Introduction to Computer Science

Part I – The basics

27.09.2018

SIRE507

=

These topics are less important right now,
but you should know about them.

The very basics

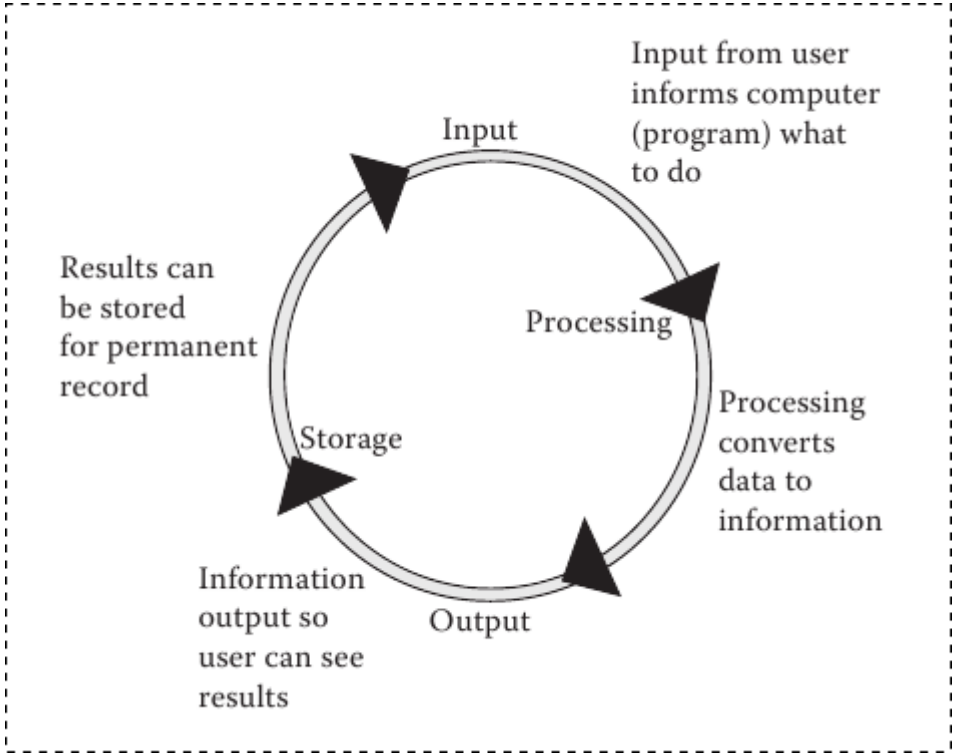
Functionalities

- What is it computers do?

- Takes data as input.
- Processes the data and converts it into useful information
- Generates the output
- Stores the data/instructions in its memory and use them when required.
- Controls all the above four step.

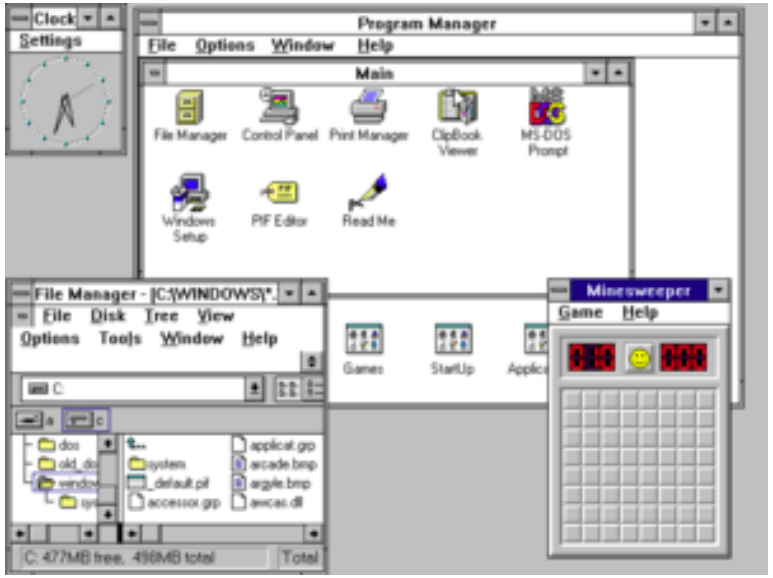
IPOS Cycle

- Input
- Processing
- Output
- Storage



Interacting with a computer

- GUI – graphical user interface
  - Graphical windows
  - Mouse to point and click
- CLI – Command line interface
  - Terminals (text based window)
  - Keyboard to enter commands (“enter” to execute)



The numbers

Unit of measurements

- How does a computer understand numbers?
- Gradients are difficult: 0,1,2,3,4,5,6,7,8,9
  - and what about decimals: 0.1, 0.2, 0.3, 0.4, 0.5, 0.6, 0.7, 0.8, 0.9
- Switches are much easier
  - On or Off
  - 0 or 1
  - True or False
- In computers this is called a binary digit (bit)
  - Which is the basis of the binary number system

Binary number system

- Counting with binary:
  - 0, 1 …?
  - Add another digit: 10
  - 0, 1, 10, 11, 100, 101, 110, 111, 1000
  - 0, 1, 2, 3, 4, 5, 6, 7, 8
  - x x x x

  - 1, 2, 4, 8, … , ?
  - 2^0, 2^1, 2^2, 2^3, … , 2^n
  - Base is said to be 2
- Parallells with decimals (base 10):
  - 1, 10, 100, 1000, …
  - 10^0, 10^1, 10^2, 10^3, … , 10^n

Converting from binary to decimal

0110: 0 x 8 = 0

1 x 4 = 4

1 x 2 = 2

0 x 1 = 0

6

Quiz 1:

- `01000000 = ?`
- `00111001 = ?`

Hexadecimal numbers

- Hexadecimal is a number system with base 16
  - 0, 1, 2, 3, 4, 5, 6, 7, 8, 9, A, B, C, D, E, F
  - (In decimal: 0 to 15)
- We can map 4 bits to one hexadecimal number
  - 4 digit binary: 0000 to 1111 = 0 to 15
- Map hexadecimal to binary
  - 0 = 0000
  - 4 = 0100
  - 7 = 0111
  - E = 1110
  - 47 = 0100 0111

Octal numbers

- Octal is a number system with base 8
  - 0, 1, 2, 3, 4, 5, 6, 7
  - (In decimal: 0 to 7)
- We can map 3 bits to one octal number
  - 3 digit binary: 000 to 111 = 0 to 7
- Map octal to binary
  - 0 = 000
  - 4 = 100
  - 7 = 111
  - 47 = 100 111

Quiz 2:

- FF = ?
- 1A = ?

