Privacitat, seguretat i anonimat

Xerrada introductoria

Contacte:

projectenadki@protonmail.com

Índex

Privacitat


Exposed record
Data breach
Protection
digital
classification
search
DATA
PRIVACY
law
anonimous
Metadata
Regulations
Patient privacy
Privacy
RISK
Sensitive Information
Authentication
compliance

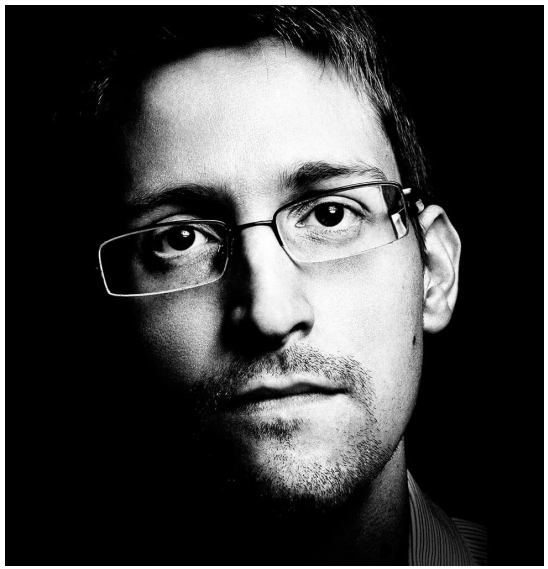
Introducció

Declaració Universal dels Drets Humans
Ningú serà objecte d'injerències arbitràries a la seva vida privada, [...], ni d'atacs a la seva honra i reputació. Tota persona té el dret a la protecció de la llei contra tals injerències o atacs.

Tot i així, tots els països tenen lleis que d'alguna manera limiten la privacitat dels ciutadans.

- Lleis de seguretat nacional
- Lleis de terrorisme

Exemples



Espionatge massiu

Five Eyes

1. Australia
2. Canada
3. New Zealand
4. United Kingdom
5. United States of America

Nine Eyes

1. Denmark
2. France
3. Netherlands
4. Norway

Fourteen Eyes

1. Belgium
2. Germany
3. Italy
4. Spain
5. Sweden

Evaluació dels riscos

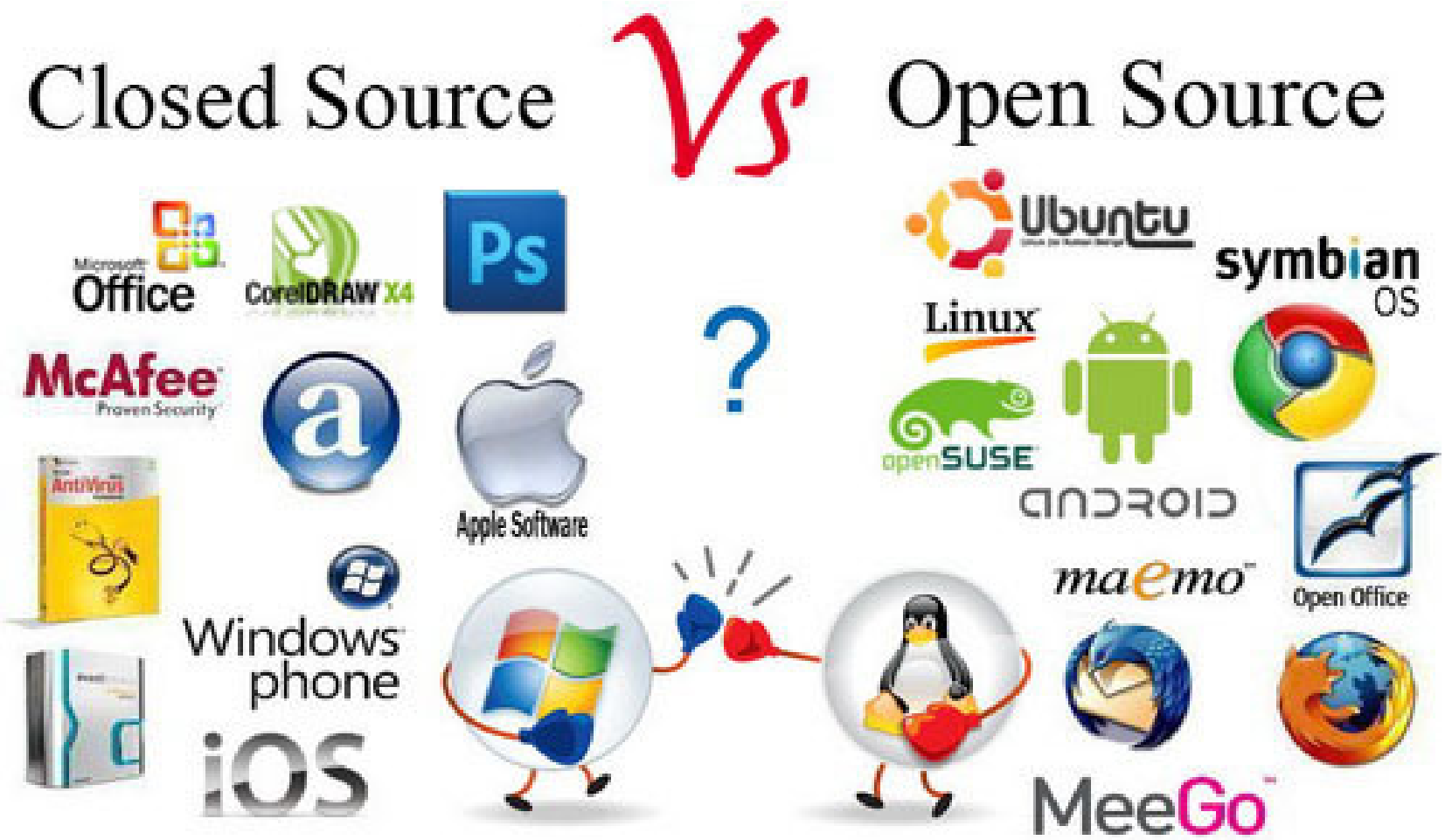
El primer pas és determinar quines són les amenaces i com afrontar-les.

Model d'amenaces, algunes preguntes a fer-se:

- Què val la pena protegir?
- De qui s'ha de protegir?
- Com de probable és que s'hagi de protegir?
- Quant de destructives són les conseqüències en cas de fallar?
- Quin esforç estàs disposat a fer?

