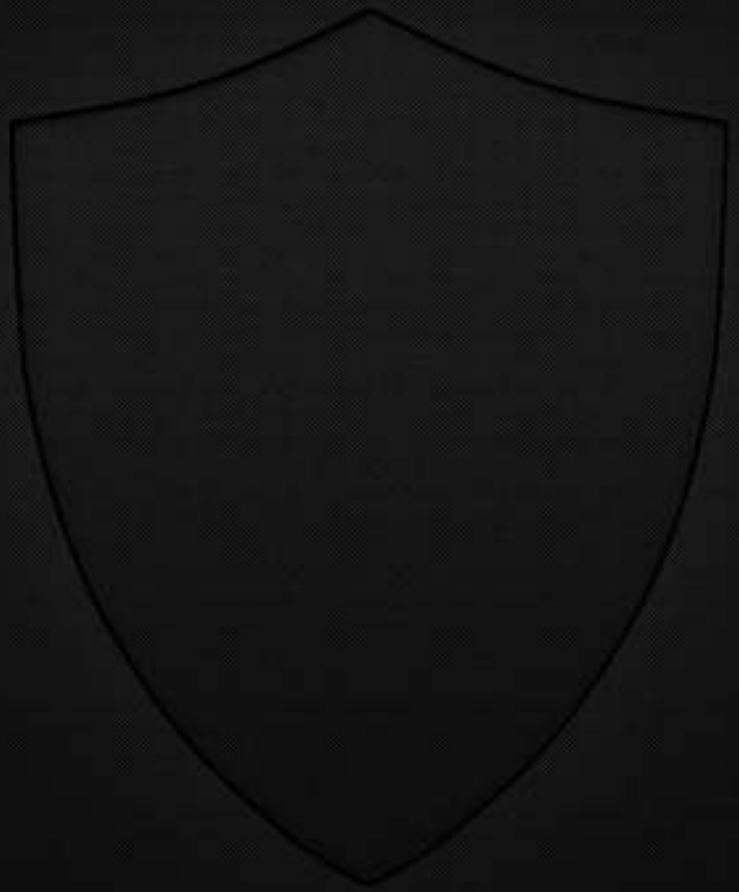
Intro a Seguridad de las Operaciones



-Michael Altfield

Qué es Seguridad de las operaciones?

OPSEC

Métodos de protección información crítica de adversarios

Cual Información?

Evaluación de riesgos

seguridad es una compensación

1) Mensajes a tu madre
2) Mensajes a su amante
3) Negocio R&D IP
4) Tarjetas de crédito del cliente
5) Archivos de billetera bitcoin

Cuales Adversarios?

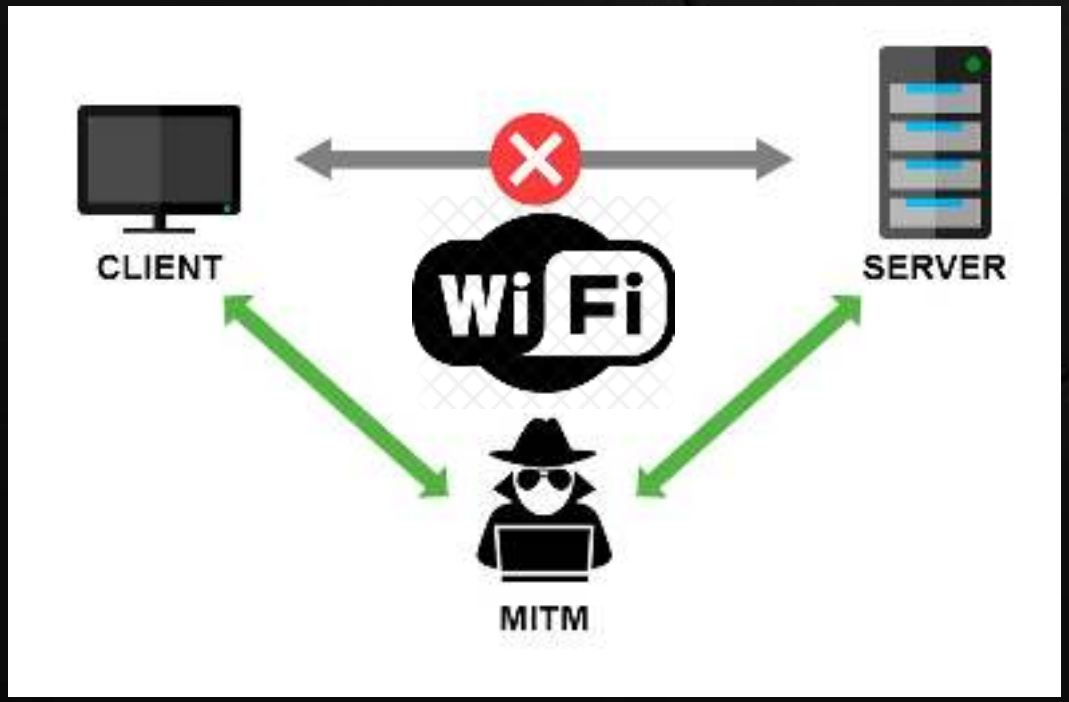
1) Oportunista
   spray and pray
   vigilancia masiva