Bytes

- Usually, you need several bits together to be informative.
- Byte – collection of 8 bits
- 8 bits: 0000 0000
  - Possible combinations: 256 (0 – 255)
- This is used together with the prefixes:
  - K = kilo (i.e. KB = kilobyte)
  - M = Mega
  - G = Giga
  - T = Tera
  - P = Peta
  - E = Exa

Units of measurement

- 1 bit (b) – Answer to yes/no question.
- 1 byte (B) – A number from 0 to 255.
- 90 bytes – Store one line of text from a book.
- 4 KB – One page of text.
- 120 KB – Content of one typical pocket book.
- 3 MB – A three minute song. (mp3)
- 650 – 900 MB – A CD-ROM
- 1 GB – 114 minutes of uncompressed CD-quality audio.
- 8-16 GB – DVD

Units of measurement

- DNA sequence from one human genome: 100GB
- DNA sequence from only the genes: 6 GB

Data transfer / bandwidth

- USB
  - USB 1.1 (full speed) – 12 Mb/s
  - USB 2.0 (high-speed) – 480 Mb/s
  - USB 3.0 (SuperSpeed) – 5 Gb/s
  - USB 3.1 (SuperSpeed+) – 10 Gb/s

Bits and bytes

- Everything in a computer is stored as bytes (bits)
  - Letters, numbers, text, images, music, videos, …
- ASCII – American Standard Code for Information Interchange
  - One byte codes for one character

Dec	Hex	Oct	Char	Binary
51	33	063	3	00110011
61	3D	075	=	00111101
65	41	101	A	01000001
97	61	141	a	01100001

http://www.asciitable.com/

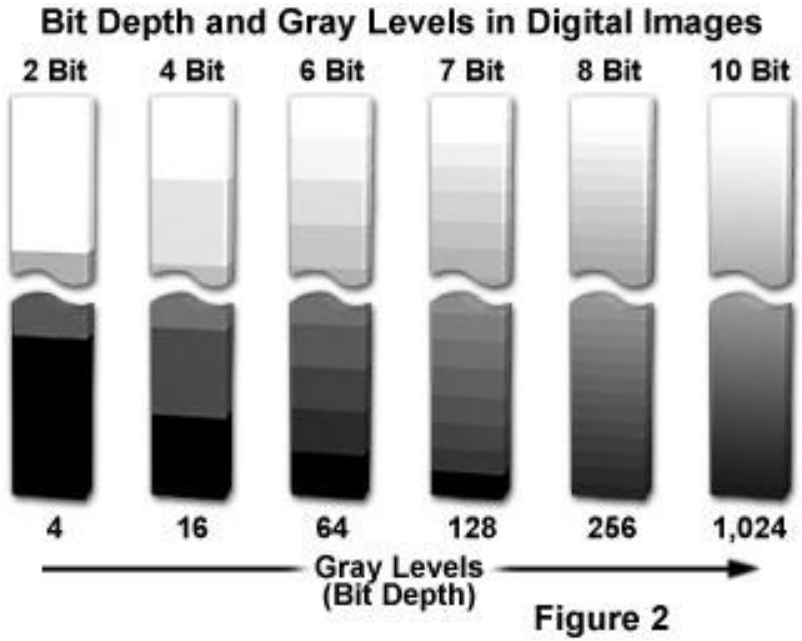
Bits and bytes

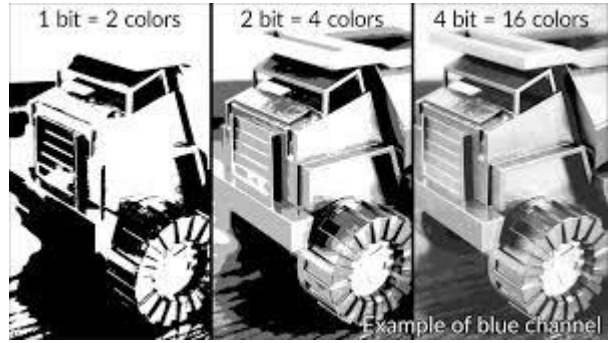
- ASCII only has 256 possible characters (1 byte)
  - Barely enough for one alphabet (English)
- Unicode uses 2 bytes
  - 65535 possible characters
  - Binary: 0000000000000000 – 1111111111111111
  - Hex: 0000 – FFFF
- Allows for many more characters
  - Thai is represented between 0E00 and 0E7F
  - ก – 0E01
  - ๕ – 0E55

http://www.unicodetables.com/

Bits and bytes

- Color is also bytes
- RGB uses 1 byte for each of the three colors (R, G, B)
  - Black = (0, 0, 0)
  - White = (255, 255, 255)
  - Gray = (128, 128, 128)
  - Red = (255, 0, 0)
  - Green = (0, 255, 0)
  - Blue = (0, 0, 255)
  - Yellow = (255, 255, 0)
- Color depth = how many bytes are used to store color



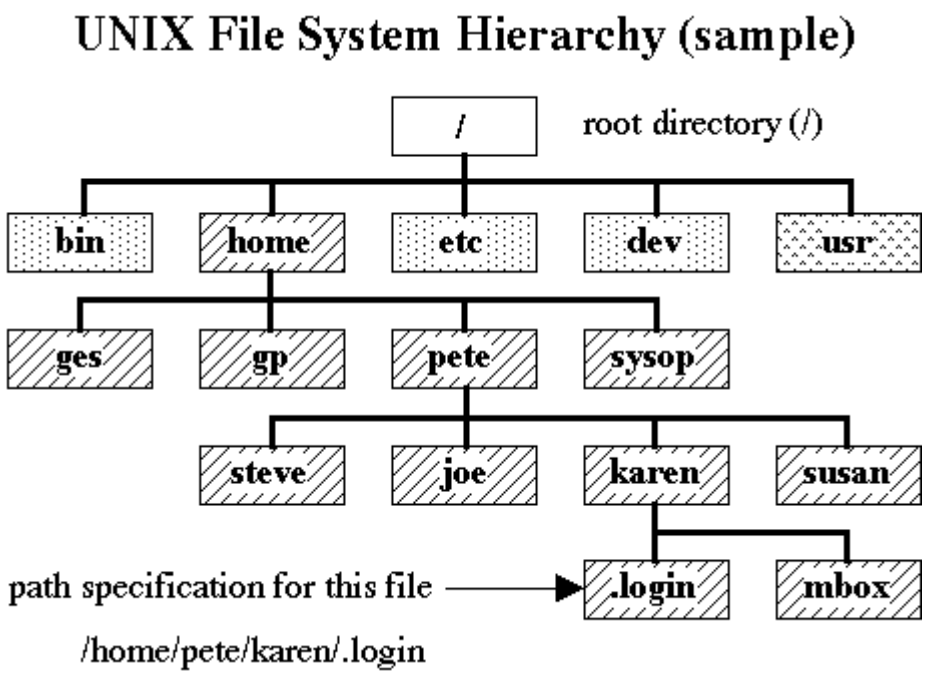


Special character sets

- Whitespace (a special set of characters with no displayed character)
  - Space
  - Tabulator (Tab)
  - Line shift (Enter)
- Alphanumeric
  - Letters and numbers for a given language set
  - English: a – z, A – Z, 0 – 9
  - May also contain some punctuation marks (! , ? @ # . & %)
    - Depends on the situation

Files and folders

- Organized in a file system.
- Every folder can contain (sub-)folders and files.
- Files and folders needs names and these names have restrictions on what characters you can use.



