CSc 466/566

Computer Security

2 : Physical Security

Version: 2019/08/28 10:34:10

Department of Computer Science
University of Arizona

collberg@gmail.com

Christian Collberg

Outline

Direct Attacks Against Computers

- What kind of damage can an adversary cause if
  1. he has direct physical access to it?
  2. he is in close physical proximity to it?
- It is usually assumed that the user of a computing system is trusted — but the reality is often different!

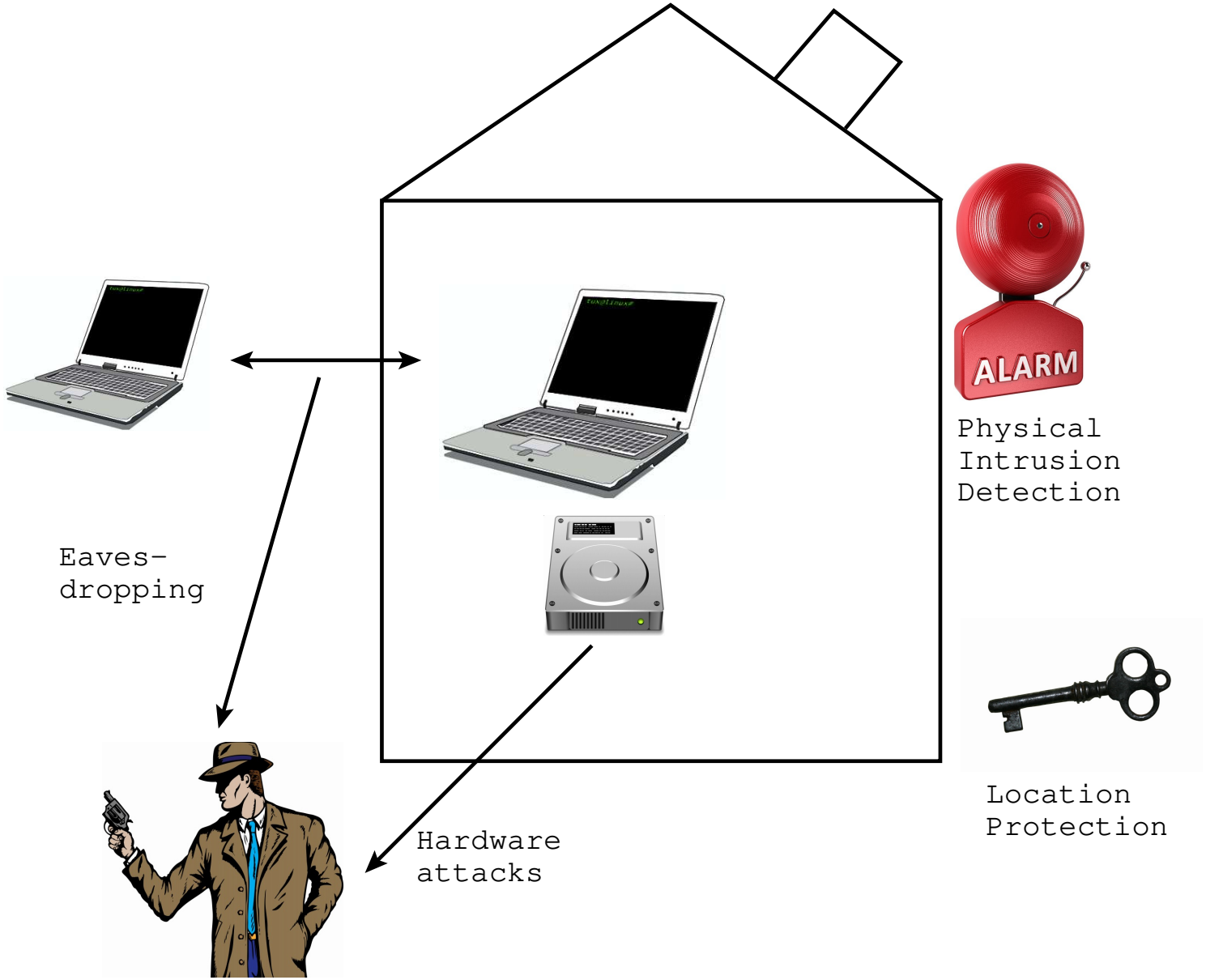
Physical vs. Digital Interface

- We access computers
  - over the network
  - keyboard
  - other well-defined digital interfaces
- Or with a
  - sledge hammer, a bottle of liquid nitrogen, ...
- We need to protect access to computers physically as well as digitally.

Physical Security

Definition (physical security)

The use of physical measures to protect valuables, information, or access to restricted resources.

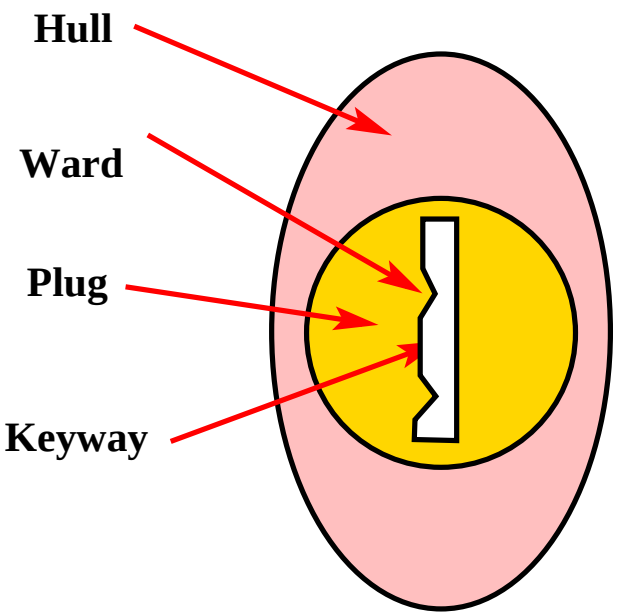

ALARM
Physical
Intrusion
Detection
Eaves-
dropping
Hardware
attacks
Location
Protection

