org/wiki/File:Fingerprint_scanner_in_Tel_Aviv.jpg used with permission under the Creative Commons Attribution 3.0 Unported license

Requirements for Biometric Identification

- **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

2.4.1 Direct attacks against computers -- Environmental attacks

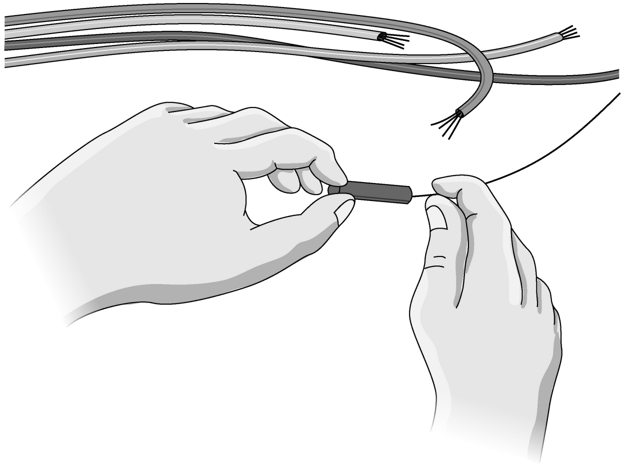
- **Electricity.** Computing equipment requires electricity to function; hence, it is vital that such equipment has a steady uninterrupted power supply.
- **Temperature.** Computer chips have a natural operating temperature and exceeding that temperature significantly can severely damage them.
- **Limited 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).

2.4.2 Direct attacks against computers -- 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.**

Direct attacks against computers -- 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.



2.4.2 Direct attacks against computers - Signal Emissions

- 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.

2.4.2 Direct attacks against computers Acoustic Emissions

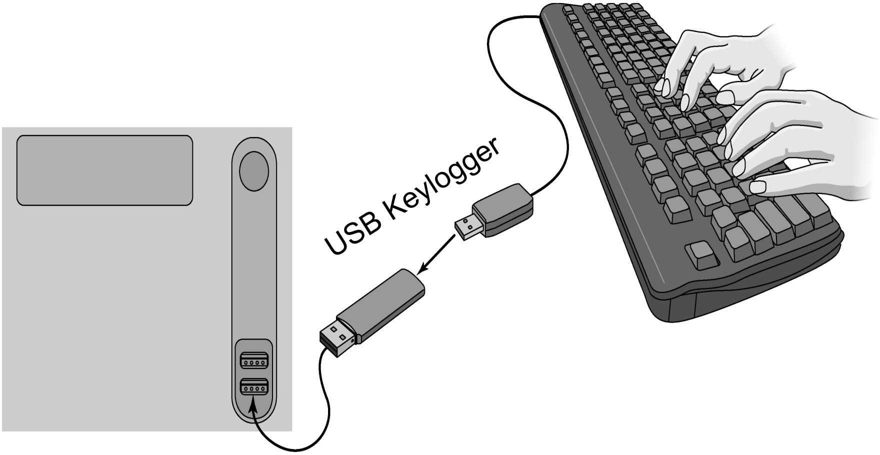
- Dmitri Asonov and Rakesh Agrawal published a paper in 2004 detailing how an attacker could use an audio recording of a user typing on a keyboard to reconstruct what was typed.
  - Each keystroke has minute differences in the sound it produces, and certain keys are known to be pressed more often than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

sound recording device

microphone to capture keystroke sounds

2.4.2 Direct attacks against computers 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 coming from a keyboard.



2.4.3 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.

2.4.3 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.