The naming of files

- Basic rule: Only use alphanumeric characters, underscore and dots “.”. (e.g. “test_10.txt”)
- Lower and upper case characters are *usually* treated as separate but it is often best to avoid the possibility of confusion.
- Whitespace characters are often allowed, but is **not recommended** when you use a CLI.
- Different OS’s may have different rules.
  - Windows does not allow / \ : * ? “ < > |
  - Linux does not allow /

The importance of a name

- Traditional file names are on the form: <filename>.<extension>
  - Filename is the name a user can choose to identify the contents of the file.
  - The extension is a (usually) short name identifying the type of file.
- Some common file extensions:
  - .txt – Plain text file
  - .csv – Plain text file, but with columns separated with commas.
  - .xls – Excel spreadsheet
  - .pdf – Adobe Acrobat Reader
  - .fasta – DNA/RNA sequence file.

Compression

- Files can be compressed (zipped) to take less space
- File extension tells which compression method has been used
  - .gz – gzip
  - .zip – zip
  - .rar – WinRAR
  - .bz2 – bzip2
  - .7z – 7zip
- Compressed files must be decompressed
  - usually the compressed files are decompressed to return the original files.
  - some software can work on compressed files by having decompression routines built-in.

Programming

How to tell the computer what to do.

What is programming

- Programming language
  - A language the computer can understand.
  - Several levels: from bits and bytes to almost English.
- Compiler
  - Converts complete code to machine readable commands.
- Interpreter
  - Reads code line by line and translates to machine readable commands
- Bug
  - Any mistakes in a program, causing it (or the computer) to malfunction.

Compiled languages

- The source code is compiled directly to machine code
- Examples:
  - C
  - Fortran
- Advantages
  - Faster speed because the compiler can optimize for the current system.
- Disadvantages
  - Less portable

Interpreted languages

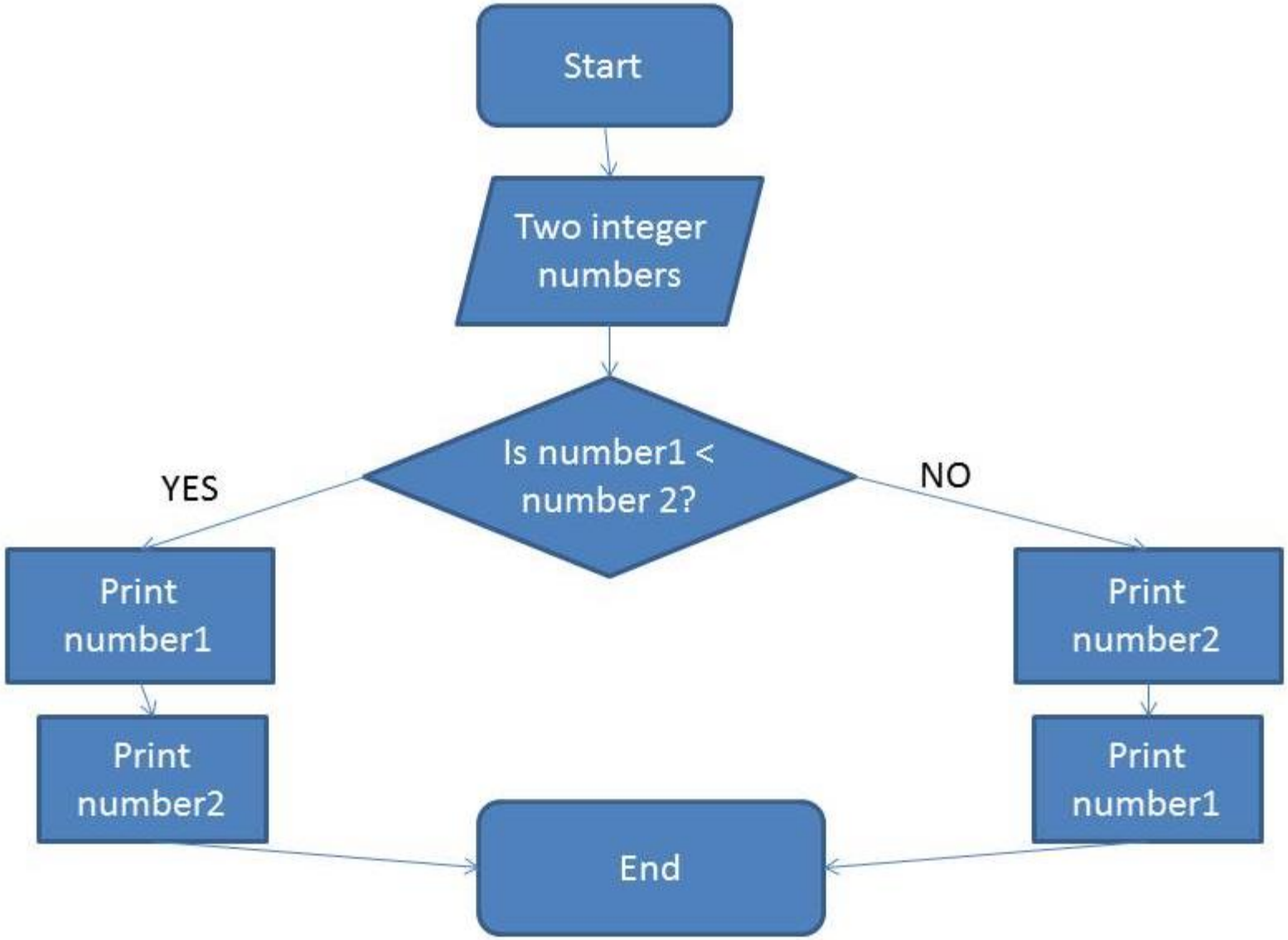
- Programs require an interpreter to be installed on the system
- The interpreter takes care of any system specific issues.
- Examples
  - Java
  - R
  - Python
- Advantages
  - Platform independence
- Disadvantages
  - Not compiling
  - Usually slower

Basics of programming

- Flow control
  - The program decides what to do based on input
  - Do one thing or another
    - If the input is a number, divide it by half.
    - If not, print it out with a message.
  - Repeat an action
    - Create an email for each name in an address book.
- Data manipulation
  - Combine numbers (e.g. add, subtract, multiply, divide, …)
  - Change data from one format to another (e.g. text to numbers)

Problem: Compare two numbers and print them in order, smallest first.

Flowchart:



Network

How to connect

What do we mean by network?

- A computer network is two or more computers that communicate.