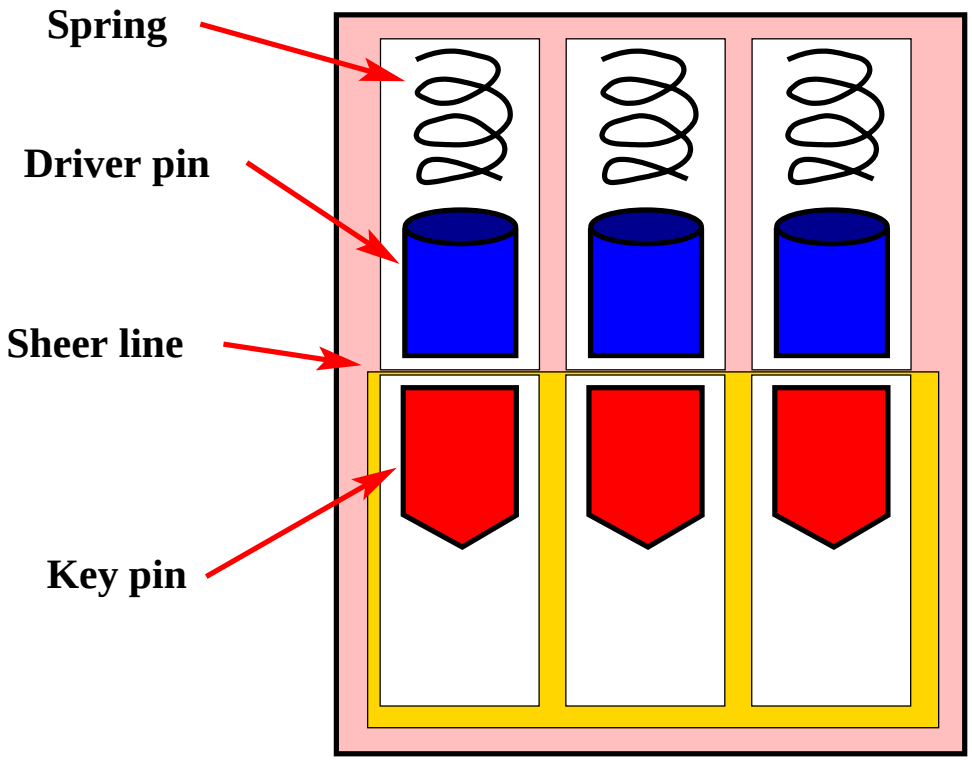
Physical Security

1. Location protection: protecting the location where hardware resides;
2. Physical intrusion detection: detecting intrusion into the location where hardware resides;
3. Hardware attacks: attacks against hard drives, CPUs, etc.;
4. Eavesdropping: attacks that monitor signals from or between computers;

Outline

Locks: Terminology and Layout





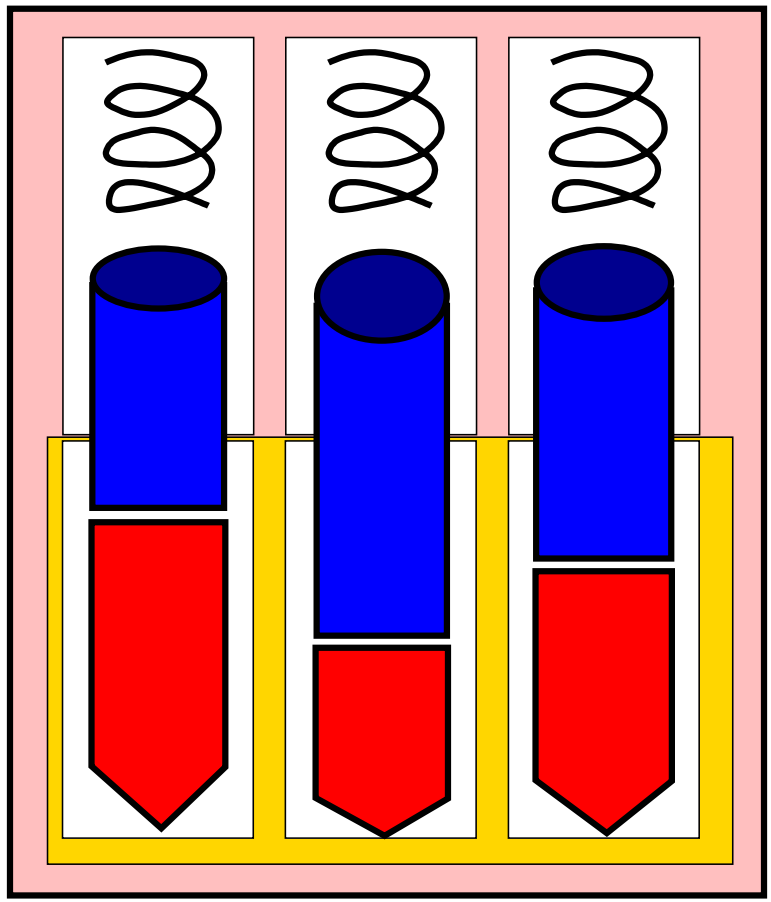
- plug: the cylinder that contains the keyway and turns when the proper key is inserted
- keyway: where the key is inserted
- ward: sticks out of the sides of the keyway to restrict what keys will fit
- hull: the non-rotating part of the lock
- key pin: they pin that touches the key, also lifts the driver pin
- driver pin: This pin sits on top of the key pin
- sheer line: The space where the hull and plug meet
- spring: pushes the driver pin into the plug.

Lock Layout

A lock consists of

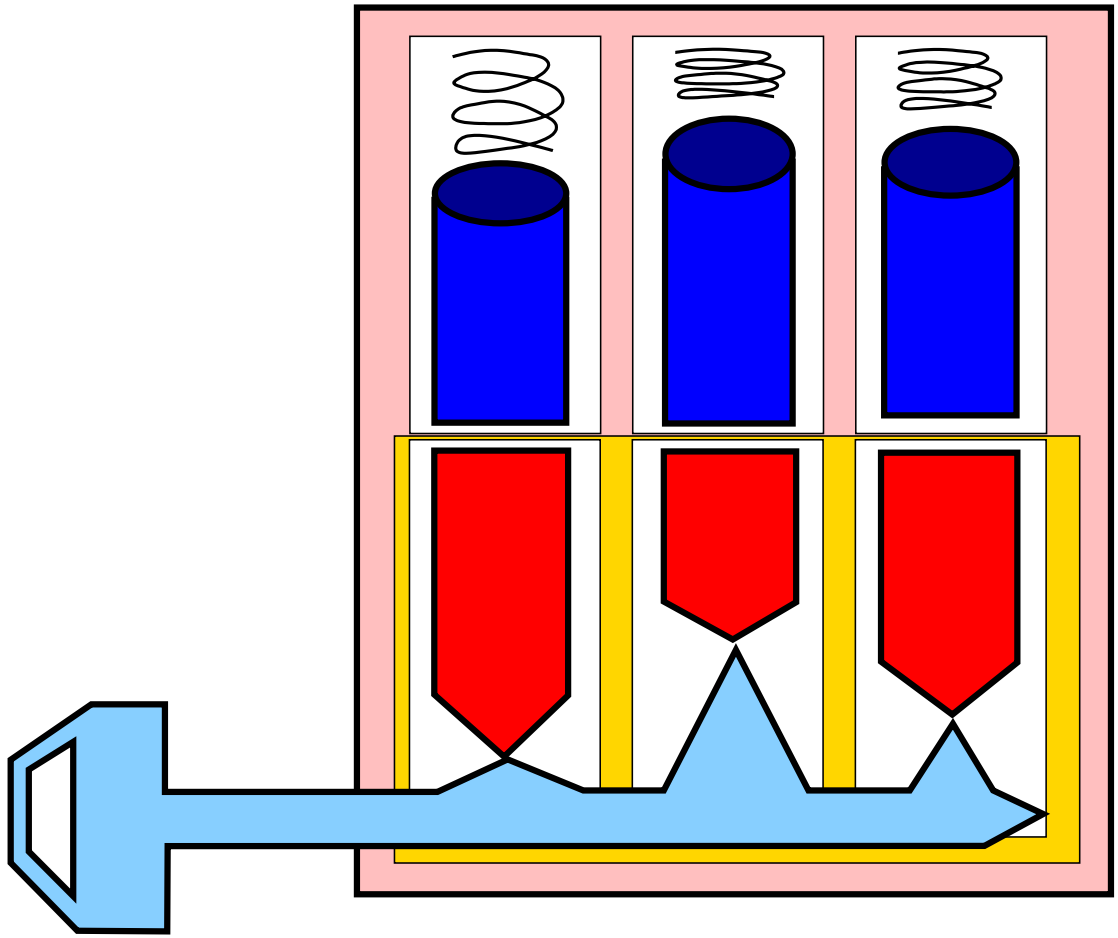
1. a hull and a plug, where the plug sits inside the hull such that rotating it opens the lock;
2. a keyway inside the plug that gives the key access to the pins;
3. a set of pins:
   - driver pins prevent the plug from rotating;
   - key pins allow the key to push the driver pins above the sheer line.