Conceptes Bàsics

Software Privat vs Software Lliure



Centralització vs Descentralització

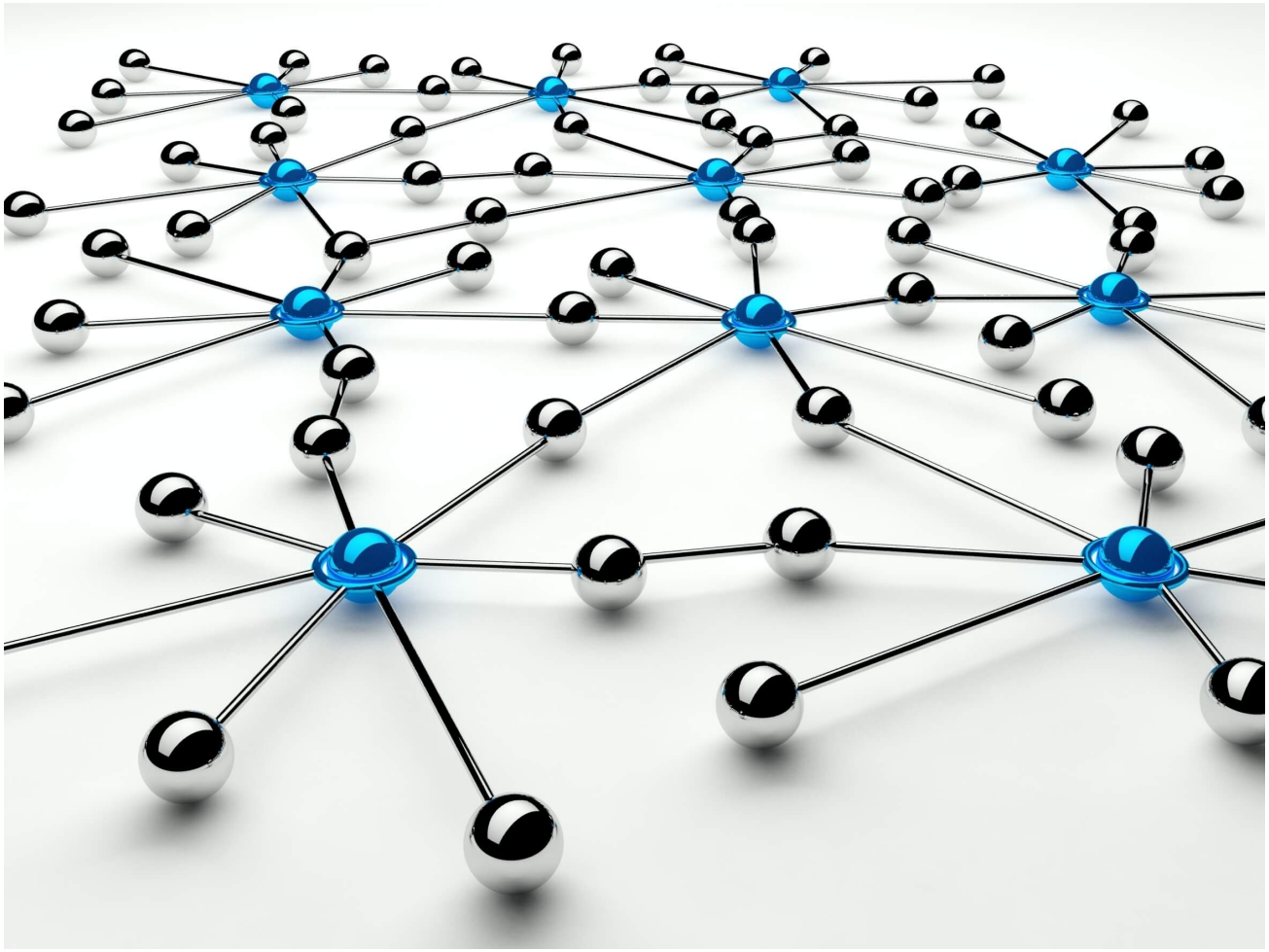
Centralized Framework

Decentralized Framework

Xifratge punt a punt

Internet

Internet



Conclusions

Tenim control de:

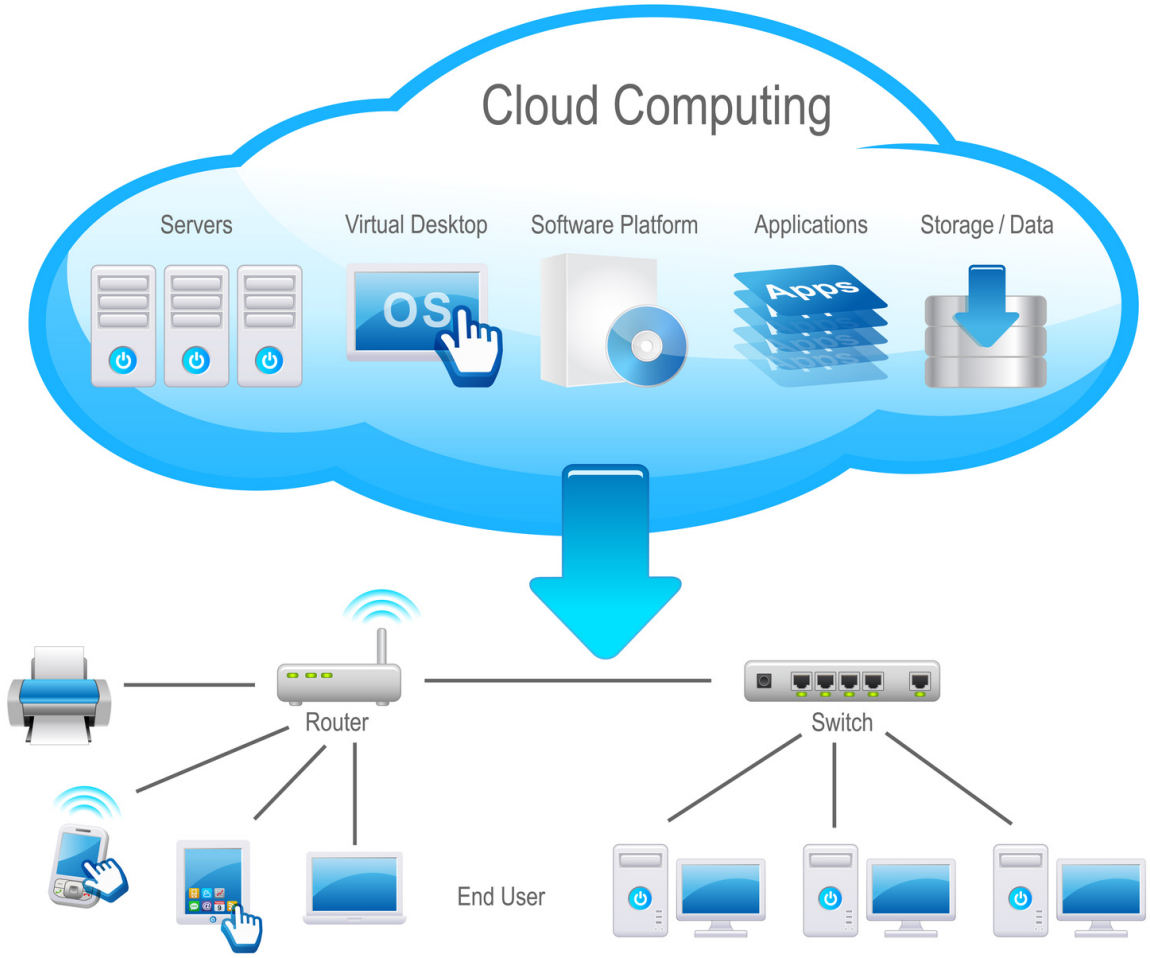
- Dispositius de la xarxa interna
- Router "de casa"

No tenim control de:

- ISP: empresa de telefonia
- Routers intermitjos: delincuents, empreses espionatge, governs...
- Servidor final: empresa privada

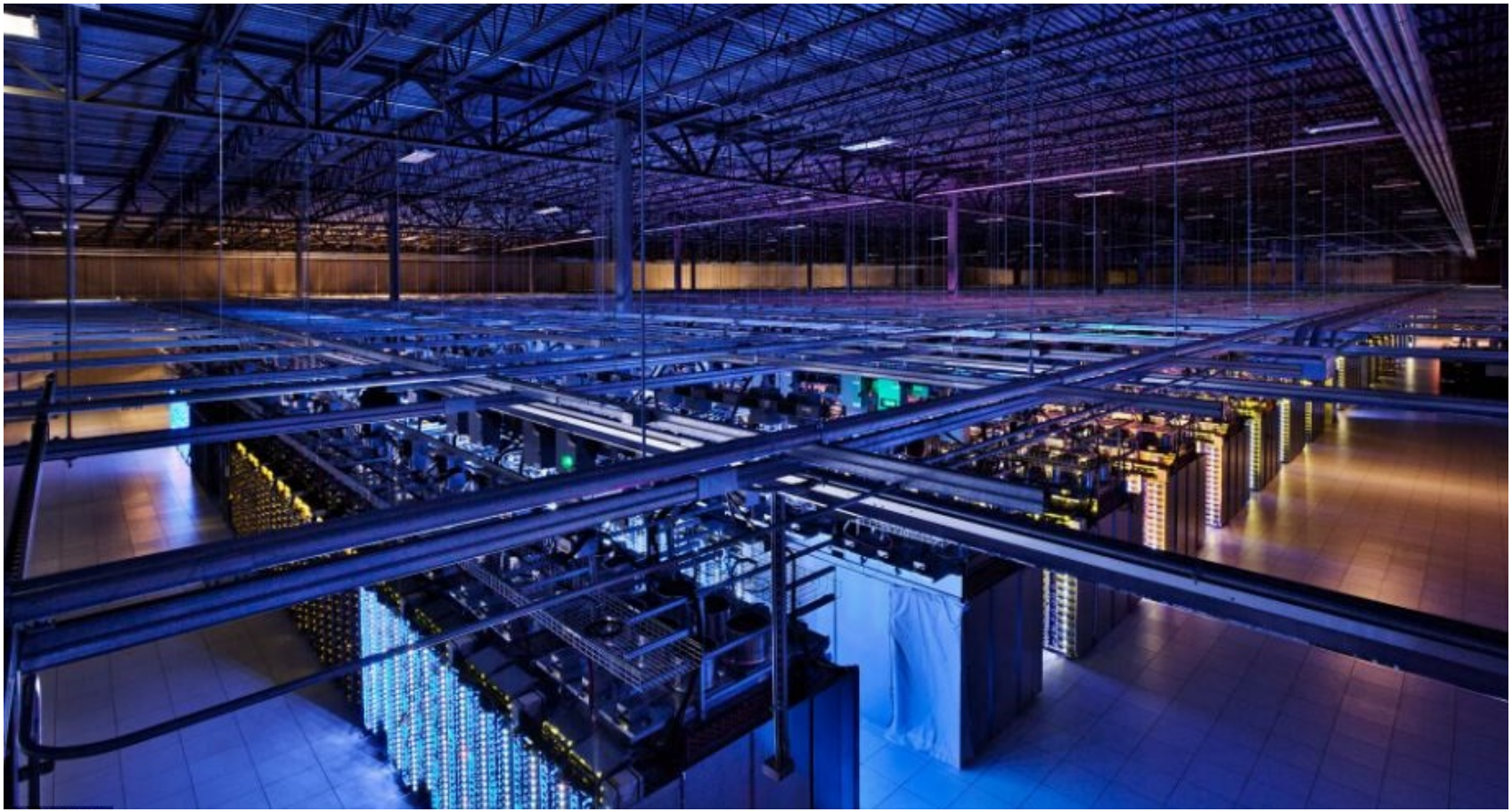
Cloud

Què és?