2.4.3 Faraday Cages

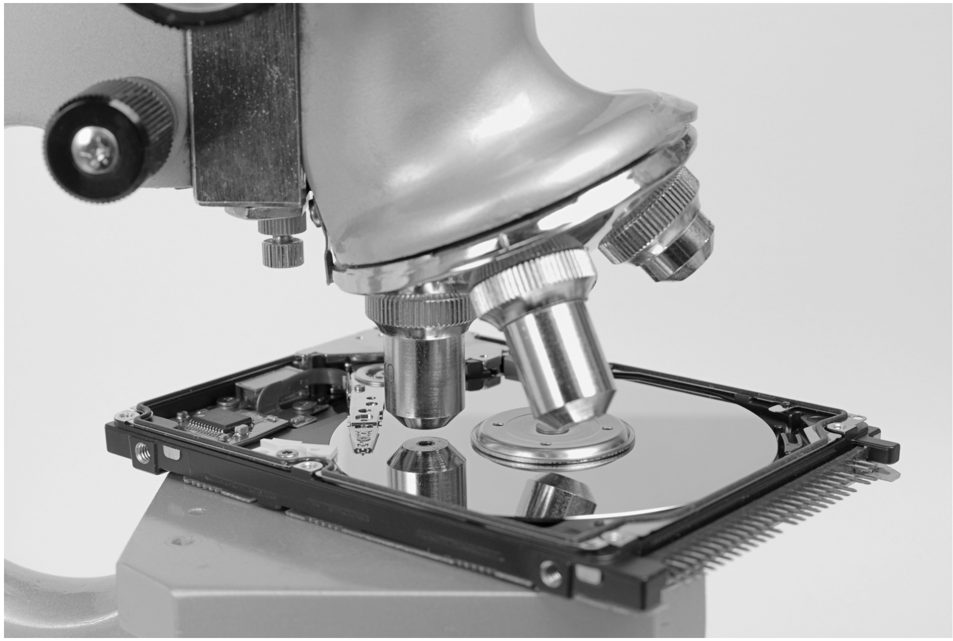
- To block electromagnetic emanations in the air, we can surround sensitive equipment with metallic conductive shielding or a mesh of such material, where the holes in the mesh are smaller than the wavelengths of the electromagnetic radiation we wish to block.
- Such an enclosure is known as a **Faraday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

2.4.5 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.

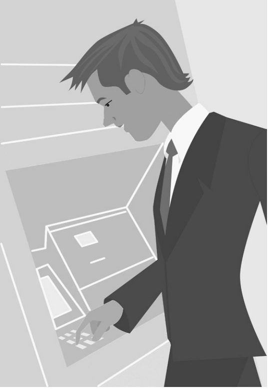
2.4.5 Computer Forensics

- 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.



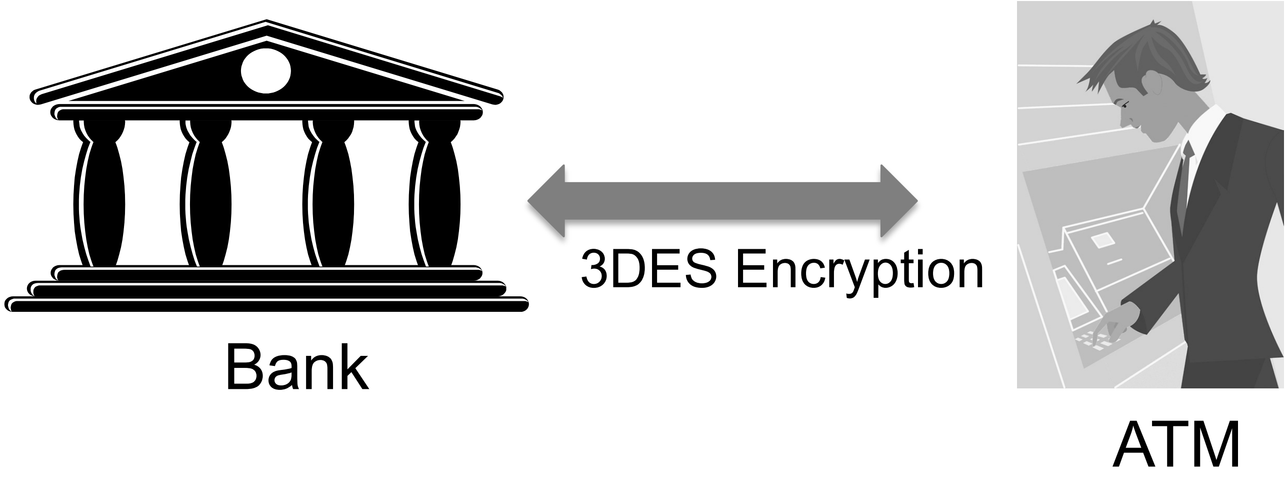
2.5 Special-Purpose Machines - ATMs

- 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 for older systems that are not connected to a network) or in a remote database.



2.5 Special-Purpose Machines - ATMs

- 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

3DES Encryption

ATM

2.5 Special-Purpose Machines - 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.

2.6 Peripheral Security

- Risks associated with common peripherals can come from removable media, laptops, shoulder surfing, discarded devices, and printed documents.
- In order to mitigate risks, we need control access to devices such as printers, copiers, mobile devices, imaging devices, or any other devices that store data and are connected to networks.