Locked Lock



- In a locked lock, the driver pins are stuck between the sheer line, stopping the plug from rotating.

Opened Lock

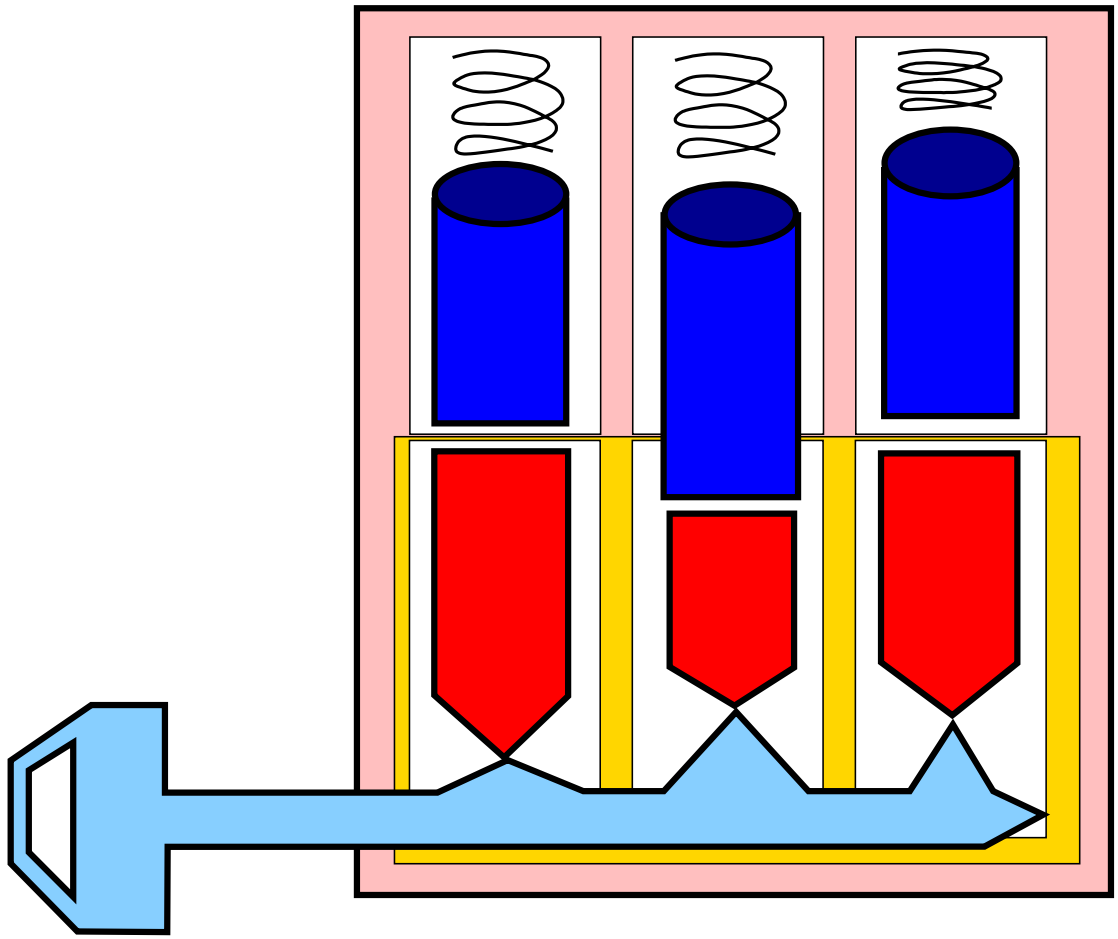


- In an opened lock the key pins push the driver pins above the sheer line allowing the plug to be rotated.

How Locks Work — Animation

- https://www.youtube.com/watch?v=Wtl2hmHZCLw&feature=youtu.be

Wrong key



- An incorrect key will leave some of the driver pins stuck between the sheer line, stopping the plug from rotating.

Locks with Master Keys

- Certain locks can be opened with two different keys.
- Terminology:
  - Change key: the regular key for the lock.
  - Master key: Can also open other locks.
  - Grandmaster key: Can open any lock in the organization.
  - Control key: Can remove the entire cylinder, for rekeying.
- These locks add a spacer pin between the driver pin and the key pin.
- The master key pushes the spacer and driver pins above the sheer line.
- The change key only pushes the driver pin.

Picking a lock: Tools of the Trade

- Terminology:
  - setting a pin: The act of trapping the driver pin above the sheer line even though the key pin is not holding it in place.
  - binding: scissoring (pinning) a pin between the plug and the hull.
- Lock picking requires two tools:
  - A pick for moving the pins
  - A tension wrench for moving the plug.