Cloud Computing
Servers
Virtual Desktop
Software Platform
Applications
Storage / Data
OS
Apps
Router
Switch
End User

Exemple

Exemple



Conclusions

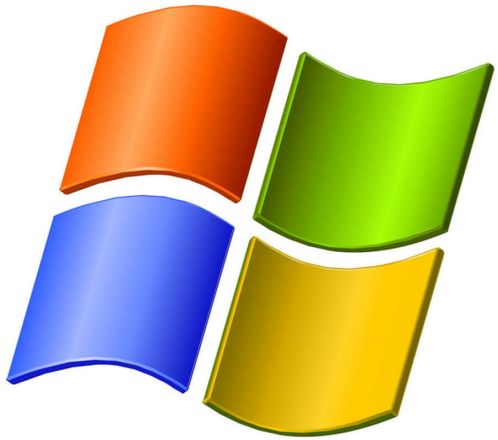
A tenir en compte:

- Les nostres dades i documents s'emmagatzemen a servidors d'empreses privades.
- No es pot saber si compleixen les lleis de privacitat.
- No es pot saber si venen les dades a tercers.
- No es pot verificar la seguretat de les seves instal·lacions.

Ordinador

Windows

- 90% de quota de mercat
- Fàcil d'utilitzar
- Software privat
- És necessari antivirus (molts virus)
- Preu: 200 euros

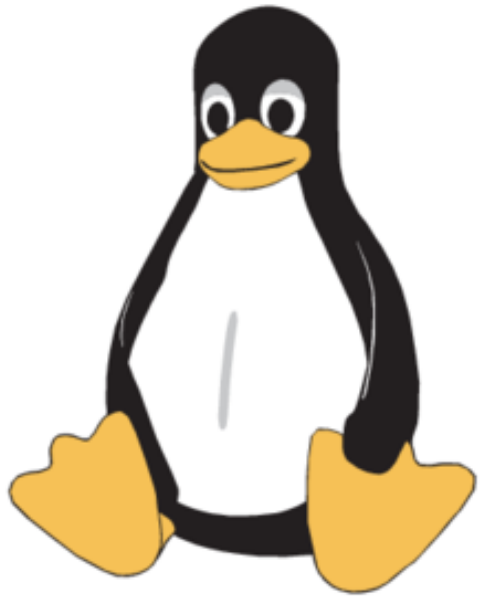


OS X

- 7% de quota de mercat
- Fàcil d'utilitzar
- Software privat
- No hi ha gaires virus
- Software i hardware restrictiu
- Preu: +800 euros

Linux

- 1% de quota de mercat
- Difícil d'utilitzar
- Software lliure
- No hi ha gaires virus
- Diversos tipus de sistema operatiu
- Preu: 0 euros



Linux - Distribucions

Whonix

- Basat en Linux (Debian i Tor)
- Software lliure
- Centrat en la privacitat i anonimat
- Persistència
- Configurat per funcionar amb Tor

Tails

- Basat en Linux (Debian)
- Bootar des de USB
- Software lliure
- Centrat en la privacitat i anonimat
- Bastant restrictiu en quant a instal·lar software o modificar el sistema operatiu
- Preu: 0 euros

Contrasenyes

Contrasenyes segures

Recomanacions:

1. Més de 8 caràcters
2. Alfanumèrica: lletres i números (o símbols)
3. Majúscules i minúscules
4. No repetir contrasenyes
5. Canviar contrasenyes freqüentment

Suggerències:

- Frases (ex. ViatjeAParisMoltBonic)
- Afegir complexitat (ex. Viatje.A.Paris.Molt.Bonic!)

Atacs

Complexitat:

- només minúscules: 3:30 hores
- majúscules i minúscules: 1 mes i 9 dies
- alfanumèrica: 5 mesos
- alfanumèrica i símbols: 9 anys i 6 mesos

Fàcil d'endivinar:

- Noms de familiars o mascotes
- Dates importants
- Patrons reconeguts (ex. canviar les e per 3, les a per 4, ...)

Gestor de contrasenyes

Servei que emmagatzema contrasenyes de manera segura: KeePass

- Multiplataforma
- Software lliure
- Contrasenyes xifrades
- Interficie antiquada
- No connexió a Internet
- Preu: 0 euros

Xifratge

Disc Dur - Windows

BitLocker

- Exclusiu per Windows PRO
- Software propietari
- Fàcil de configurar i ràpid
- Preu: 99 - 200 euros

VeraCrypt

- Multiplataforma
- Software lliure
- Més complicat de configurar i lleugerament més lent
- Preu: 0 euros

Disc Dur - OS X

FileVault

- Exclusiu per MAC
- Software propietari
- Fàcil de configurar i ràpid

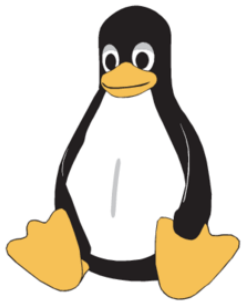
VeraCrypt

- Multiplataforma
- Software lliure
- Dependecia de OSXFUSE
- Més complicat de configurar i lleugerament més lent
- Preu: 0 euros

Disc Dur - Linux

Durant la instal·lació (LUKS)

- Fàcil de configurar i ràpid
- Adaptat per sistemes Linux



VeraCrypt

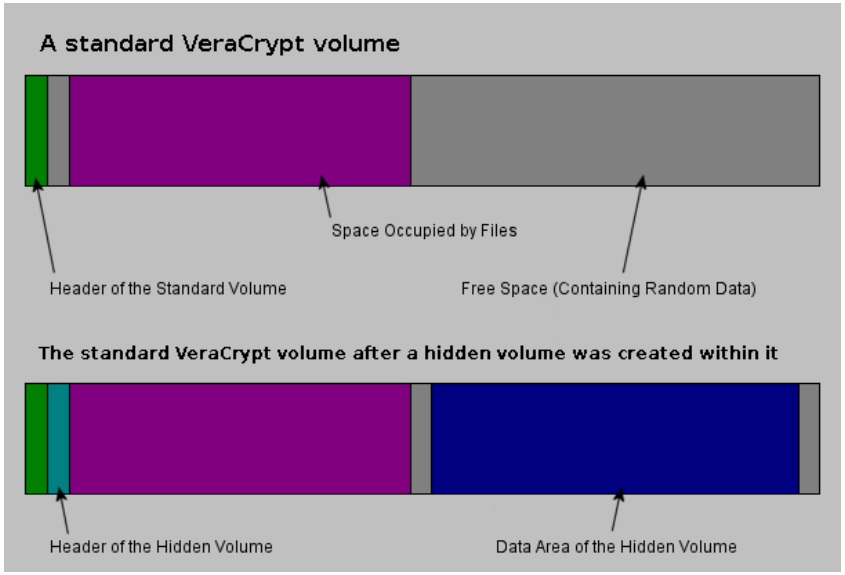
- Multiplataforma
- Software lliure
- Més complicat de configurar i lleugerament més lent
- Preu: 0 euros

Veracript - USB / Particions / Fitxers

VeraCrypt

- Permet xifrar particions
- Permet xifrar USB
- Permet xifrar fitxers
- Permet guardar tots els documents xifrats en un sol fitxer. Facilita la movilitat.
- Tan per xifrar com per desxifrar, es necesari que el programa estigui instal·lat.

Veracript - Carpeta fantasma



- Veracrypt crea dues petites particions.
- S'assigna una contrasenya a cada una.
- Depenent de la contrasenya introduida al desxifrar, es mostrarà un contingut o un altre.