- A network allows for
  - Sharing files
  - Access databases
  - Collaborate on projects
  - Browse websites
  - Send e-mail
  - Play games
  - Place phone calls
  - Research
  - Shop
  - …

Network types

- LAN (Local area network)
  - Computers or other devices usually located in a small area
    - House, small office, single building.
  - Connected via switches
  - Connects to the Internet via a router
  - Wireless LAN (WLAN)
  - Wi-Fi is one type of WLAN, using a specific wireless protocol (802.11).
- WAN (Wide area network)
  - Two or more LANs connected over a large geographic area
  - (e.g. Internet)

Network devices

- Hub
  - A device for connecting computers on a LAN.
  - Receives signals from connected computers and transmits out to all computers.
  - The target computer accepts the signal, the rest just drop it.
  - Only two computers can talk together at any given time.
- Switch
  - A device for connecting computers (like a Hub).
  - Receives signals, but sends it to directly to the target computer.
  - Has almost completely replaced the Hub as a connection point.

Network devices (cont…)

- Wireless Access Point (WAP)
  - Device for connecting computers via radio waves (2.4 GHz or 5 GHz).
  - The basis of a Wi-Fi network (WLAN, using the 802.11 protocol).
  - Similar to a switch, it sends received data directly to the target computer.
- Router
  - Connects two or more networks (LAN, WAN or Internet).
  - Uses IP addresses and IP network numbers to direct data from point to point.
  - Can contain a switch and a WAP to allow both wired and wireless connections.

More network devices

- Firewall
  - Hardware or software to protect a computer from unwanted intrusion.
  - Either inbuilt in the router or a separate piece of hardware.
- Bridge
  - A device to connect two LANs, or separate them into two sections.
  - Can be either wired or wireless.
- Modem
  - A device that translates digital signals from the computer to analog signals used for the phone lines.
  - Offers slow connections are now only used for backups or if there is no other way to get internet access.
- VoIP (Voice over Internet Protocol)
  - Collection of technologies, devices and protocols that allows voice communication over internet.
  - Spoken words are converted into data packets and sent over the network, like any other data packets.

Protocols

A set of rules describing how different entities communicate over a network.

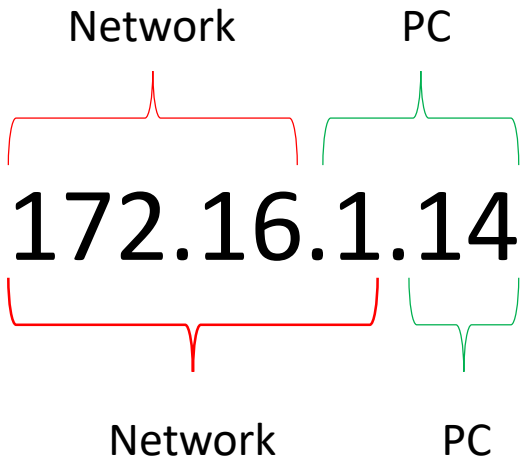
TCP/IP (Transmission Control Protocol/Internet Protocol)

- TCP/IP is (probably) the most well known acronym
  - The two most used protocols when information is sent across an IP network.
- One aspect of the IP protocol is that each unit has a unique address
- There are two versions
  - IPv4
  - IPv6

IPv4

- IP-address
  - A unique address for each computer on the internet.
  - Consists of four octets, with value ranging from 0 to 255.
    - Octet refer to the numbers consisting of 8 bits (=1 byte).
    - 192 = 11000000
    - Collectively, an IP address is a 32 bit number.
  - Written out each number is separated by a dot (192.168.0.100).
- There are two types
  - Dynamic
    - The computer contacts a DHCP server and gets assigned an IP automatically.
  - Static
    - The computer is manually assigned an IP address.
    - Some effort is needed to be sure the address is unique.

IPv4 – subnet



- Subnet
  - An IP address consists of two parts
    - The network portion (which network the computer is on)
    - The host portion (the individual number of the computer)
  - The subnet mask defines which portion is which.
    - Same structure as an IP address
    - The value 255 indicates the network portion, 0 the individual computer.
    - IP: 172.16.1.14, subnet: 255.255.255.0 (see figure)
    - Network: 172.16.1, This computer: 14
- Gateway
  - The gateway address is the IP address of the host enabling internet access.
  - This should always be on the same network as the computer.

URL vs IP (IPv4)

- Uniform Resource Locator (URL)
  - i.e. web address
  - Format: protocol://hostname/other_information
  - https://money.cnn.com/international
- DNS Server
  - The server responsible for converting domain names (URLs) to IP addresses.
  - This server is often on a different network (e.g. your ISP).
  - But could also be a local server, particularly if you are part of a big company.

IPv4 Classes

- IP addresses are classified into three groups based on the first number.

Class	Range	Networks	Hosts pr. network	Who uses it?	Default subnet
A	1 – 126	126	16,777,214	Large Corps, ISPs	255.0.0.0
B	128 – 191	16,384	65,534	Corps, Universities	255.255.0.0
C	192 – 223	2,097,152	254	Small offices/home offices	255.255.255.0

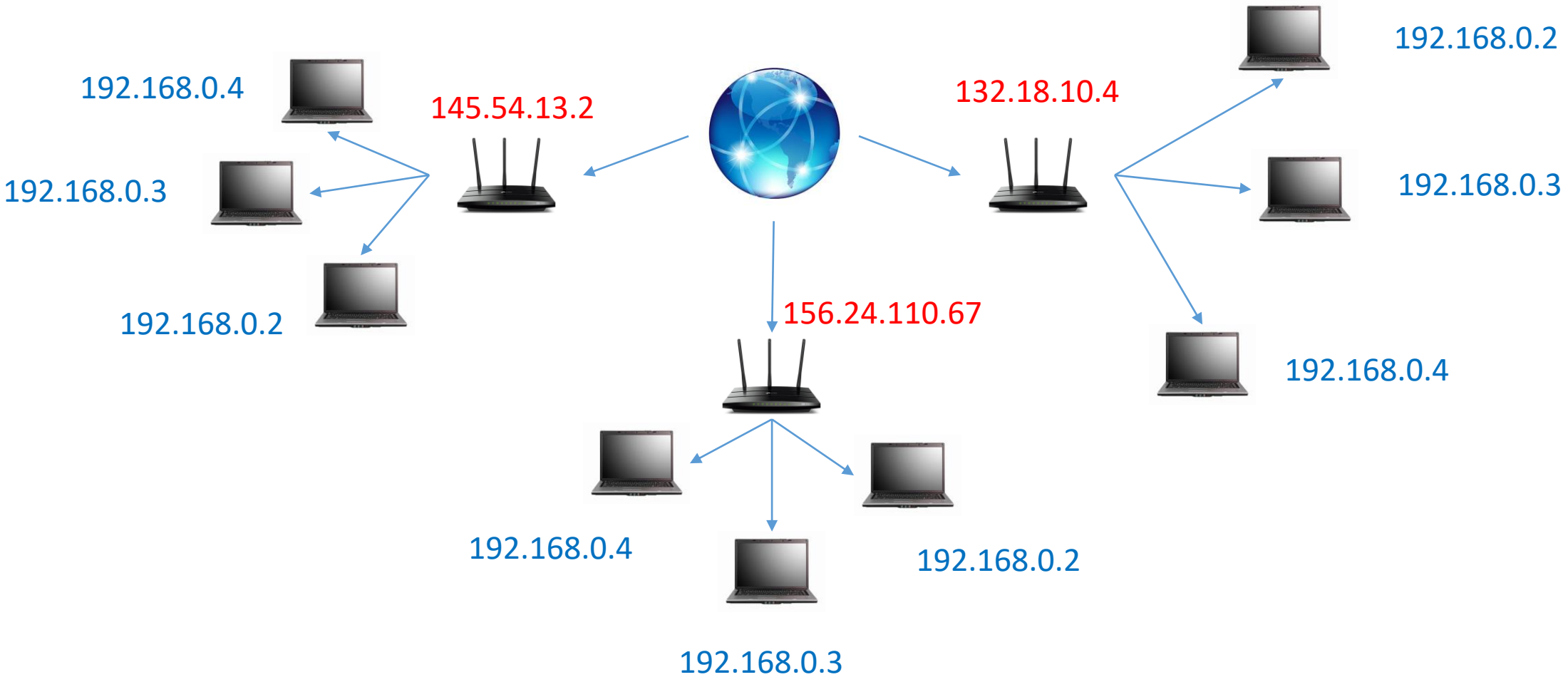
Notice:

- 127 is skipped, this range is only used for loopback testing. (i.e. Looping a signal back to the transmitting unit.)
- Class D (224-239) is used for multicast testing.
- Class E (240-255) is reserved.
- There are only 254 possible hosts in Class C, because 0 is the network name and 255 is the broadcast address.
  - Messages sent to the broadcast address are received by all attached hosts.
- The total number of hosts is just under four billion, and there is not much room left for more devices.
  - This is a problem when more and more devices want internet access. (Internet of Things).

IPv4

- Public
  - Open and displayed directly to the internet.
  - Anyone can (try to) connect to these addresses.
- Private
  - Hidden from view and not open for direct access.
  - Reserved private IP ranges:
    - Class A: 10.0.0.0 – 10.255.255.255
    - Class B: 172.16.0.0 – 172.31.255.255
    - Class C: 192.168.0.0 – 192.168.255.255
- Loopback address - 127.0.0.1
  - This address points back to the device itself, can be used to test if IPv4 is working

Private vs. Public



IPv4 vs. IPv6

- The ~4 billion IP addresses in IPv4 are almost all used up.
- IPv6 is the upgrade, designed to fix this problem.
  - And also increase security
- IPv4 is 32 bit (4 groups of 3 digits each)
  - 000.000.000.000
- IPv6 is 128 bit (8 groups of 4 digits each)
  - 0000.0000.0000.0000.0000.0000.0000.0000

IPv6

- An IPv6 address: 2001:7120:0000:8001:0000:0000:0000:1F10
- Global routing prefix:
  - 2001:7120:0000
- Subnet:
  - 8001
- Individual interface ID:
  - 0000:0000:0000:1F10
- Abbreviations:
  - Remove leading zeros
  - Truncate consecutive groups of zeros to a double colon (::). (only once)
- A shortened IPv6 address: 2001:7120:0:8001::1F10

Locating (your) IP address

- Windows:
  - ipconfig
- Linux:
  - ifconfig
  - nslookup (ask DNS to convert host name to IP address)
- MacOSX
  - ifconfig

ifconfig and ipconfig

```
$ ifconfig
enp1s0    Link encap:Ethernet  HWaddr 00:25:22:4e:3f:13
          inet addr:172.21.126.40  Bcast:172.21.126.255  Mask:255.255.255.0
          UP BROADCAST RUNNING MULTICAST  MTU:1500  Metric:1
          RX packets:291775 errors:0 dropped:0 overruns:0 frame:0
          TX packets:76817 errors:0 dropped:0 overruns:0 carrier:0
          collisions:0 txqueuelen:1000
          RX bytes:340656893 (340.6 MB)  TX bytes:11072860 (11.0 MB)

lo        Link encap:Local Loopback
          inet addr:127.0.0.1  Mask:255.0.0.0
          UP LOOPBACK RUNNING  MTU:65536  Metric:1
          RX packets:870 errors:0 dropped:0 overruns:0 frame:0
          TX packets:870 errors:0 dropped:0 overruns:0 carrier:0
          collisions:0 txqueuelen:1
          RX bytes:70789 (70.7 KB)  TX bytes:70789 (70.7 KB)
```

```
C:\Users\Harald>ipconfig

Windows IP Configuration


Ethernet adapter Ethernet:

   Connection-specific DNS Suffix  . :
   Link-local IPv6 Address . . . . . : fe80::6c31:cfa3:aa8b:fba9%5
   IPv4 Address. . . . . . . . . . . : 10.0.2.15
   Subnet Mask . . . . . . . . . . . : 255.255.255.0
   Default Gateway . . . . . . . . . : 10.0.2.2
```

Web page protocols

- HTTP (Hypertext Transfer Protocol)
  - Transfers web pages and other web-based materials.
  - Connects between web server and web browser.
  - Usually compressed but not secured.
- HTTPS (Hypertext Transfer Protocol Secure)
  - Like HTTP.
  - Includes a protocol to encrypt the information sent.
    - Secure Sockets Layer (SSL)
  - Increasingly more common, and should be standard for any financial or confidential web-sites.

Ports

- When two computers want to talk together
  - They have to use the same protocol
    - Choice of protocol depends on type of communication.
  - Open a port on the network adapter (outbound).
  - Have an open port on the inbound network adapter.
- When visiting a web-site (www.google.com)
  - The protocol used is HTTP (HyperText Transfer Protocol)
  - The protocol chooses an unused port on your computer (outbound port).
  - Google.com's web-server uses a specific port, usually 80, to accept incoming sessions (inbound port).

More ports

- There are a total of 65,536 ports. (0 – 65,535)
  - And about as many protocols.
- The four most common protocols and their ports

Protocol	Port	Name
FTP	21	File Transfer Protocol
SSH	22	Secure Shell
HTTP	80	Hypertext Transfer protocol
HTTPS	443	HTTP Secure

Servers

Centralizing tasks and data management

Server roles

- File servers
- Authentication servers
- Print servers
- E-mail servers
- Web server

Server roles

- DHCP server
  - Responsible for handing out IP addresses to clients.
- DNS server
  - Translating domain names (i.e. ‘google.com’) to IP addresses (8.8.8.8).
- Proxy server
  - A gateway between the client and the website.
  - Can filter content and restrict access to certain websites.
  - Can store (cache) data from a website so next user won’t have to get it from the internet.