Lockpicks

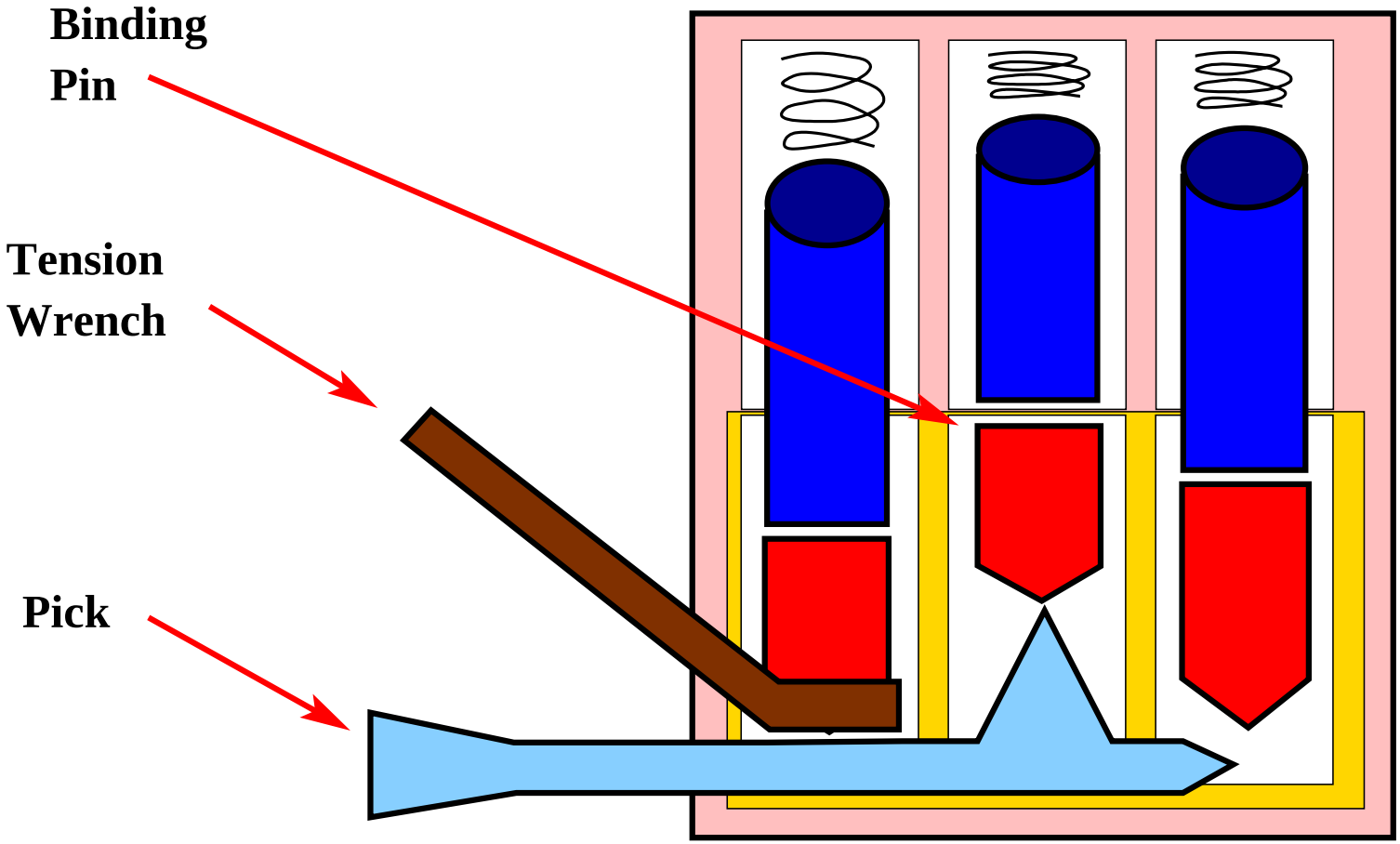
$29.95 Buy Now!

http://www.southord.com/Lock-Pick-Tools/Lock-Pick-Set-8-Piece-Metal-Handles-MPXS-08.html

Technique

- The following technique is used to pick a lock one pin at a time:
  1. Apply a sheer force (torque from the tension wrench);
  2. Find the pin that is binding the most (the binding pin);
  3. Push that pin up until you feel it set at the sheer line;
  4. Go to step 2.

Technique



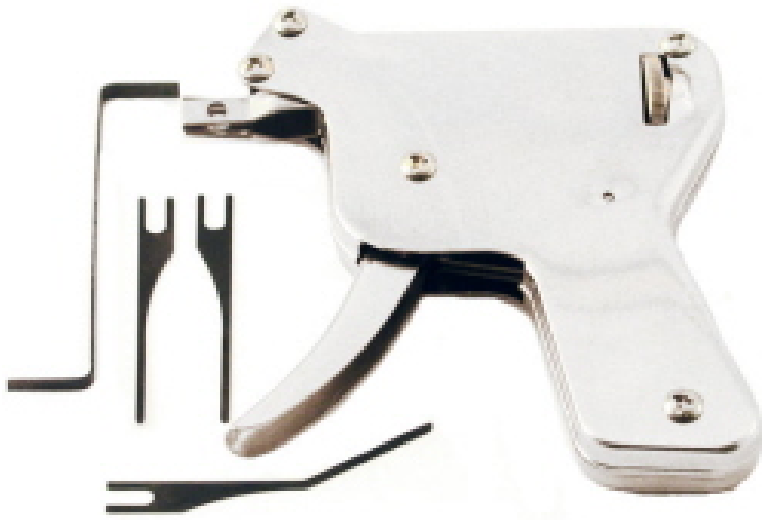
Technique: Scrubbing

- Scrubbing tries to set multiple pins each time the pick is inserted or removed from the keyway.
- The tension wrench is used to bind pins and then a pick is bounced along the pins.
- Technique:
  1. Insert a snake pick (designed to lift multiple pins at the same time) into the keyway;
  2. Move the pick back and forth in the keyway;
  3. Gradually increase the pressure on the pins;
  4. Gradually increase the torque from the tension wrench (to keep pins set);
  5. Pick remaining pins manually.

Demo

- Watch: http://www.youtube.com/watch?v=JZJe23UD8wU

Vibration Picking with Lockpicking Guns



$74.95 Buy Now!

https://www.lockpickshop.com/LAT-17.html

- Watch: https://www.youtube.com/watch?v=NPRVTU-rCnc

Bump Keys

- https://www.youtube.com/watch?v=hr23tpWX81M
- You can do vibration picking manually as well, called lock bumping.

Brute Force

- https://www.youtube.com/watch?v=p-ID-wUYoHY
- With a bit of ingenuity, many locks are simple to break!

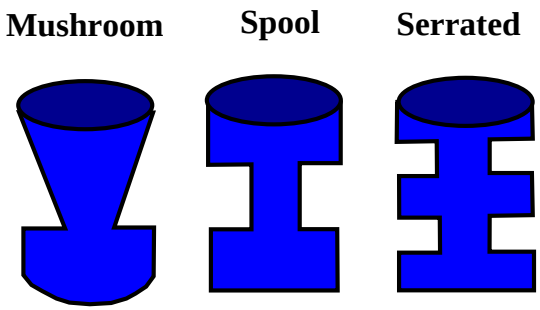
Vibration Picking with Electric Gun

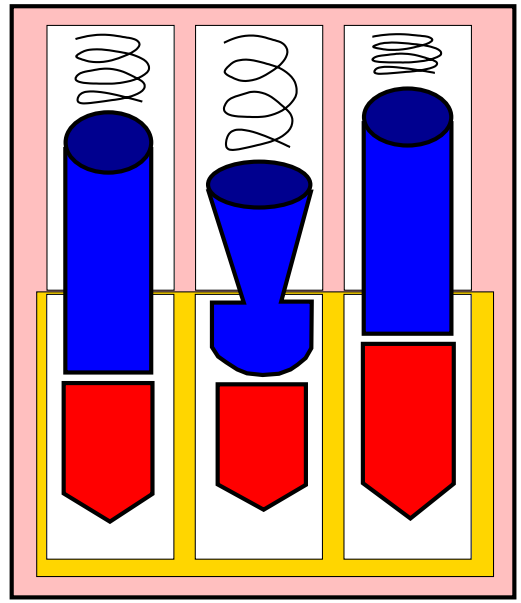
$294.95 Buy Now!