A tenir en compte

- Protegeix només contra atacants que tinguin accés físic, no d'atacs dirigits des de Internet.
- No es pot recuperar la contrasenya a no ser que es disposi d'una clau de recuperació.
- Un cop xifrat, no es poden recuperar les dades.
- Xifrar tot el disc evita filtracions.

Introducció

Smartphone

Actualment els smartphones són ordinadors en miniatura capaços de fer gaire bé el mateix que un ordinador portàtil o de sobretaula.

Això implica que, igual que els ordinadors, tenen problemes de seguretat i la privacitat de l'usuari pot ser compromesa.

De fet, és més fàcil comprometre un dispositiu mòbil ja que els usuaris no estan concienciats.

Sistema operatiu




Companyies


HUAWEI
MOTOROLA
NOKIA
Connecting People
htc
Sony Ericsson
BlackBerry
micromax
SAMSUNG
hp

Mòbil

Xifratge

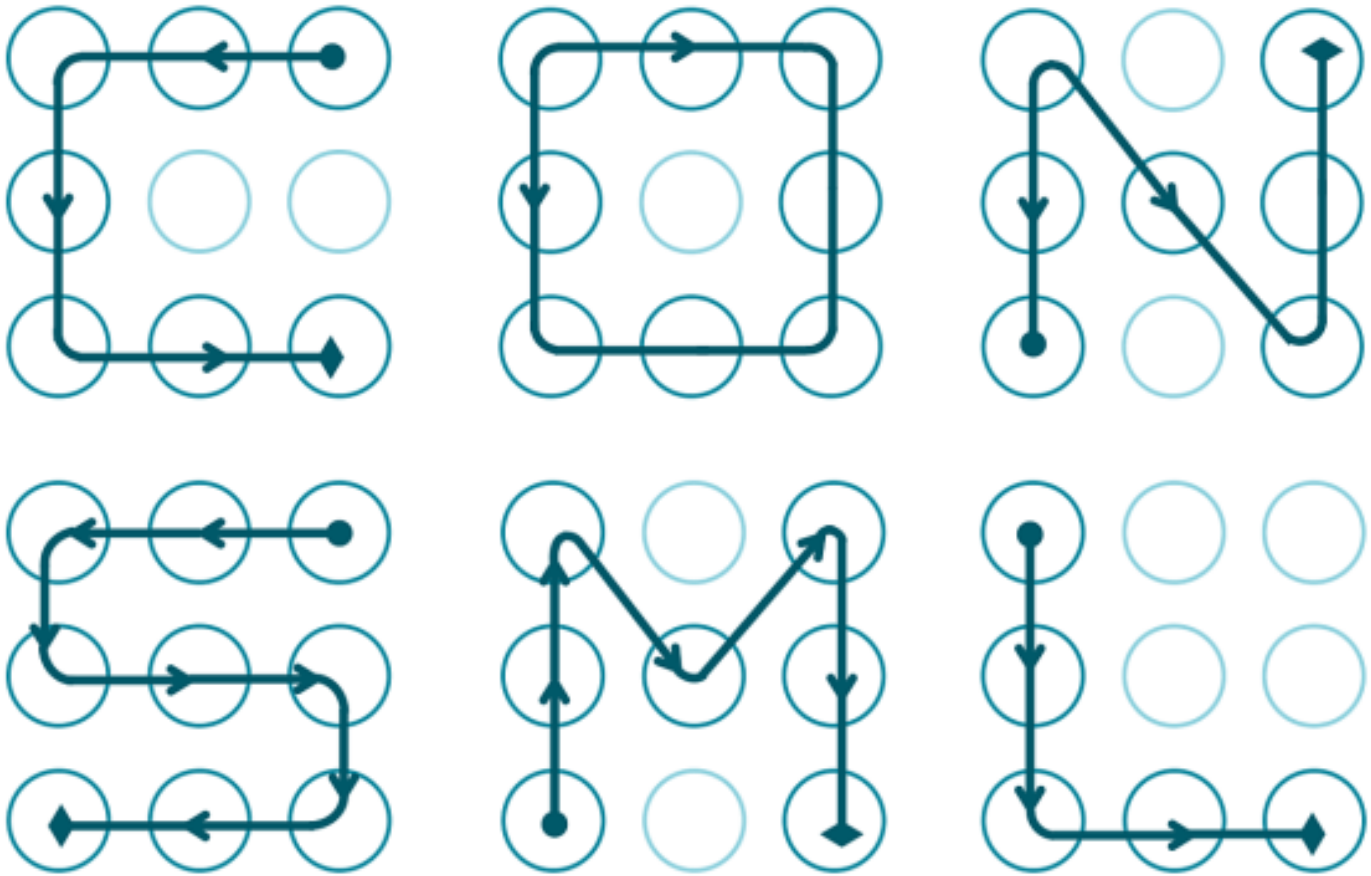
Android

- Opcions del telèfon - Seguretat - Xifratge
- Fer una copia de seguretat abans
- El procés pot durar 1 hora
- Tenir el dispositiu amb més d'un 80% de bateria

iOS

- Mòbils superiors a Iphone3G ja té el disc xifrat per defecte

Patrons



Patrons - Attacs

Totes les combinacions possibles. Si s'exclouen repetir punts, les combinacions es redueixen molt:

- 4 punts: 1624 combinacions (3h 30min)
- 5 punts: 7152 combinacions (7h 10min)
- 6 punts: 26016 combinacions (55h 30min)
- 7 punts: 72912 combinacions (6d)
- 8 punts: 140704 combinacions (12d 12h)
- 9 punts: 140704 combinacions (12d 12h)

Pin

Dos punts molt importants sobre com protegir-nos dels atacs mencionats:

1. Escollir una contrasenya forta
2. Activar que el mòbil es bloquegi al cap de X intents
   Per exemple:
   - 3 intents: 30 segons
   - 5 intents: 5 min
   - 10 intents: 30 min
   - 15 intents: 2h

   Això incrementa exponencialment el temps que s'ha d'invertir per descobrir una contrasenya usant atacs de força bruta.

Emprempta dactilar i reconeixement facial

Avantatges:

- No és necessari recordar una contrasenya
- No poden veure la contrasenya si es desbloqueja en públic
- Els atacs de força bruta passen a ser ineficients

Desvantatges:

- Si és compromesa, mai més es podra canviar
- S'està investigant com extreure premses dactilars i cares de fotografies
- Molt fàcil d'immovilitzar i forçar a l'usuari per desbloquejar el telèfon

Aplicacions malicioses

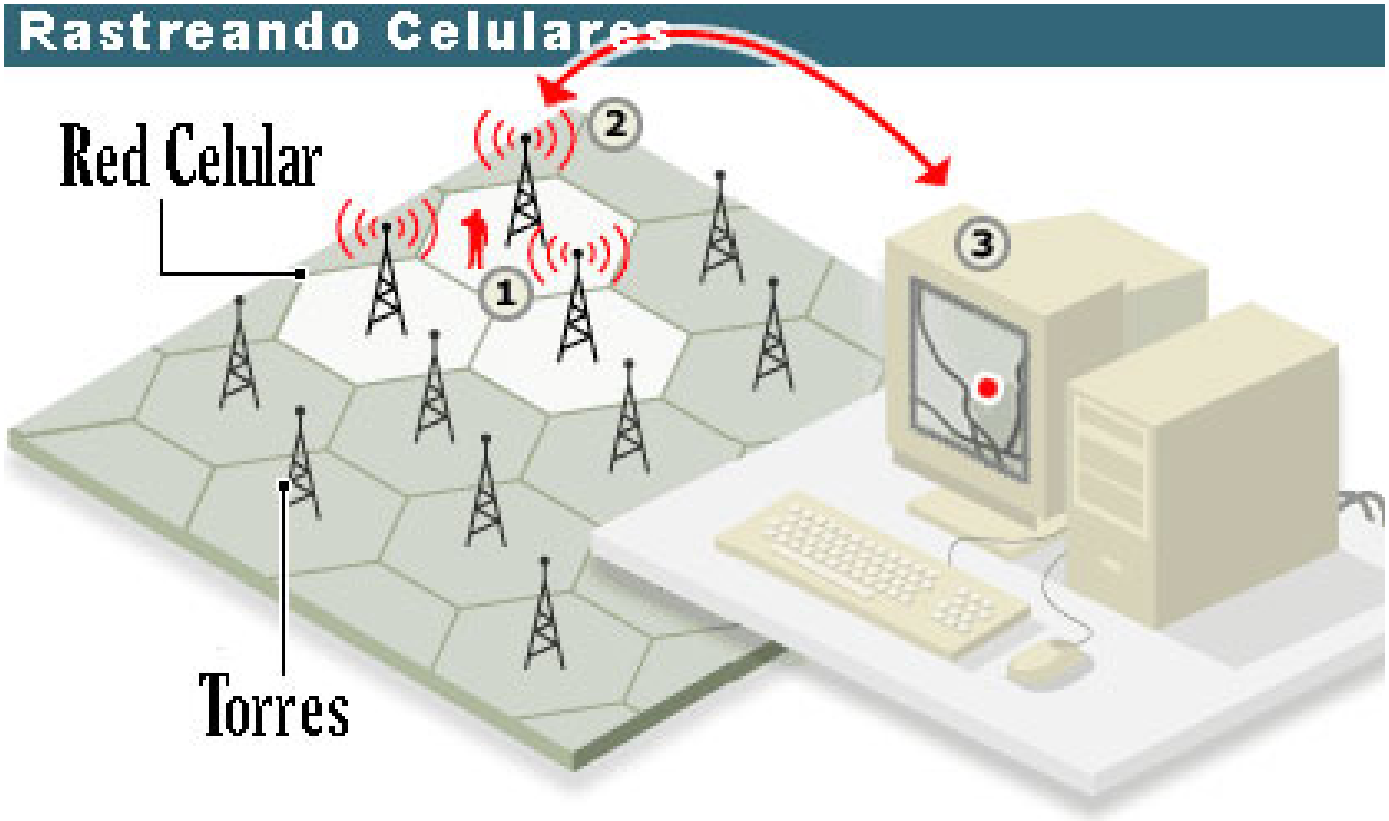
Existeixen milers d'aplicacions malicioses a la botiga d'Android i d'Apple.