2) Dirigido
   Spear Phishing

3) Amenaza Persistente Avanzada (APT)
   Patrocinado por el estado

Cuales Vulnerabilidades?

Física



Cuales Vulnerabilidades?

Ingeniería social

Cuales Vulnerabilidades?

Error de Usuario

Aislamiento

personal

trabajo

- QubesOS

Whonix

- TAILS

Contraseñas

¿Todos sus dispositivos requieren una contraseña?

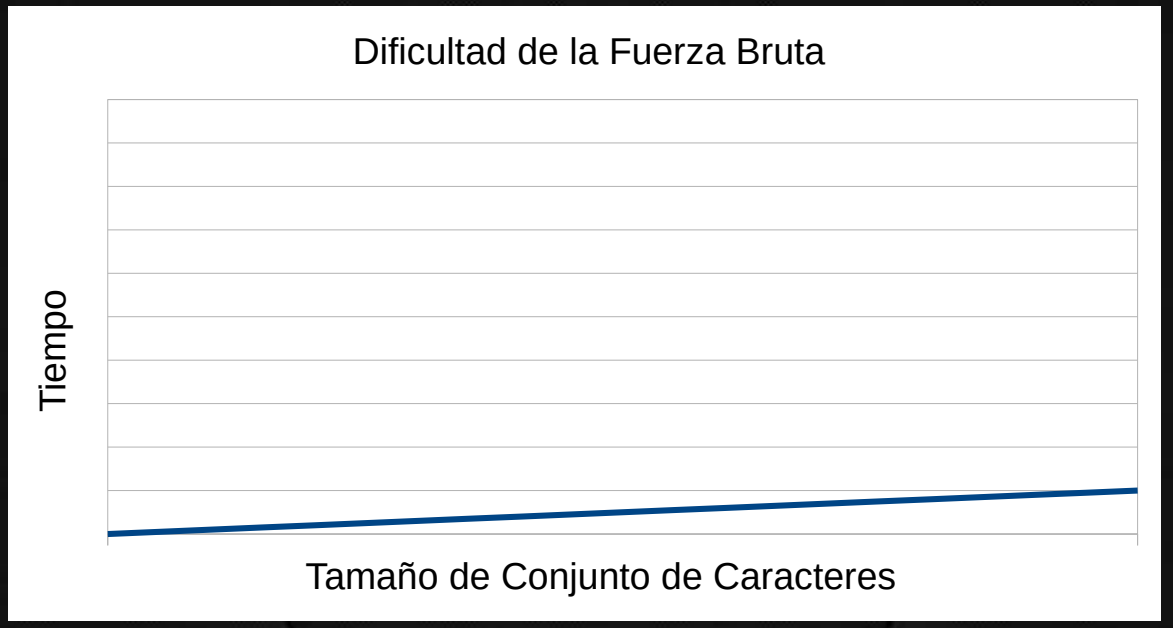
Contraseñas

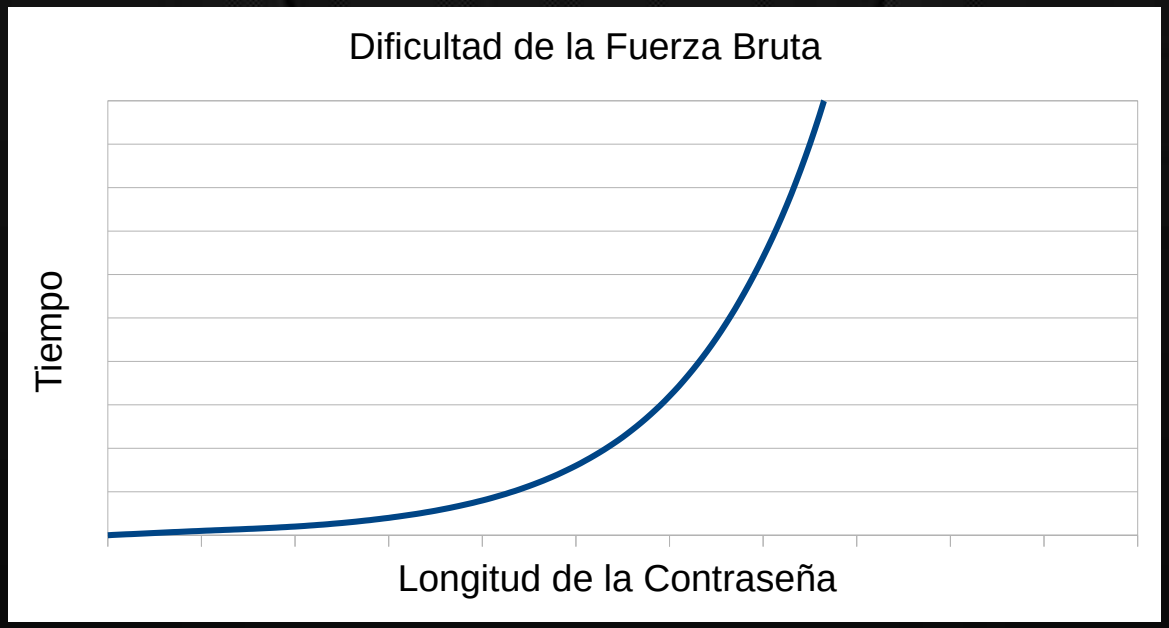
¿Qué hace una buena contraseña?

Contraseñas (cont)

- Listas de contraseñas comunes
  - 123456, contraseña123, teamo123, bobby …
- Listas de Diccionario
  - aalenianas, ababa … zwitterión, zioty
- Fuerza Bruta
  - a, b, c, d, e …
  - aa,ab, ac, ad, ae …