Connecting to servers

- Accessing a server, using SSH (secure socket shell)
  - Open a connection to the server
  - Authenticate (username and password)
  - Start working (CLI)
  - Windows – you can use Putty
  - Linux – open a terminal window and use the command “ssh”
- File transfers with FTP
  - Windows – use WinSCP for file browsing and copying
  - Linux – use FileZilla or the command “ftp”

Cables

- Cable material:
  - Copper cable
  - Fiber optic
- Fiber optic is (much) better, but (for now) more expensive
  - Higher bandwidth and longer distance
  - Less affected by environmental interference, less noise
  - The expense is not necessarily the cables themselves, but all the equipment required to use them.

SOHO

Small office / Home office

Internet services

- DSL (Digital subscriber line)
  - High-speed digital data transmission over the phone line.
  - Typically the option for users unable to get cable internet.
  - Two types:
    - ADSL (Asymmetrical DSL)
      - Download speeder is faster than upload. (8 Mb/s to 52 Mb/s down)
    - SDSL (Symmetrical DSL)
      - Installed as separate line
      - Upload and download speeds are equal (symmetrical). (1.5 Mb/s to 5 Mb/s)

Internet services

- Cable Internet
  - Broadband cable supports cable Internet and cable TV.
  - Download speeds from 5 Mb/s to 150+ Mb/s. (Upload is slower).
  - Connetion point at user is a cable modem, which often connects to a router.
- Fiber Optic
  - Copper cables are replaced with fiber optic cables, increasing speed (from 100 Mb/s to 1000 Mb/s).
  - The fibre cable can be installed all the way to the user (Property)
    - Fibre To The Property (FTTP).
  - It is also possible to have the fibre cable stop before that
    - Neighborhood, Cabinet, distribution point, Building/Business, Desktop
    - FTTN, FTTC, FTTdp, FTTB, FTTD

Internet services

- Satellite
  - A parabolic antenna connects via line-of-sight to a satellite.
  - More affected by electrical and natural interferences.
  - High delay (latency) on the signals (0.5 to 5 seconds).
- Cellular
  - GSM, CDMA, GPRS, 4G, LTE, …
  - Wireless WAN (WWAN).
  - Requires a subscription with a cellular provider.

Setup of router for SOHO

- Usually connects to a cable modem (cable internet).
- Often contains a switch and a wireless acces point (WAP)
- Computers connect either wired or wireless.
- Routers often have two IP adresses
  - A private LAN IP adress in the 192.168.x.x range
  - A public address from the ISP (WAN address)
- The router is then the gateway for the devices on the LAN.

Wireless networks.

- Wireless LAN (WLAN), Wi-Fi.
- The protocol for handling wireless connections and communications is called 802.11, and consists of several different versions.
  - 802.11a, b, g, n, ac.

802.11 version	Maximum data rate	Frequency
802.11a	54 Mb/s	5 GHz
802.11b	11 Mb/s	2.4 GHz
802.11g	54 Mb/s	2.4 GHz
802.11n	300/600 Mb/s	5 and/or 2.4 GHz
802.11ac	1.7 Gb/s	5 GHz

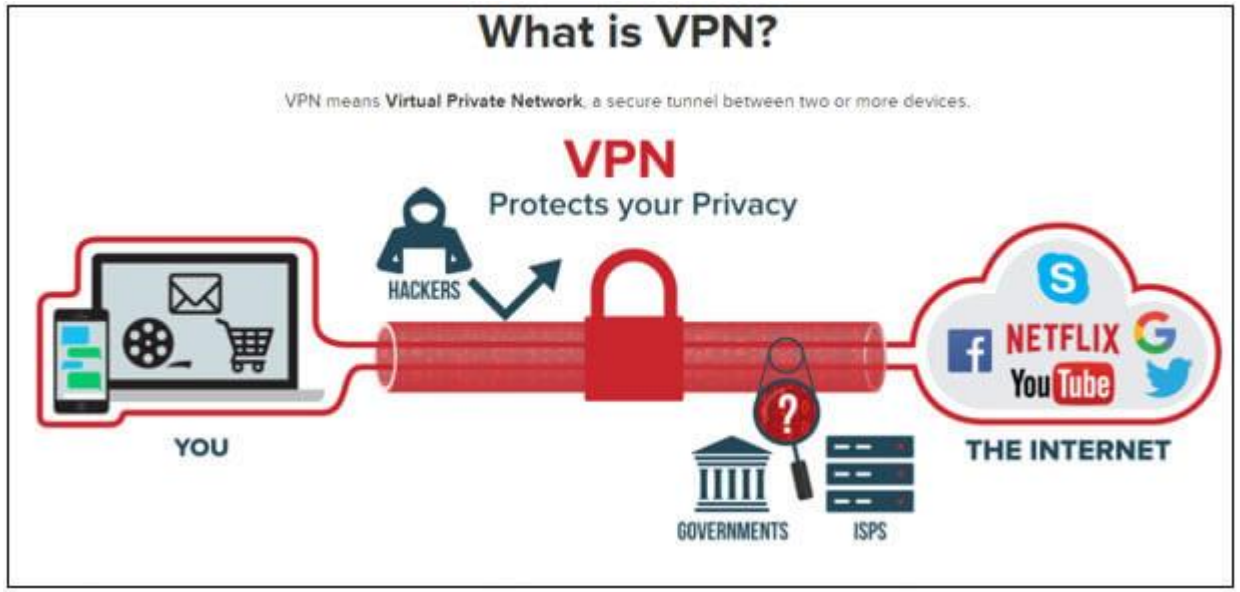
Coverage and distance is also important properties, but depends on many additional factors.

Connecting to a router

- Wired
  - Only require an Ethernet cable
- Wireless
  - The wireless network has its own name, known as Service Set Identifier (SSID)
  - This is used by the user to identify the correct network.
  - The network adapter has to be compatible with the 802.11 protocol used by the router.
    - Some routers allow for multiple protocols to connect, but this can cause reduced efficiency.

VPN

- A virtual private network (VPN) is a technology that creates a safe and encrypted connection over a less secure network, such as the internet.
- A way to be a part of a LAN, even if not physically close to the LAN.



Is the server on?

- The command «ping» will send a small signal and wait for a response.
- From commandline:
  - ping <IP-address>
  - Sends small packages to the target computer, and receives and answer.
  - Will show if your computer is able to talk to the target.
- NB, will keep sending until stopped: <Ctrl+c>
- Some servers might block ping requests

IT Security

Potential threats

- Unauthorized access
- Data destruction (accidental or deliberate)
- Administrative access
- Environmental threats
- Malware

Unauthorized access

- Someone accesses resources without permission.
- Social engineering
  - Gain access through people inside the organization.
  - Often easier than trying to break IT security.

