Passwords Sucks

Foro de Seguridad RedIRIS Murcia 2025

Victor Barahona (UAM)

Hubo un tiempo en que no había

“Cuando llegué al laboratorio no había contraseñas ni seguridad. Cuando las impusieron, rompí el cifrado y sugerí a los usuarios usar la tecla enter como contraseña —por el principio de que no debía haber contraseñas.”

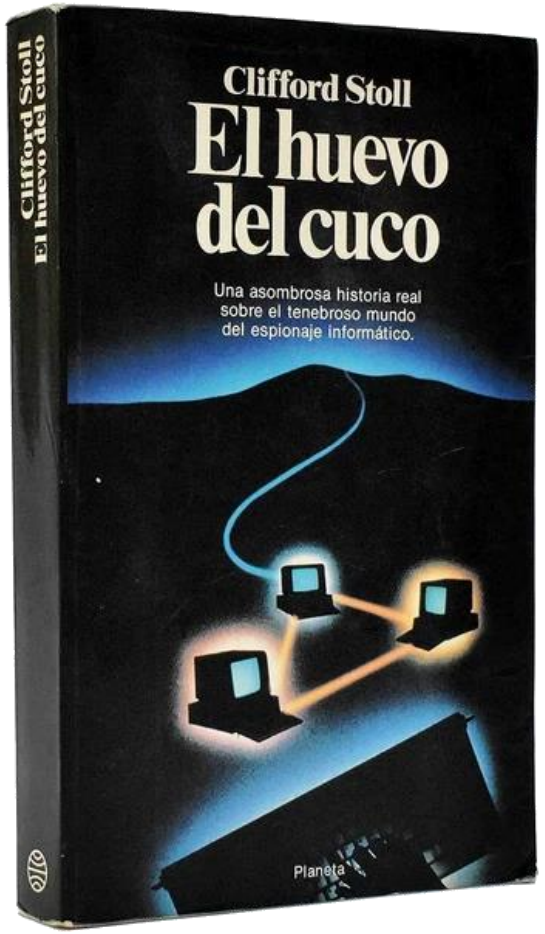
Richard Stallman (MIT AI Lab, finales de los 70)

Pero llegaron

- En sistemas monousuario el acceso era físico.
- En los sistemas multiusuario debía ser lógico.
- Aparecen las contraseñas para cubrir la necesidad.
- Las contraseñas son un procedimiento.
  - Fácil.
  - Barato.
  - Inseguro.
- Algo que sabes y si lo sabe un tercero deja de servir.

Amenazas de su tiempo

- 70's – el estandar pero mala gestión y almacenamiento.
  - Contraseñas sin cifrar.
  - Cifrado crackeable crypt().
  - Salt en /etc/passwd.
- 80's – ataque offline y hashes inseguros.
  - Cracking offline de hashes.
  - /etc/shadow y hashing más fuerte.
  - Passwords por defecto o triviales.
- 90's – capturas en tránsito, phishing, vulnerabilidades.
  - Sniffing (telnet/ftp/pop3/imap/http).
  - Phishing (AOHell).
  - Ataques NTLM (cracking, reutilización de hash, etc).
  - Windows 9x/Me “Share Level Password”.
  - Keylogers asociados a malware.
- 2000 – de lo artesano a lo industrializado.
  - Rainbow tables, GPU cracking, phishing industrial, network bruteforce, etc.



Fuente: The Top 500 Worst Passwords of All Time

Entropía de la información (Shannon 1948)

Definición:
Medida de la **incertidumbre** o cantidad promedio de información que contiene una fuente de mensajes. Cuanto más impredecible sea el mensaje, mayor será su entropía.

Lo que aplicado a contraseñas:
Estima la **dificultad para adivinar** una contraseña, basada en el **tamaño del conjunto de caracteres y la longitud**. A mayor entropía, más combinaciones posibles y, por tanto, mayor resistencia frente a ataques de fuerza bruta.

William Burr
(Bill)

Porque tenemos las contraseñas que tenemos

- Bill trabajaba en el NIST desde finales de los 70.
- En 2003 le encargan definir los estándares de autenticación electrónica remota en las agencias federales de EE.UU.
- La guía NIST SP 800-63 Apendice A (8 páginas) establecen las famosas reglas de composición para añadir entropía a las contraseñas:
  - Mínimo 8 caracteres.
  - Mayúsculas, minúsculas, números y símbolos obligatorios.
  - Caducidad periódica y rotación.
  - Evitar el uso de palabras comunes o secuencias repetidas.
- Se convirtió en referencia global para políticas de contraseñas.

¿Por qué la jod## Bill?

- Porque **tenía prisa**: 2 semanas.
- Porque se basó en **conocimiento antiguo**: whitepaper de los 80 sobre entropía y complejidad de contraseñas previo a la web.
- Porque partió de las siguientes premisas:
  - Si los usuarios usan contraseñas sencillas, definamos una forma de hacerlas más complejas.
  - Si tarde o temprano las contraseñas son adivinadas, obliguemos a que las cambien con frecuencia.