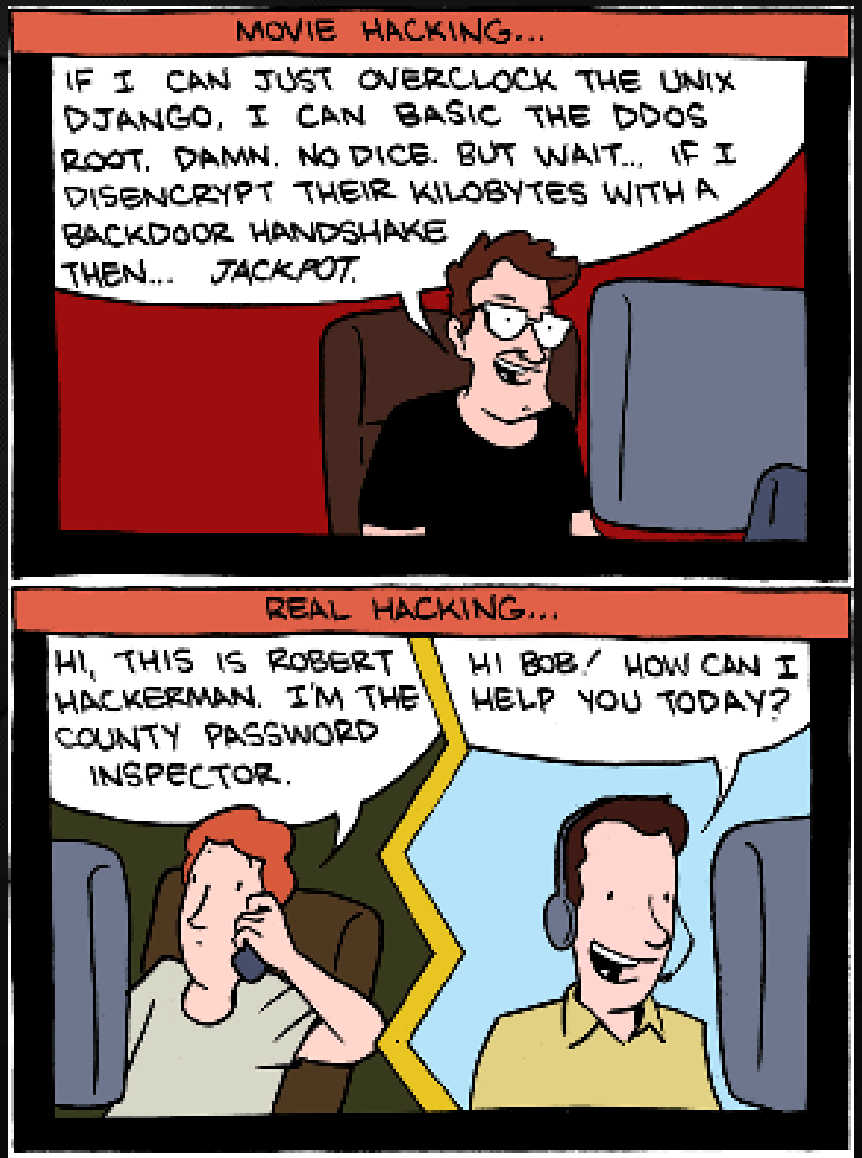
Contraseñas (cont)





Phishing

- ¡No comparta contraseñas!
- Contraseñas únicas para <u>cada</u> cuenta

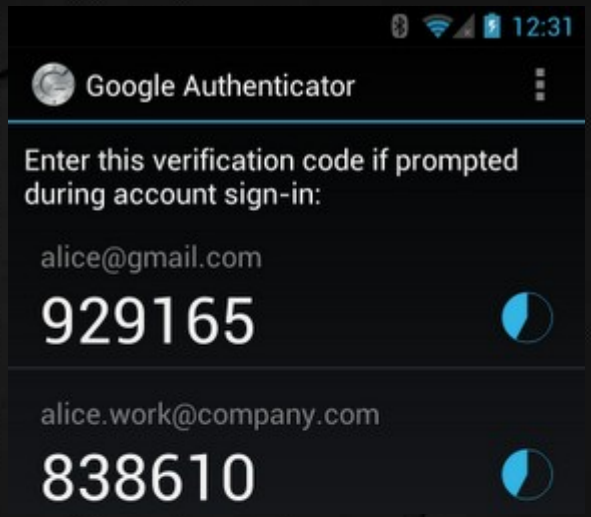


Administrador de contraseñas

- KeePassXC (Windows, macOS, Linux)
- KeePassDroid (Android)