És important aprendre a detectar aplicacions malicioses:

- Al descarregar, verificar l'empresa i l'informació de l'aplicació
- Detectar si l'aplicació demana més permisos dels necessaris
- Detectar si l'aplicació demana massa informació personal o, fins i tot, contrasenyes

Rastreig de localització

Torres de telefonia



Torres de telefonia

Un operador pot localitzar un telèfon si:

- El dispositiu està encés
- El dispositiu està registrat a la xarxa

A més a més, depenent de la companyia i el telèfon, l'operador pot calcular amb moltíssima precisió la localització del dispositiu, utilitzant la potència de la senyal entre el dispositiu i cadascuna de les torres.

Evasió

No hi ha cap manera de d'escapar d'aquest tipus de rastreig.

Simulador de torre telefònica

El govern o les autoritats utilitzen torres de telefonia falses, IMSI (International Mobile Subscriber Identity) catcher, per obtenir la presència física i/o interceptar les comunicacions dels dispositius.

Detecció

Algunes aplicacions diuen de detectar els simuladors, però la detecció és imperfecta

Wifi i Bluetooth

Quan un dispositiu té Wifi o Bluetooth obert i encara que no estigui utilitzant-ho activament, transmet ocasionalment senyals enviant la direcció MAC d'aquest.

Què és la direcció MAC?

- MAC: Media Access Control
- És un identificador únic de cada dispositiu
- És coneix també com a direcció física
- Exemple: D4:BE:D9:8D:46:9A

GPS

El GPS (Global Position System) permet calcular la localització d'un dispositiu de manera ràpida i exacta.
El GPS opera basat en l'anàlisi de les senyals que envien uns satèl·lits al servei públic, operats pels EEUU.

Falsa Creença

Els satèl·lits NO observen ni tenen coneixement de l'ubicació dels dispositius dels usuaris, només emeten senyals.

GPS

Són les aplicacions que, si tenen permisos, fan les peticions al satèl·lit per obtenir la localització del dispositiu.

- Aplicacions instal·lades per l'usuari
- Aplicacions del proveidor d'Internet
- El sistema operatiu i software de tercers
- Navegant per Internet

On poden enviar la localització:

- Altres usuaris que utilitzin la app
- Proveidor d'Internet
- Servidors d'empreses privades

Recomanacions

Si s'han de tenir converses sensibles és recomanable apagar els mòbils, o inclús treure les bateries.

- Deixar o apagar el mòbil a casa
- Apagar els telèfons, tenint en compte que si s'apaguen tots de cop al mateix lloc el proveidor ho sabrà
- Deixar el telèfon a una altra habitació, tenint en compte que el proveidor pot arribar a saber que els telèfons estan junts

Navegació

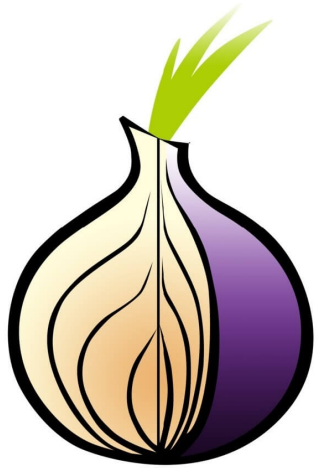
Navegadors

Problemàtics

- Chrome
- Safari
- Internet Explorer

Protegeixen la privacitat

- Firefox
- Tor Browser



Cercadors

Problemàtics

- Google
- Bing
- Yahoo

Protegeixen la privacitat

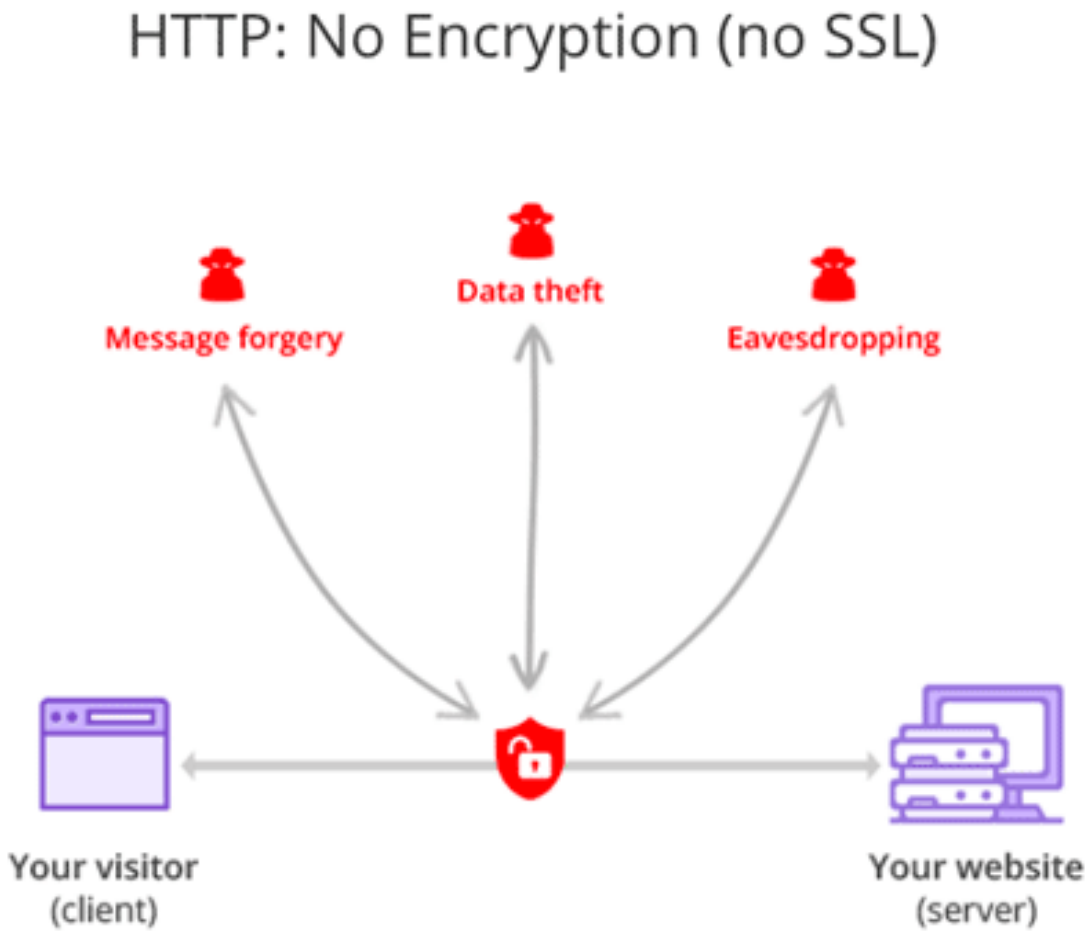
- DuckDuckGo (Estats Units)
- StartPage (Països Baixos)
- searx (software lliure)
- Swisscows (Suïssa)