A mayor complejidad mayor entropía y la entropía protege las passwords ¿No?

Complejidad forzada ⇒ patrones previsibles

- Las contraseñas pasaron a tener de media **8 caracteres**.
- Casi todos los caracteres en **minúscula**.
- ¿**Máyuscula**? Pues que sea la primera letra.
- ¿**Números**? Sustituyamos "aeio" por "4310".
- ¿**Simbolos**? $ por "s", @ por "a" o añadamos ! al principio o al final.

`password`

`P4$$w0rd!`

Entropía en contraseñas: Teórica vs Efectiva

- ***Entropía teórica*:** mide el espacio de búsqueda basado en longitud y conjunto de caracteres **asumiendo aleatoriedad de cada carácter.**

- ***Entropía efectiva (guessability)*:** mide la dificultad real considerando patrones y diccionarios. **Predictibilidad humana.**

Teórica vs Efectiva

Contraseña	Teórica (bits)	Efectiva (bits)[1]
password	37.60	1.58
Password	45.60	2.32
P4ssword	47.63	3.17
P4$$w0rd	52.56	5.04
P@$$w0rd	52.46	5.04
t4$W?>op	52.46	-
@\FJyFHm:1}=6nx|s*kR	131.40	-

[1] Estimada usando zxcvbn

Tiempo estimado de password cracking[1]

Contraseña	Online 100/h	Online 10/s	Offline 10^4/s	Offline 10^10/s
password	2 min	< 1 seg	< 1 seg	< 1 seg
Password	3 min	< 1 seg	< 1 seg	< 1 seg
P4ssword	5 min	< 1 seg	< 1 seg	< 1 seg
P4$$w0rd	20 min	3 seg	< 1 seg	< 1 seg
P@$$w0rd	20 min	3 seg	< 1 seg	< 1 seg
t4$W?>op	siglos	3 years	1 day	< 1 seg
@\FJyFHm:1}=6nx|s*kR	siglos	Siglos	Siglos	siglos

[1] Estimado usando zxcvbn

Rotación de contraseñas

- ¿Por qué se rotan?
  - Reducir el tiempo de **exposición.**
  - Cumplimiento **normativo.**
  - Protección ante **ataques offline.**
- Aspectos negativos y riesgos.
  - Contraseñas más **débiles y predecibles**: lleva a patrones simples.
  - **Fatiga del usuario**: generan frustración y malas prácticas.
  - **Carga operativa** innecesaria: costes y tiempo sin aportar valor.
  - **Evidencia científica** en contra: los atacantes usan las credenciales de inmediato mientras que los usuarios terminan debilitando sus contraseñas.

Como elegir una password

- ¿Qué buscamos en una contraseña?
  - Que sea **fácil de recordar.**
  - Que sea **difícil de adivinar.**
- Diceware es una posible aproximación al problema.
  - 1 lista de 7776 palabras.
  - 1 dado.
  - Cada palabra de nuestra passphrase son 5 tiradas del dado.
- Por ejemplo: "morder ostras carcel guerra" (27).
- Hay herramientas para generar diceware passwds sin dado.

¿Son faciles de recordar las diceware passwords?

morder ostras carcel guerra

vs

t4$W?>op

Durante 20 años de esfuerzo, hemos entrenado satisfactoriamente a todo el mundo a usar contraseñas que son dificiles de recordar para los humanos, pero faciles de adivinar para las máquinas. **(xkcd #936)**

¿Cómo de seguras son las diceware passwords?

Tipo de contraseña	Nº posibilidades (≈)	Entropía (bits)
Diceware 4 palabras	$7.776^4 \approx 10^{15}$	~51,6
8 min+may+números+símbolos (~94)	$94^8 \approx 10^{15}$	~52,6
Diceware 5 palabras	$7.776^5 \approx 10^{19}$	~64,5
Diceware 6 palabras	$7.776^6 \approx 10^{23}$	~77,4
Diceware 7 palabras	$7.776^7 \approx 10^{27}$	~90,3
15 min+may+números+símbolos (~94)	$94^{15} \approx 10^{29}$	~98,3
Diceware 8 palabras	$7.776^8 \approx 10^{31}$	~103.4
20 min+may+números+símbolos (~94)	$94^{20} \approx 10^{39}$	~131.1

¿Son los usuarios tontos?

Pues no, solo tratan de enfrentar la complejidad de los sistemas que hemos diseñado:

- Cientos de servicios.
- Complejidad F0rz4d@.
- Prohibición de reutilización de contraseñas
- Expiración periódica de las contraseñas
- ¡Y que no las apunten!