Autenticación de Factores Múltiples

- 2FA = Dos Factores
- MFA = Múlti Factores



huella dactilar son nobres de usuarios

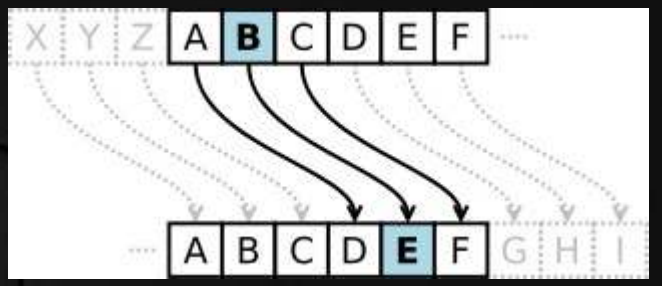
- Algo que **sabes**
- Algo que **tienes**
- Algo que **eres**

- SMS vs TOTP

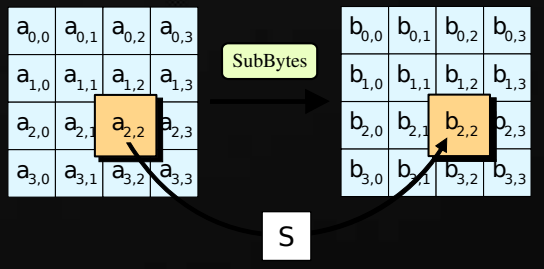
[1] CC BY-NC http://www.securitybydefault.com/2012/04/google-authenticator-2.html
[2] PD https://commons.wikimedia.org/wiki/File:Defense.gov_photo_essay_120110-A-3108M-006.jpg
[3] CC BY-NC http://www.securitybydefault.com/2011/01/contrasenas-de-un-solo-uso-en-linux.html

Cifrado

- Confidencialidad
- Cifrado césar
- Enigma
- AES
- RSA
- Cifrado en Reposo
- Cifrado en Tránsito