https://www.lockpickshop.com/ELECTROPICK.html

- DIY watch: https://www.youtube.com/watch?v=rDlZbQ20aLI

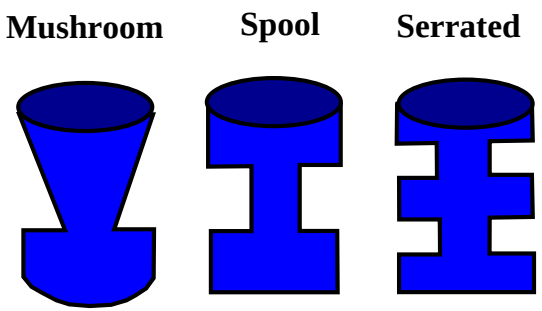
Countermeasures

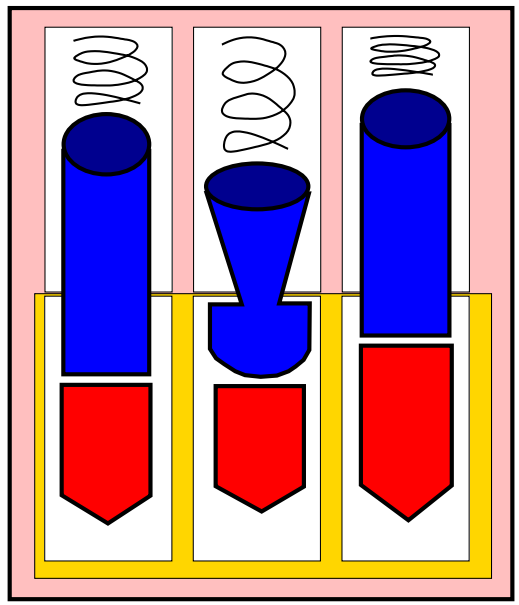




- Security pins:
  - Special driver pins in an attempt to make lock picking harder.
  - These pins will cause a low false set.
  - Particularly damaging to vibration picking.

Countermeasures to the countermeasure





- Use less torque and more pressure with the pick.

Combination Locks

- https://www.youtube.com/watch?v=09UgmwtL12c
- https://www.youtube.com/watch?v=w4wkCcsWs4c

Open Masterlock with zip tie!!!

- https://www.youtube.com/watch?v=BIq9khF-axs&feature=youtu.be

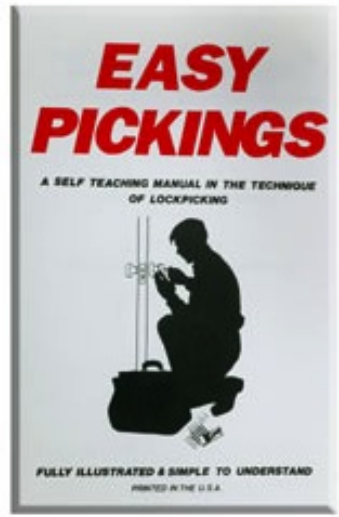
Unpickable (?) Bike Lock!

- https://youtu.be/OLsJDELd4lo?t=83

LockPickingLawyer

- Youtube channel
- https://www.youtube.com/channel/UCm9K6rby98W8JigLoZOh6FQ

Assignment: Learn to Pick Locks!



$99.95 Buy Now!

- http://www.southord.com/Lock-Pick-Tools/Locksmith-School-In-A-Box-ST-23.html
- We have several of these, for you to practice on.

Assignment: Learn to Pick Locks!

$39.95 Buy Now!

- http://www.southord.com/Lock-Pick-Tools/Practice-Lock-Cutaway-Visible-Locks-ST-34.html
- And we have three of these, too. . . .

Exercise: Goodrich & Tamassia C-2.3

- A group of n pirates has a treasure chest and one unique lock and key for each pirate.
- Using hardware that is probably already lying around their ship, they want to protect the chest so that any single pirate can open the chest using his lock and key.
- On the next slide, draw how they set this up!

Exercise: Goodrich & Tamassia C-2.3...

Exercise: Goodrich & Tamassia C-2.3...

The pirates link their locks together with links of chain and wrap that chain around the treasure chest (augmenting with a extra links of chain if the chain with the locks is not long enough). If any pirate opens his lock it breaks the chain and he can open the chest.

Exercise: Goodrich & Tamassia C-2.4

- A group of n red pirates and a group of n blue pirates have a shared treasure chest and one unique lock and key for each pirate.
- Using hardware that is probably already lying around their two ships, they want to protect the chest so that any pair of pirates, one red and one blue, can open the chest using their two locks and keys.
- No group of red or blue pirates can open the chest without having at least one pirate from the other group.
- On the next slide, draw how they set this up!

Exercise: Goodrich & Tamassia C-2.3...

Exercise: Goodrich & Tamassia C-2.3...

The red pirates link their locks together in a chain and wrap that chain through a latch on the chest that is big enough to let locks slide through it. The blue pirates do the same through the same latch. To open the chest, they need one red pirate to open the chain of red-pirate locks and they need one blue pirate to open the chain of blue-pirate locks.

Exercise: Goodrich & Tamassia C-2.5

- A group of four pirates has a treasure chest and one unique lock and key for each pirate.
- Using hardware that is probably already lying around their ship, they want to protect the chest so that any subset of three of these pirates can open the chest using their respective locks and keys, but no two pirates can.
- On the next slide, draw how they set this up!

Exercise: Goodrich & Tamassia C-2.5...

Exercise: Goodrich & Tamassia C-2.5...

Each pirate uses his lock and key to lock down one of the four sides of the lid to the chest. If any three pirates open their latches, they can lift the top by essentially using the fourth (locked) latch as a hinge.

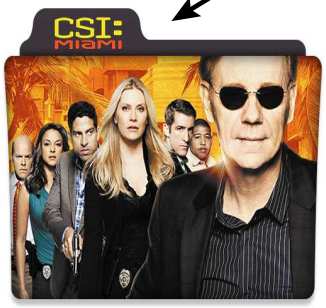
Outline

Computer Forensics

Definition (Computer Forensics)

Identifying, preserving, recovering, analyzing and presenting facts and opinions about the information found on digital storage media, to be used in legal proceedings.


Department of Investigation
FBI
SCULLY, DANA
FBI RANK
SPECIAL AGENT
ID CODE
XF-SD-9415
ISSUED:
9/10/1993
VALID:
9/10/2020
DEPARTMENT OF INVESTIGATION
DIRECTOR
ORDER OF
THE ATTORNEY GENERAL
OF THE UNITED STATES


CSI:
MIAMI

Computer Forensics. . .