Data destruction

- Data is deleted, corrupted or made inaccessible.

- An extension of unauthorized access
- Accidents, either software- or hardware-based.
- Ignorance/Good intentions

Adminstrative access

- Damage potential is proportional to the level of access
- Administrator accounts have full access to everything
  - What if it gets compromised?
  - What if it’s used by someone inexperienced?
- Not all user know the safe limits to what they can do.
- “If it wasn’t safe, I wouldn’t be allowed to do it.”

Environmental threats

- Heat/Fire
- Humidity/Water
- Dust

- Typical operating conditions:
  - Temperature: 22°C
  - Relative humidity: 30-40%

Malware, types

- Virus
  - Computer program. Main goals to replicate and activate.
  - Attaches to other software for replication.
  - Does not replicate across networks.
- Worm
  - Similar to virus, but can replicate by itself across networks or hardware.
- Trojan Horse
  - Malware that pretends to do one thing, while secretly doing something evil.
  - Does not replicate
- Rootkit
  - Malware with administrator priviliges.
  - Able to hide by modifying anti-malware software to ignore the rootkit.

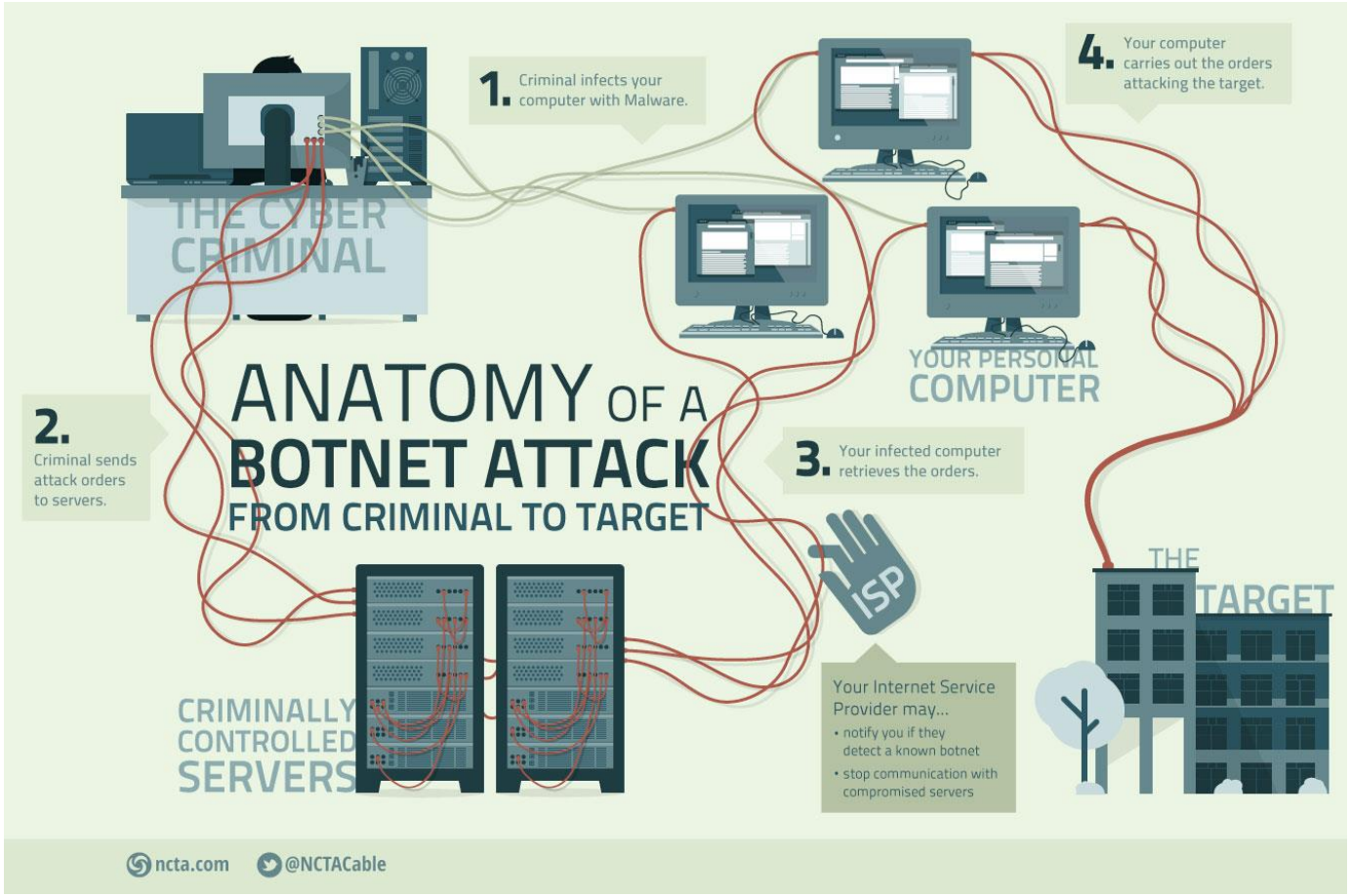
Malware symptoms

- Slow system
- Random crashes
- Files disappeared / renamed / changed permission
- E-mails being sent without your knowledge
- OS updates stops working

Malware, behavior

- Corruption/deletion of data
- Spyware
- Ransomware
- A hijacked bot in a network of many other machines (“botnet”)

Botnets


1. Criminal infects your computer with Malware.
4. Your computer carries out the orders attacking the target.
THE CYBER CRIMINAL
YOUR PERSONAL COMPUTER
ANATOMY OF A BOTNET ATTACK
FROM CRIMINAL TO TARGET
2. Criminal sends attack orders to servers.
3. Your infected computer retrieves the orders.
ISP
THE TARGET
CRIMINALLY CONTROLLED SERVERS
Your Internet Service Provider may...
• notify you if they detect a known botnet
• stop communication with compromised servers
ncta.com
@NCTACable