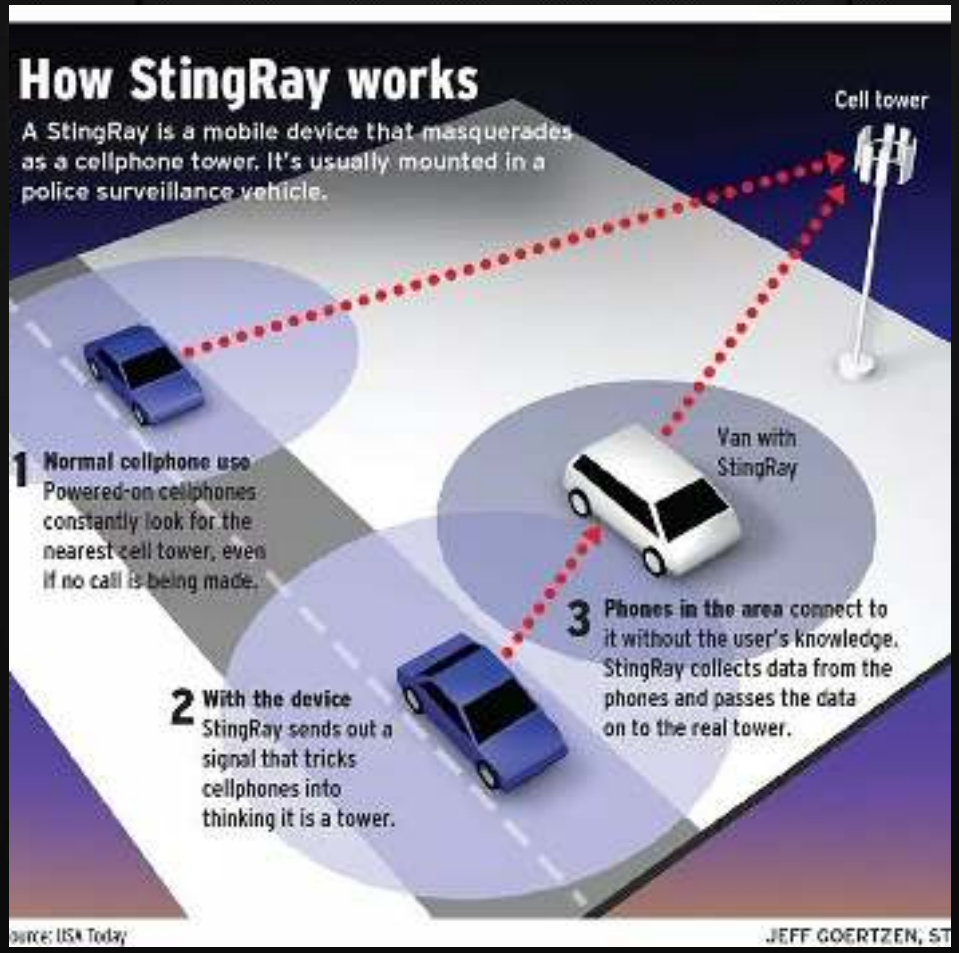


$$\begin{bmatrix} b_{0,j} \\ b_{1,j} \\ b_{2,j} \\ b_{3,j} \end{bmatrix} = \begin{bmatrix} 2 & 3 & 1 & 1 \\ 1 & 2 & 3 & 1 \\ 1 & 1 & 2 & 3 \\ 3 & 1 & 1 & 2 \end{bmatrix} \begin{bmatrix} a_{0,j} \\ a_{1,j} \\ a_{2,j} \\ a_{3,j} \end{bmatrix} \qquad 0 \leq j \leq 3$$



Cifrado en Tránsito

- Stingray = IMSI Catcher



Cifrado en Tránsito

- Drones

Cifrado en Tránsito (cont)

- SMS es Malo
- Las llamadas telefónicas son malas
- La aplicación de Signal es buena!