Pero algo cambió en 2017

NIST SP 800-63-4 (Agosto 2025)

Característica	V1 (2003)	V3 (2017)	V4 (2025)
Modelo	Entropia calculada	Longitud+blocklist+usabilidad	Modelo de 2017 + distingue entre contraseñas single-factor y MFA
Longitud	8	8	15 single-factor 8 + MFA
Reglas de composición	SI	NO	IGUAL que 2017
Checkeos de diccionario	SI	SI + blocklist	SI + blocklist extendido y mantenido
Caducidad periodica	SI	NO. Salvo evidencia de compromiso	IGUAL que 2017
Preguntas de seguridad	NP	NO	IGUAL que 2017
Usabilidad	NP	Permitir paste y gestores de contraseñas, opción ver passwd	IGUAL que 2017

ENS: Guia CCN-STIC 821 – Apendice V (2018)

- Coge cosas de NISP 800-63-3 pero…
- Descarta el modelo de entropia basado en reglas de composición
- Longitud mínima ≥ 8 caracteres alfanuméricos (espacios incluidos)
- Preferencia por “passphrases”
- Gestión del ciclo de vida:
  - cambio ante indicios de compromiso
  - renovación periódica en plazo razonable. Sugiere 1 año (no dogma)
- Usabilidad:
  - Password Paste
  - Gestores de contraseñas
  - Posibilidad de ver contraseña escrita

Gestores de contraseñas

- Hoy son herramientas **fundamentales**.
- Si un usuario no los usa se puede decir con gran certidumbre:
  - Que sus contraseñas son **predecibles.**
  - Que **reutiliza** contraseñas entre servicios.
  - Que está en **riesgo** si las usa como único factor.
- Deben incluir **generador de contraseñas.**
- Las contraseñas generadas serán criptograficamente robustas: **"aleatorias y largas".**
- Un **gestor de contraseñas + usuario formado** hacen buenas a las contraseñas.
- Hay que desarrollar **guías para los usuarios.**

MFA – No hay más remedio

- **Hemos inventado el MFA porque el primer factor es la contraseña y es un factor muy malo.**
- Con tal de reforzarlo, a veces aceptamos códigos por SMS o al correo como segundo factor.
- Cuando tenemos un factor fuerte, quizás debemos plantearnos quitar las contraseñas.

FIDO2 - Passkeys
El fin de las contraseñas

- Funcionan con **criptografía de clave pública**:
  - **Clave privada**: permanece en el dispositivo.
  - **Clave pública**: se almacena en el servicio.
- Autenticación mediante **biometría** (huella, rostro) o **PIN local**
- Ventajas:
  - **Resistentes al phishing**: no hay secretos reutilizables.
  - **No se pueden robar en brechas**: la clave privada nunca sale del dispositivo.
  - **Experiencia más simple**: inicio de sesión rápido y sin recordar contraseñas.
  - **Compatibilidad**: soportadas por Apple, Google, Microsoft, etc y navegadores modernos.
- **Adopción lenta** en entornos corporativos por:
  - Recuperación de cuentas.
  - Compatibilidad con sistemas heredados.
  - Regulaciones y cultura de seguridad.

C0nclu$10n3s

- NO a las reglas de composición para generar entropía.
- NO a la rotación periódica de contraseñas sin motivo.
- NO a seguir culpando al usuario del problema de las contraseñas.
- SI a aumentar el tamaño de las passwords/passphrases >15.
- SI a usar passwords de >8 + MFA.
- SI a verificar la fortaleza de las contraseñas del usuario con blocklist.
- SI al uso gestores de contraseñas.
- Si a los generadores de contraseñas.
- SI a recordar solo una contraseña, pero que sea buena.
- SI al MFA (que remedio).
- SI a las passkeys.
- SI a reconocer que **nos hemos equivocado**. Hay que **cambiar las politicas** de passwords.

Referencias

- El huevo del cuco (libro) https://www.goodreads.com/book/show/5164299-el-huevo-del-cuco
- The Top 500 Worst Passwords of All Time https://uatechserv.com/information/the-top-500-worst-passwords-of-all-time/
- Of Passwords and People: Measuring the Effect of Password-Composition Policies https://users.ece.cmu.edu/~lbauer/papers/2011/chi2011-passwords.pdf
- The Security of Modern Password Expiration: An Algorithmic Framework and Empirical Analysis https://www.cs.unc.edu/~fabian/papers/PasswordExpire.pdf
- NIST SP 800-61 https://csrc.nist.gov/pubs/sp/800/63/final
- NIST SP 800-63-4 https://pages.nist.gov/800-63-4/
- Bill Burr https://www.wsj.com/articles/the-man-who-wrote-those-password-rules-has-a-new-tip-n3v-r-m1-d-1502124118
- XKCD Password Strength https://xkcd.com/936/
- zxcvbn https://github.com/dropbox/zxcvbn
- Diceware home https://theworld.com/~reinhold/diceware.html
- Diceware-wordlist-es https://github.com/jawlenskys/diceware/blob/master/diceware/wordlists/wordlist_es.txt
- Security analysis of Diceware Passphrases https://isij.eu/system/files/download-count/2023-01/4719_diceware_passphrases.pdf
- FIDO2 Passkeys https://fidoalliance.org/passkeys/

Gracias