- Forensic techniques can be used by attackers to extract information from computer equipment.
- It is essential for forensic analysts to maintain the chain of custody.
- The prosecutor has to be able to convince the judge and jury that data extracted from a hard drive, for example, has not been tampered with.
- Criminals will try to prevent forensic analysis of their systems.

Computer Forensics — Job Opportunities

> *Computer Forensics Salary. The median salary for information security analysts was around $95,510 in 2016, according to the BLS. Those in the lowest 10 percent earned as little as $55,560, while those in the highest 10 percent earned as much as $153,090 annually.*

Source: https://www.forensicscolleges.com/careers/computer-forensics-examiner

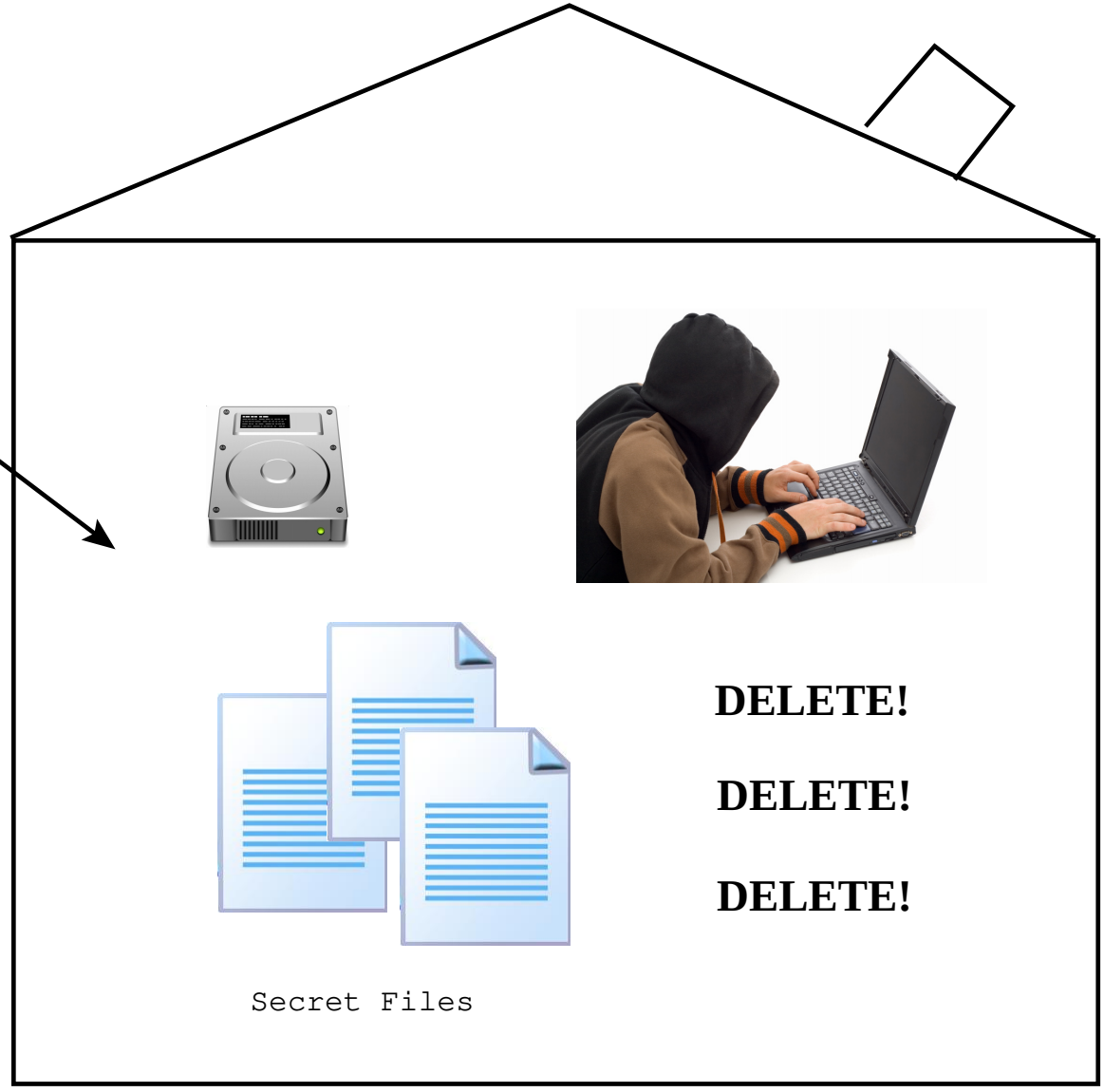
- Glassdoor:

  https://www.glassdoor.com/Salaries/computer-forensics-salary-SRCH_KO0,18.htm

Recovering Deleted Files

- A common way to hide secrets from forensic analysis is for the criminal to simply delete the files from the hard drive.
- However, a simple "delete" will often just remove the links to the file (its meta data), not the file contents.
- A forensic analyst can search through the disk and recover deleted files.


Department of Investigation
FBI
SCULLY, DANA
SPECIAL AGENT
DEPARTMENT OF INVESTIGATION
DIRECTOR
ORDER OF:
THE ATTORNEY GENERAL
OF THE UNITED STATES


DELETE!
DELETE!
DELETE!
Secret Files

Searching for Disk Encryption Keys

- But, what if the disk is encrypted (Microsoft's BitLocker, Apple's FileVault, ...)?
- Encryption keys are, essentially, just large (64-256 bits) random numbers.
- Normal data in memory isn't random at all! Images, text, code, ...
- So, to find an encryption key in memory, the forensic analyst just has to search through RAM looking for a large random number!

Encrypted Disk

Disk Encryption Key:

SEARCH FOR RANDOM-LOOKING DATA!!!

Java Class File:

PNG file:

Computer's RAM

Buy milk and eggs

0xAF65E7890BD6C5...

```
int main(){
  int x=47+y;
}
```

0xCAFEBABE

0x89504E470D0A1A0A

Countermeasure: Secure Delete

- Government standards say how to do this securely:

  clear: Overwrite the sensitive files with other data.

  purge: Remove the sensitive files from the media.

  destroy: Disintegrate, pulverize, melt, incinerate, shred the media.

Source: *NIST Special Publication 800-88, Guidelines for Media Sanitization*,

https://ws680.nist.gov/publication/get_pdf.cfm?pub_id=50819

Countermeasure: Secure Delete...

- **Peter Gutmann** invented a 35-pass method to securely erase information from a disk:

  https://en.wikipedia.org/wiki/Gutmann_method

- However, he says *"A good scrubbing with random data will do about as well as can be expected"*.


Department of Investigation
FBI
SCULLY, DANA
SPECIAL AGENT
DEPARTMENT OF INVESTIGATION
DIRECTOR
ORDER OF:
THE ATTORNEY GENERAL
OF THE UNITED STATES


WRITE 00000...!
WRITE 11111...!
WRITE 0101010...!
Secret Files

Exploiting Data Remanence

Definition (Data Remanence)

Data remanence is the residual representation of digital data that remains even after attempts have been made to remove or erase the data. This residue may result from data being left intact by a nominal file deletion operation, by reformatting of storage media that does not remove data previously written to the media, or through physical properties of the storage media that allow previously written data to be recovered.