<

<

WhatsApp

Signal

Cifrado en Tránsito (cont)

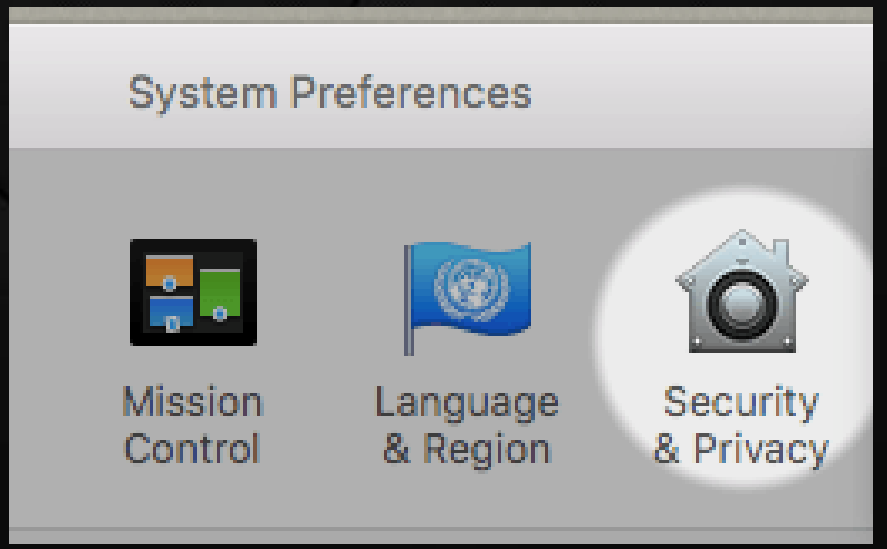
- Correo Electrónico
  - No Privado!
  - Evitar 14 ojos
    - 5: US, UK, CA, AU, NZ
    - 9: DK, FR, NL, NO
    - 14: BE, DE, IT, ES, SE
  - ProtonMail, Tutanota, etc
- PGP (GPG)
  - Cifrado de Extremo a Extremo

ProtonMail

Tutanota®

Cifrado en Reposo

- Cifrado de Disco Completo
- Veracrypt, FileVault
- "Borrar" no se borrar
- Las huellas dactilares son nombres de usuario, no contraseñas