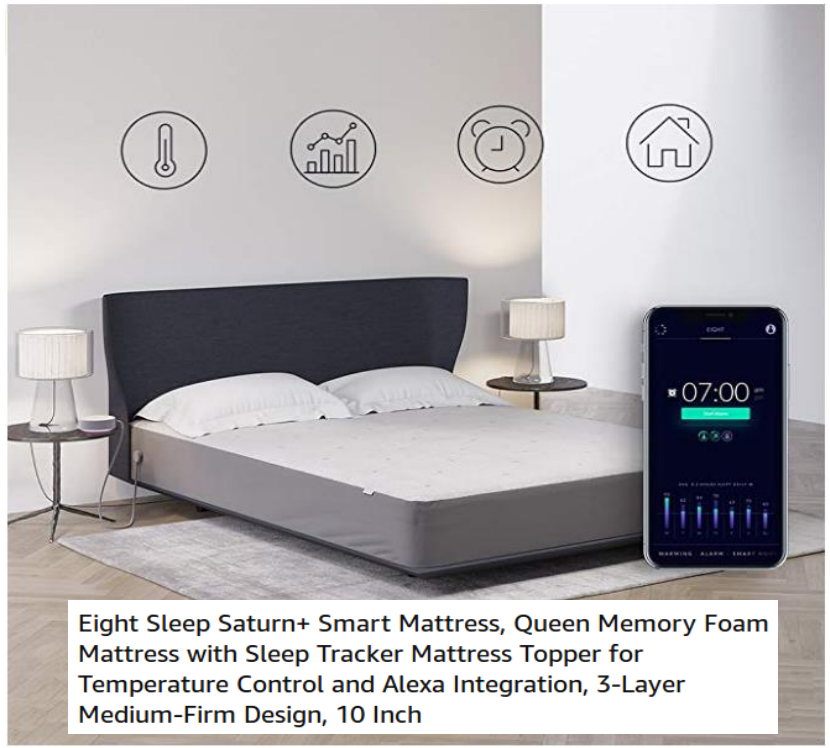
Internet of things - IoT

YD
YANKO DESIGN

PRODUCT DESIGN / TECHNOLOGY / AUTOMOTIVE / ARCHITECTURE / DEALS / RANDOM / SUBMIT / + NEWSLETTER

A SMART HANGER THAT RECOMMENDS CLOTHES BASED ON THE WEATHER FORECAST!

BY SARANG SHETH / 06/04/2018



Eight Sleep Saturn+ Smart Mattress, Queen Memory Foam Mattress with Sleep Tracker Mattress Topper for Temperature Control and Alexa Integration, 3-Layer Medium-Firm Design, 10 Inch

Here's What It Looks Like When A 'Smart Toilet' Gets Hacked [Video]

Malware, attack patterns

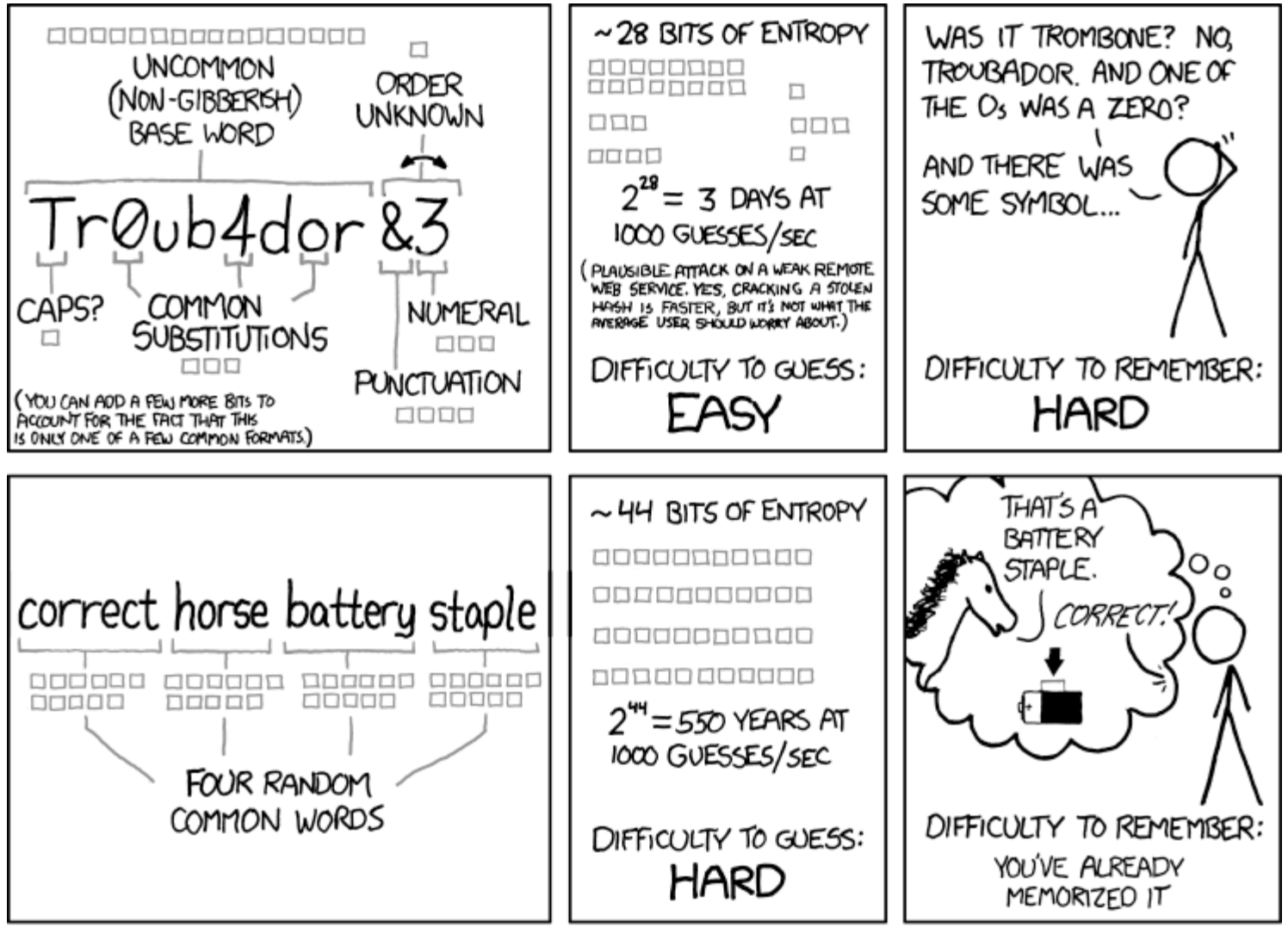
- Zero-day attacks
  - Using vulnerabilities unknown to the developer of the software.
- Spoofing
  - Pretending to be someone or something else by using false information in communication.
- Man-in-the-Middle
  - Accessing an intermediate point in the communication between two systems.
- Session hijacking
  - Interception of authentication information from a targeted system.
- Brute Force
  - Any attack reliant on guessing the content of some data field by making a large amount of attempts.

Security measures

- Access control
  - Limit users access to what they need
- Password
  - What is a strong password?
- Backups
  - Regular backups reduces the impact of most threats.
- Firewall and anti-virus software
  - Update regularly

Passwords

- How does passwords get revealed?
  - Brute force attacks tries every possible combination.
  - Social engineering can be used to guess the password, or get you to reveal it.
  - Keyloggers record all keyboard activity, including the typing of passwords.
  - Servers storing unsecured passwords can get hacked.
- Long and complex passwords can stop brute force attempts
  - But difficult to remember
- Password managers creates strong passwords and remembers them
  - Also avoids typing
  - Usually enough to remember only one password, to the password manager.



https://www.xkcd.com/936/