Extensions

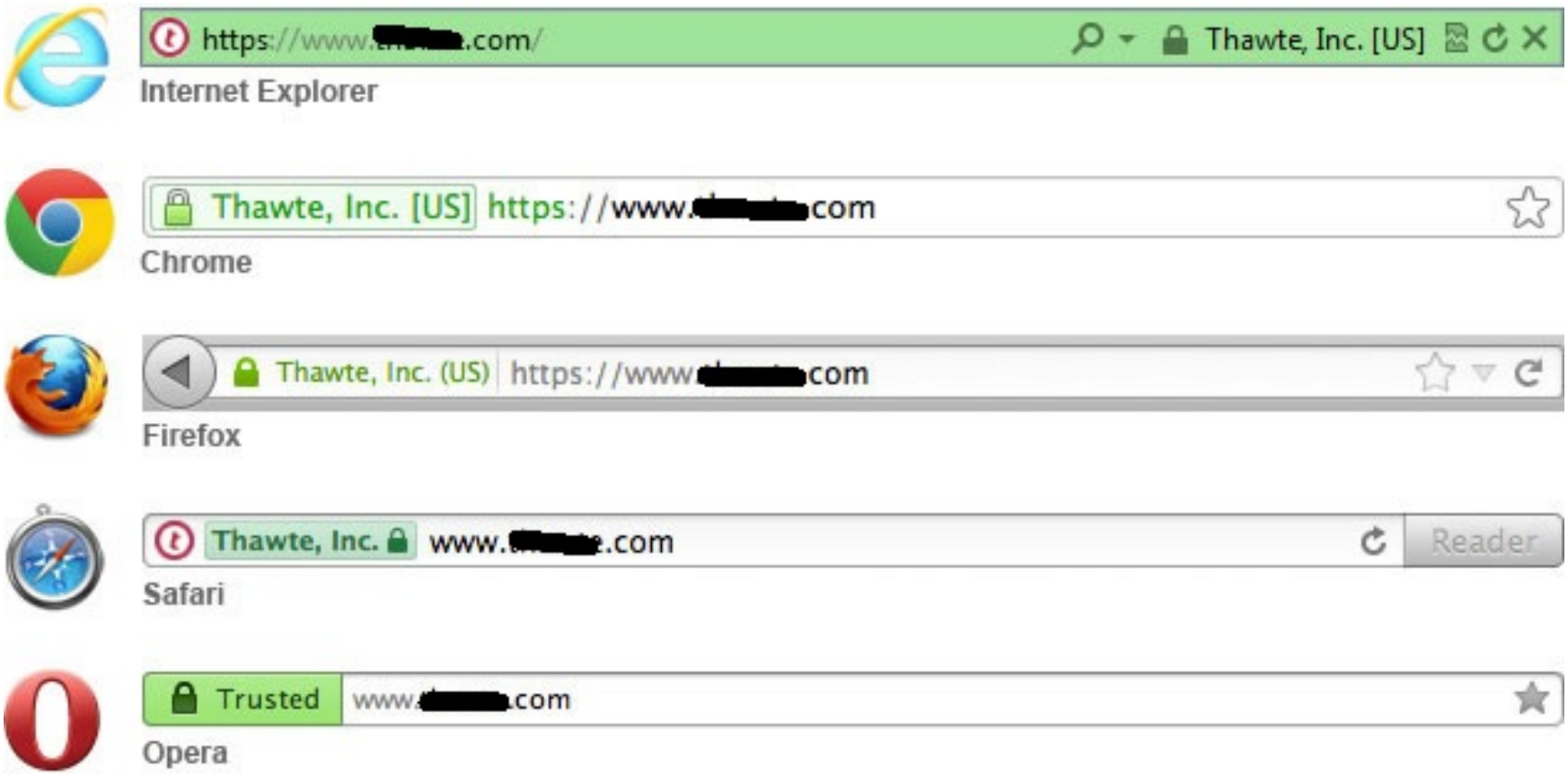
Petits programes que s'instal·len al navegador.

- **uBlock Origin**: bloquejador d'anuncis publicitaris
- **Decentraleyes**: ofereix privacitat contra anuncis publicitaris
- **Cookie AutoDelete**: elimina les cookies automàticament quan es tanca la pestanya
- **HTTPS Everywhere**: fa que totes les comunicacions vagin per HTTPS (col·laboració amb The Tor Project)
- **Terms of Service; Didn't Read**: resumeix i indica el grau de privacitat dels famosos "Terminos y condiciones de uso"
- **Privacy Badger**: evita la geolocalització dels anuncis o de tercers
- **CanvasBlocker**: evita fingerprinting

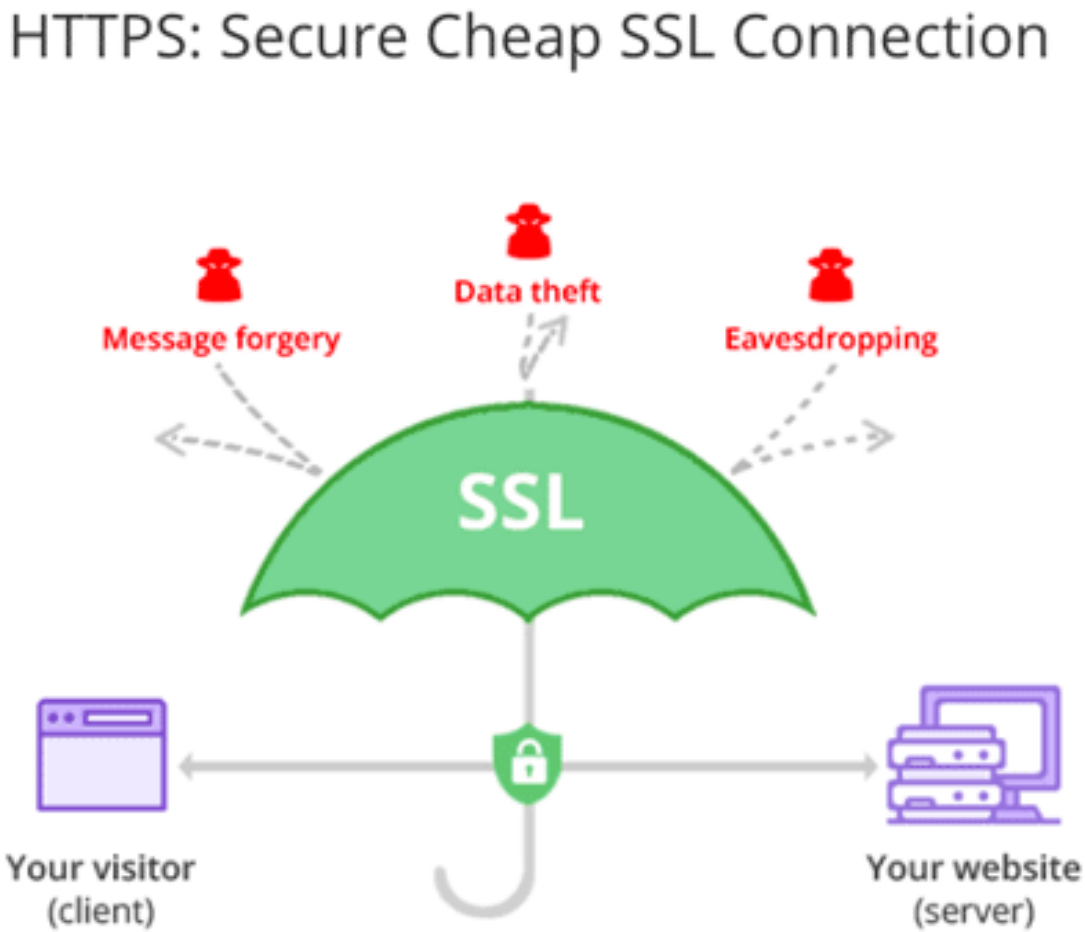
HTTP


HTTP: No Encryption (no SSL)
Message forgery
Data theft
Eavesdropping
Your visitor
(client)
Your website
(server)