Negación Plausible

- Veracrypt
  - Volumen Oculto
  - Sistema Operativo Oculto
- Contraseña de Coacción
- BusKill Autodestrucción

Metadatos

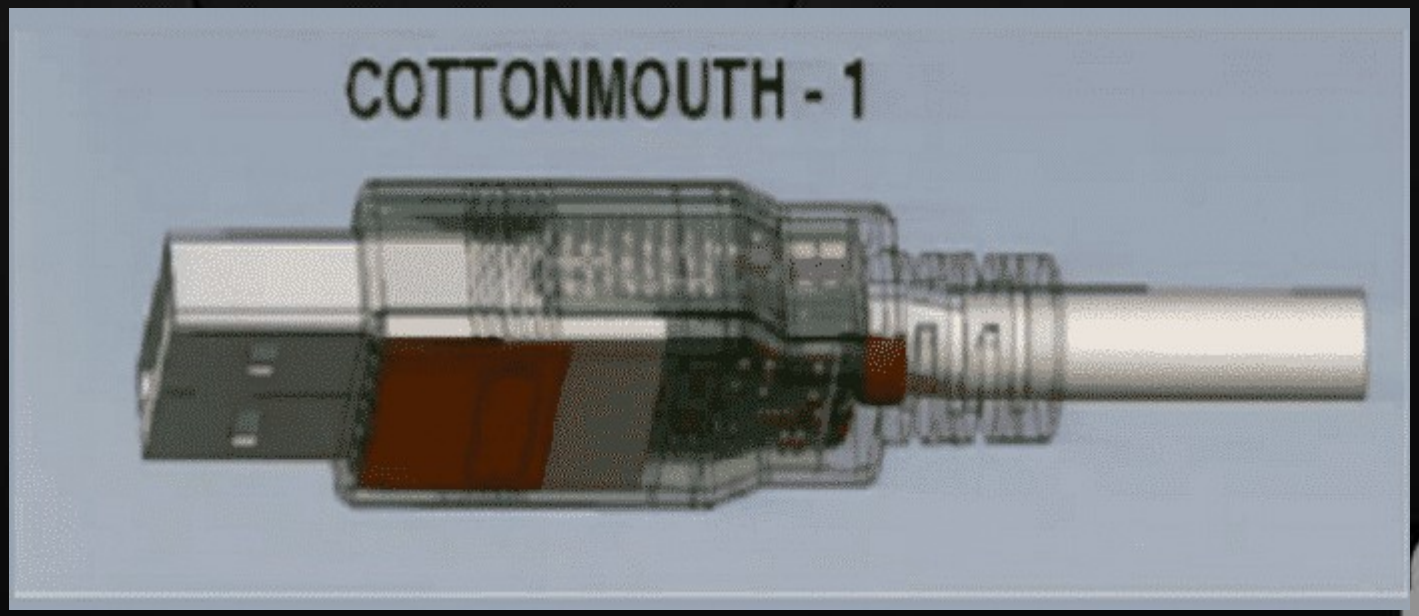
- GPS
  - Niños en Instagram
- Miniaturas
  - Desnudos Recotado?
- Reality Winner
  - Metadatos de Impresora

1) MAT2 (Linux)

2) Captura de Pantalla (Todo)

Seguridad de Hardware

- USB Condones
- Rubber Ducky
- NSA Cottonmouth
- O.MG Cable



Más información

Podcasts

- Security Now!
- Darknet Diaries
- Hablemos de Privacidad (YT)

Sitios Web

- EFF
- PrivacyGuides.org

Mantente vigilante!

@MichaelAltfield

@Mastodon.social

tech.michaelaltfield.net

PGP Fingerprint: B162 9E1F 1737 EC4F 74C9 E923 1EF1 68D2 68C4 0535

These slides are copyright © Michael Altfield. All content is licensed under a Creative Commons Attribution-ShareAlike 4.0 International License, unless explicitly stated otherwise.