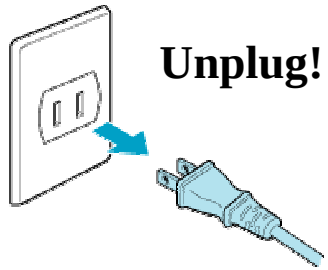
Source: https://en.wikipedia.org/wiki/Data_remanence

Encrypted Disk

Disk Encryption Key:

Computer's RAM

```
0101101010100101010
0xAF65E7890BD6C5...
0101010010001000100
0001000010111110001
1110100110001001100
0010100100000011000
```



Unplug!

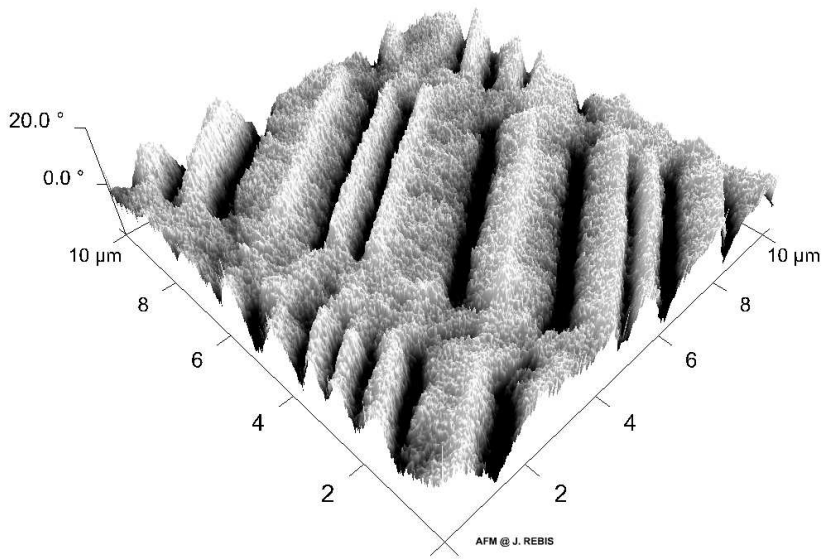
Data Remanence — Examining Hard Drive Bits

- It has been claimed that with a powerful microscope you can recover overwritten data.
- With modern hard drives, this is probably not true.
- But who knows what a sufficiently well funded adversary/government agency can do?

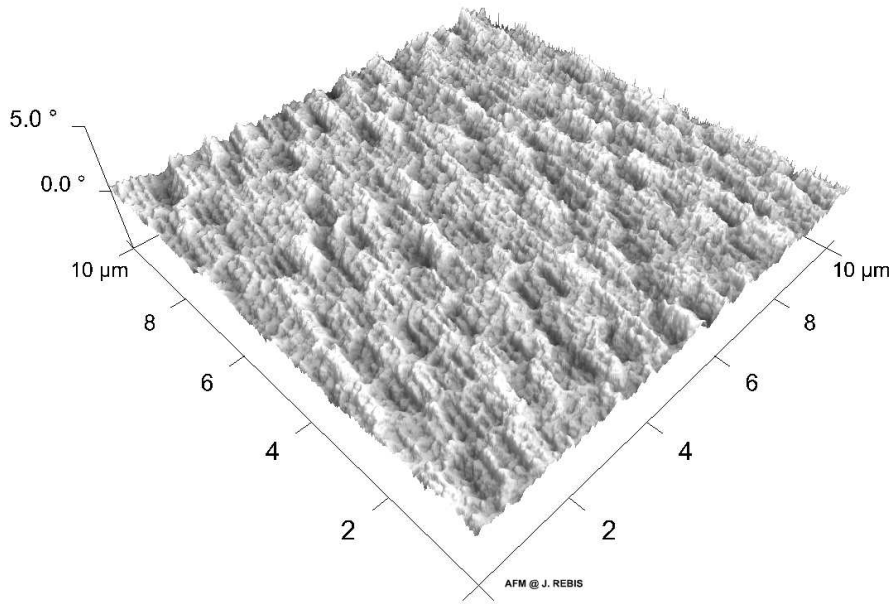
Data Remanence — Hard Drives

MAGNETIC FORCE MICROSCOPY

Dysk twardy magnetyczny 3,2 Gb



Dysk twardy magnetyczny 30 Gb



Data Remanence — Freezing RAM

- If you freeze the RAM on a running computer, and then power it off, you can still recover the contents of memory!

Data Remanence — Freezing RAM

Encrypted Disk

FREEZE!
FREEZE!
FREEZE!

Disk Encryption Key:

Computer's RAM

```
0101101010100101010
0xAF65E7890BD6C5...
0101010010001000100
0001000010111110001
1110100110001001100
0010100100000011000
```

Live CDs

Definition (Live CD)

A bootable computer operating system stored on external media (CD, DVD, USB drive) allowing a computer to be booted without a hard disk drive.

- Live CDs can be used both by good guys and bad guys to read sensitive data off a computer's hard drive.
- Also Live USB Drive etc.

Live CDs. . .

Linux-Live-CD.org

Boot without hard drive!!!

KALI LINUX

Cold Boot Attack

- A Cold Boot Attack combines three techniques we've seen to read the contents of an encrypted disk:
  1. freezing DRAM
  2. live CD booting
  3. searching for random data

Exercise: Cold Boot Attack — Algorithm

Give the detailed steps how the FBI/CSI might use a Cold Boot Attack to extract sensitive files from a criminal's computer!

Exercise: Cold Boot Attack — Algorithm

Give the detailed steps how the FBI/CSI might use a Cold Boot Attack to extract sensitive files from a criminal's computer!

1. freeze DRAM on the running computer

Exercise: Cold Boot Attack — Algorithm

Give the detailed steps how the FBI/CSI might use a Cold Boot Attack to extract sensitive files from a criminal's computer!

1. freeze DRAM on the running computer
2. power off the computer

Exercise: Cold Boot Attack — Algorithm

Give the detailed steps how the FBI/CSI might use a Cold Boot Attack to extract sensitive files from a criminal's computer!

1. freeze DRAM on the running computer
2. power off the computer
3. remove the computer to the lab

Exercise: Cold Boot Attack — Algorithm

Give the detailed steps how the FBI/CSI might use a Cold Boot Attack to extract sensitive files from a criminal's computer!

1. freeze DRAM on the running computer
2. power off the computer
3. remove the computer to the lab
4. boot the computer from a Live CD

Exercise: Cold Boot Attack — Algorithm

Give the detailed steps how the FBI/CSI might use a Cold Boot Attack to extract sensitive files from a criminal's computer!