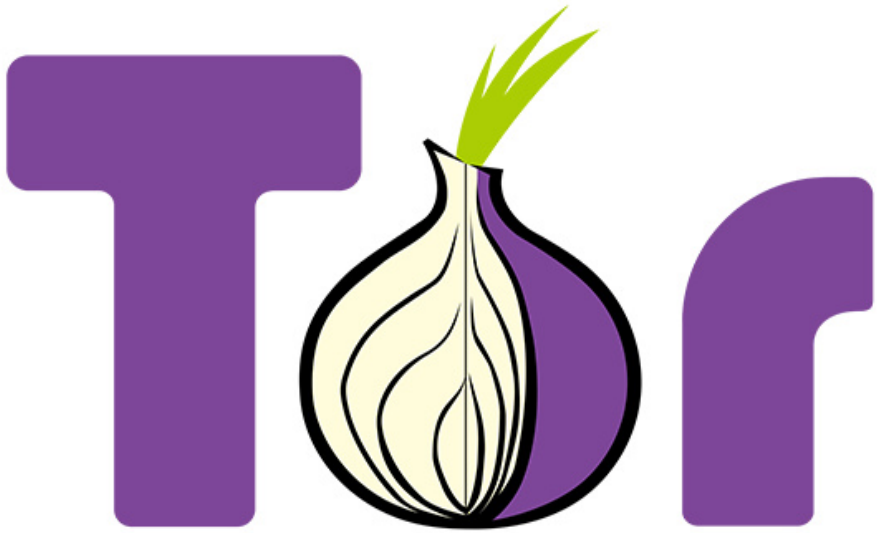
HTTPS


https://www.[redacted].com/
Thawte, Inc. [US]
Internet Explorer
Thawte, Inc. [US] https://www.[redacted].com
Chrome
Thawte, Inc. (US) https://www.[redacted].com
Firefox
Thawte, Inc. www.[redacted].com
Reader
Safari
Trusted www.[redacted].com
Opera

SSL/TLS


HTTPS: Secure Cheap SSL Connection
Message forgery
Data theft
Eavesdropping
SSL
Your visitor
(client)
Your website
(server)

Tor

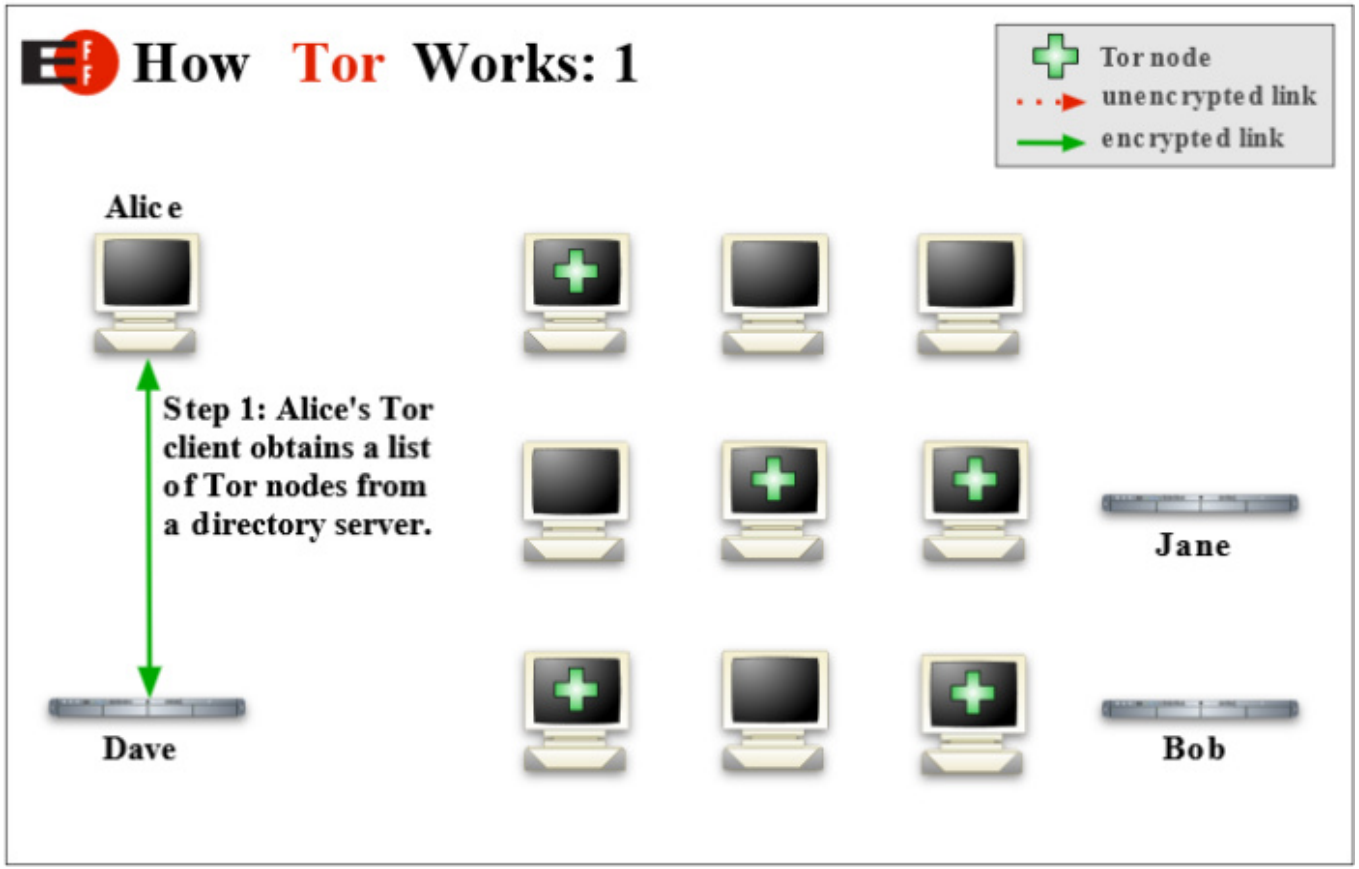


Què és?

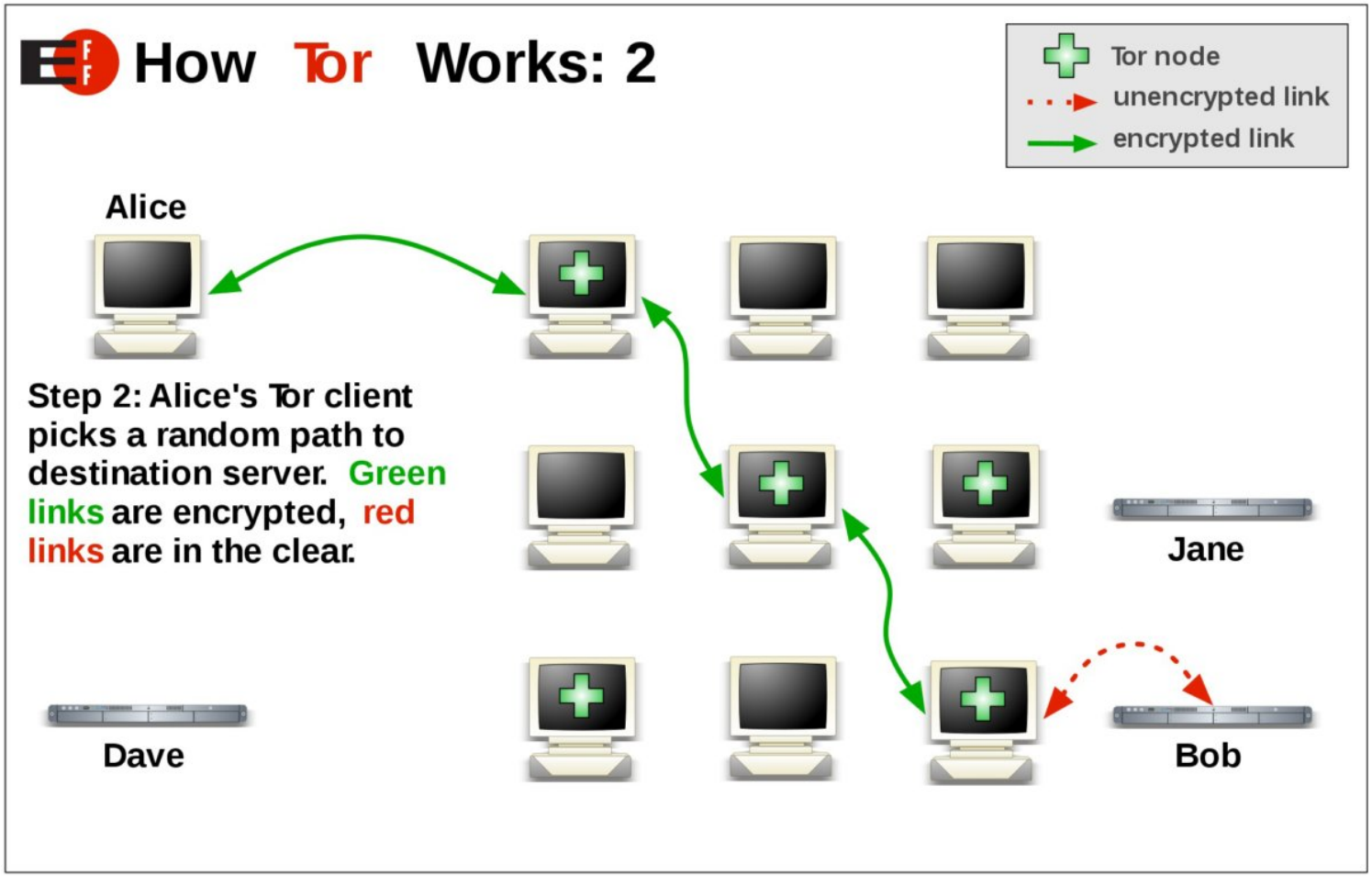
"Promovemos los derechos humanos y defendemos tu privacidad en linea a través del software libre y las redes abiertas."

- Tor Project és una ONG 501(c)3 US
- Software lliure
- Sistema de proxys amb múltiples capes de xifratge
- Defensa contra la vigilància a la xarxa
- Evita que l'usuari sigui rastrejat
- Evadeix censura

Estructura


How Tor Works: 1
Tor node
unencrypted link
encrypted link
Alice
Step 1: Alice's Tor client obtains a list of Tor nodes from a directory server.
Jane
Dave
Bob

Estructura


How Tor Works: 2
Tor node
unencrypted link
encrypted link
Alice
Step 2: Alice's Tor client picks a random path to destination server. Green links are encrypted, red links are in the clear.
Jane
Dave
Bob

VPN

Què és?

Virtual Private Network

Xarxa virtual capaç de connectar diversos dispositius com si estiguessin físicament a un mateix lloc.

- Integritat: xifra les comunicacions entre el client i el servidor VPN
- Privacitat: amaga l'IP del client
- Permet evitar la censura (geolocalització)

Estructura

Empreses VPN

Gratuites:

- Hotspot Shield Free VPN
- ProtonVPN
- TunnelBear

Pagament:

- Mullvad: 5 euros/mes
- ProtonVPN: 4 euros/mes
- IVPN: 15 euros/mes
- NordVPN: 10.5 euros/mes
- ExpressVPN: 12.95 euros/mes
- TorGuard: 9.99 euros/mes

Conclusions

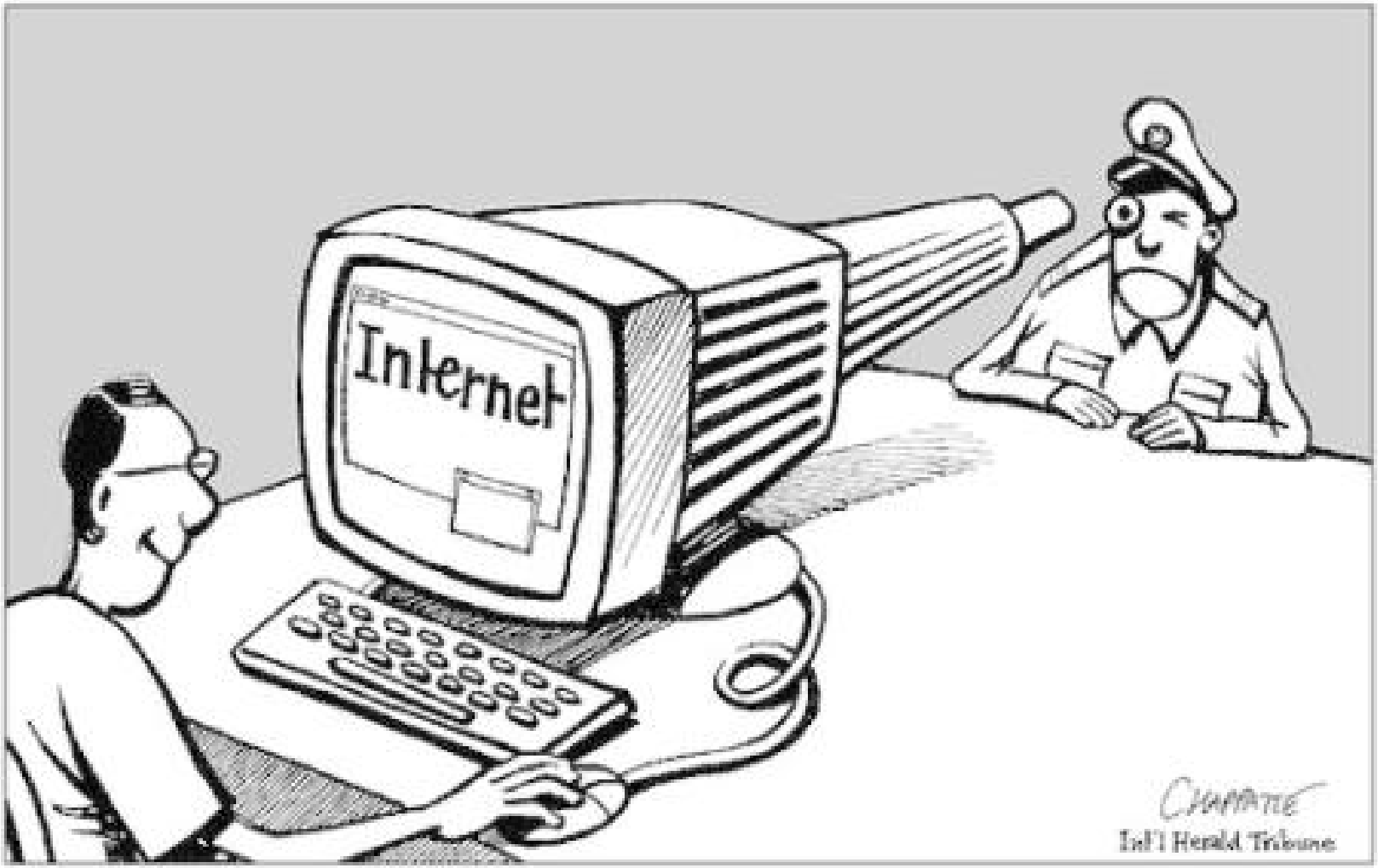
VPN

- Privacitat per política
- Protegeix la teva IP
- Protegeix contra adversaris que estiguin a la teva xarxa local

Tor

- Privacitat per disseny
- Ofereix anonimitat i privacitat

Comunicacions



Trucades i SMS

La xarxa de telefonia no va ser pensada originàriament per protegir la privacitat de l'usuari.

Important

La comunicació a través de trucades tradicionals o SMS no disposa de mecanismes de protecció contra l'escolta o les gravacions.

Email

Email

ProtonMail (Suïssa)

- Parcialment software lliure
- Xifratge punt a punt
- Basat en PGP
- No xifra l'assumpte

Tutanota (Alemana)

- Software lliure
- Xifratge punt a punt

Poden ser accedits usant el navegador del mòbil

Emails temporals

Comptes de correu d'usar i tirar. Duren uns minuts o hores i després s'elimina el compte i el contingut enviat.

Útil per obrir comptes a xarxes socials per evitar així l'SPAM i mantenir l'anonimitat o per enviar missatges que no esperen resposta.

- MintEmail
- Mailinator
- Airmail
- Guerrillamail

Aplicacions

Firewall i Tor

NetGuard

- Software lliure
- Permet escollir quines aplicacions tenen accés a Internet

Orbot

- Software lliure
- Tot el tràfic del mòbil passa per un proxy
- Utilitza Tor per xifrar i anonimitzar el tràfic

Navegadors

Tor Browser

- Software lliure
- Guardian Project
- Bloqueja localitzadors de tercers
- Evita fingerprinting
- Diverses capes de xifratge
- No és necessari utilitzar Orbot

Intercanvi de fitxers

Firefox Send

- Xifratge punt a punt
- Ofereix opcions de seguretat personalitzables
- Caducitat de l'arxiu, contrasenya per descarregar...

OnionShare

- Funciona amb Tor
- Obre un servidor privat
- Genera una URL aleatoria

Missatgeria instantania

Signal (EEUU)

- Software lliure
- Xifratge punt a punt
- Requereix el número de telèfon

Wire (Suïssa)

- Software lliure
- Requereix email
- Xifratge punt a punt
- Metadades no xifrades punt a punt
- Al registrar-se, no es xifra la localització de la IP

Càmera

ObscuraCam

- Guardian Project
- Pixela cares automàticament
- Elimina metadades que poguessin comprometre la privacitat

CameraV

- Guardian Project
- Emmagatzema les imatges i videos xifrades amb contrasenya
- Panic button

Intercanvi d'informació

PrivateBin

- Software lliure
- El servidor no sap el contingut
- Informació xifrada

CryptPad

- Software lliure
- Col·laboratiu a temps real
- Informació xifrada
- Word, Power Point, enquestes, llistat de tasques...

Privacitat, seguretat i anonimat

Xerrada introductoria

Contacte:

projectenadki@protonmail.com