1. freeze DRAM on the running computer
2. power off the computer
3. remove the computer to the lab
4. boot the computer from a Live CD
5. search through RAM to extract the disk encryption key

Exercise: Cold Boot Attack — Algorithm

Give the detailed steps how the FBI/CSI might use a Cold Boot Attack to extract sensitive files from a criminal's computer!

1. freeze DRAM on the running computer
2. power off the computer
3. remove the computer to the lab
4. boot the computer from a Live CD
5. search through RAM to extract the disk encryption key
6. decrypt the disk

Draw CSI using a Cold Boot Attack!

Exercise: Cold Boot Attack Countermeasures

How might a criminal prevent the FBI from recovering their data using a cold boot attack?

Exercise: Cold Boot Attack Countermeasures

How might a criminal prevent the FBI from recovering their data using a cold boot attack?

- Don't store encryption keys in cleartext in RAM.

Outline

Eavesdropping

Definition (Eavesdropping)

Secretly listening in on another person's conversation.

- Not really a "computer security" issue — we need to protect the environment in which the system is used.
- Passive wiretapping: monitoring or eavesdropping on communication.
- Active wiretapping: modifying or creating bogus communcation.

Eavesdropping: Shoulder Surfing

- Shoulder surfing:
  - installing small hidden cameras,
  - watch with binoculars through a window,
  - ...
- Countermeasures:
  - ATM machine displays have limited viewing angle,
  - ATM keypads shields the keypad from view,
  - Alter the physical location of the keypad keys after each keypress.

Eavesdropping: Wiretapping

- Coaxial cable, twisted pair:
  - measure the leaked electrical impulses
  - cut cable, splice in secondary one
- Ethernet cable:
  - briefly disconnect, insert passive listening device
- Fiber optic cable:
  - bend the cable, read the leaked light with an optical sensor
  - cut the fiber, reconnect it with an 80/20 splitter (80% goes through, 20% is used to monitor) in line ($100).
- Microwave/satellite communication:
  - an attacker close to receiver can read the communication

Eavesdropping: Countermeasures to Wiretapping

- Countermeasures:
  - Detect brief disconnect of cables
  - Detect drop in signal strength
  - End-to-end encryption.
- Countermeasures to the countermeasures:
  - Reboost the signal to make up for signal loss
  - Perform the attack at night when it is less likely to be detected.

Eavesdropping: Monitoring Emissions

- Electromagnetic radiation:
  - Monitor CRT displays
- Optical emissions:
  - CRT displays emit light pulses that can be monitored with a photosensor, and the screen image can be reconstructed.
- Acoustic emissions:
  - Listening to typing can reconstruct 79% of keystrokes.
  - Listening to a CPU can reveal the instructions it executes.

Eavesdropping: Hardware Keyloggers

- USB-to-USB connector, installed between keyboard and computer.
- Logs passwords to flash memory.
- Attacker can retrieve the logger or data can be transmitted wirelessly.
- Could capture BIOS passwords giving full control over the machine.

This [KeyGrabber Wi-Fi Premium] wireless keylogger is packed with state-of-the-art electronics: two powerful processors, a full TCP/IP stack, a WLAN transceiver, and 2 Gigabytes of memory. How does it work? Besides standard PS/2 and USB keylogger functionality, it features remote access over the Internet. This wireless keylogger will connect to a local Wi-Fi Access Point, and send E-mails containing recorded keystroke data. You can also connect to the keylogger at any time over TCP/IP and view the captured log. All this in a device less than 2 inches (5 cm) long!

Hardware Keyloggers: KeyGrabber Wi-Fi Premium...

- Applications:
  - Observe WWW, E-mail & chat usage by children and employees
  - Monitor employee productivity
  - Protect your child from on-line hazards and predators
- $148.99 Buy Now!

Hardware Keyloggers: KeyGrabber Wi-Fi Premium...

- Features:
  - Background connection to the Internet over a local Access Point
  - Automatic E-mail reports with recorded keyboard data
  - On-demand access at any time through TCP/IP
  - Support for WEP, WPA, and WPA-2 encryption
  - 2 Gigabytes of internal memory in all versions
  - No software or drivers required, Windows, Linux, and Mac compatible
  - Ultra compact and discrete, less than 2 inches (5 cm) long
  - Internal clock and battery with over 7 years lifetime guaranteed!

Is this legal?

Technically speaking, you should contact a lawyer to get detailed information about the local laws, and the application for which you intend to use this device for. Generally it's permitted to monitor your own computer, meaning you can watch what your kids and family are doing on the computer. If you want to monitor your employees, or perform any other type of surveillance, you should display a clear notice about this fact. It is obviously NOT LEGAL to use this device for any type spying, or stealing confidential data.

Hardware Keyloggers: KeySweeper

http://samy.pl/keysweeper

Soviets Bugged Electronic Typewriters

IBM's Selectric typewriter had been invented in 1961 and 15 years later could be found in offices the world over. . . . the Soviets managed to produce keystroke loggers back in the 1970s and successfully installed them in at least thirteen Selectric machines at America's Embassy . . . buildings in Moscow and St Petersburg.

Soviets Bugged Electronic Typewriters...

The spy devices were powered either by battery or directly from the mains supply which powered the electric typewriter itself. Once every 82 seconds the devices would transmit 400 microsecond radio bursts of eight encrypted keystrokes. In this way a record of what was being typed in the Embassy was passed directly to the Kremlin.

https://www.qccglobal.com/soviet-spies-bugged-worlds-first-electronic-typewriters

TEMPEST

Definition (TEMPEST)

U.S. government standards for limiting electromagnetic intelligence-bearing signals from computing equipment.

- NATO SDIP-27 zones of protection:
  1. Level A: almost immediate access (neighbour room, 1 m distance).
  2. Level B: 20 m distance (or similar level of building material attenuation).
  3. Level C: 100 m distance (or equivalent attenuation).
- Countermeasures:
  - Block the emissions
  - Modify the emissions.

TEMPEST: Emanation Blockage

- Block visible light:
  - Windowless room
- Block acoustic emanations:
  - Line room with sound-dampening materials
- Block electromagnetic radiation:
  - Line room with copper mesh with holes smaller than the wavelength we want to block (Faraday Cage).

TEMPEST: Emanation Masking

- Broadcast random noice signals so that the information-carrying signals are lost in the noice.

Outline

Summary Questions

19. What is Tempest?
20. What is a Hardware Keylogger?
21. In Computer Forensics, what is a Live CD?
22. In Computer Forensics, what is a Cold Boot Attack?

Readings and References

- Chapter 2 in *Introduction to Computer Security*, by Goodrich and Tamassia.
- Marshall Brain and Tom Harris, *How Lock Picking Works*, http://home.howstuffworks.com/home-improvement/household-safety/security/lock-picking2.htm
- Ted the Tool, *MIT Guide to Lock Picking*, http://www.lysator.liu.se/mit-guide/MITLockGuide.pdf
- Bruce Schneier, http://www.schneier.com/blog/archives/2007/09/eavesdropping_o_1.html