Password authentication

Myrto Arapinis
School of Informatics
University of Edinburgh

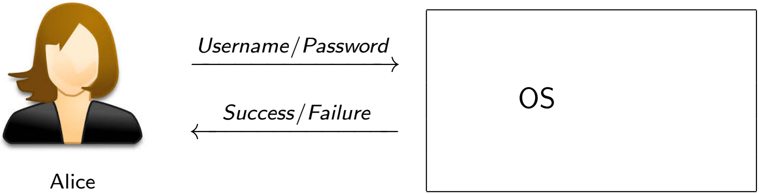
Password authentication

- The question: “who is allowed to access the resources in a computer system?”
- How does the operating system securely identify its users?
- Authentication: determination of the identity of a user

Password authentication

- The question: "who is allowed to access the resources in a computer system?"
- How does the operating system securely identify its users?
- Authentication: determination of the identity of a user

- Standard authentication mechanism: **username** and **password**



Username / Password

Success / Failure

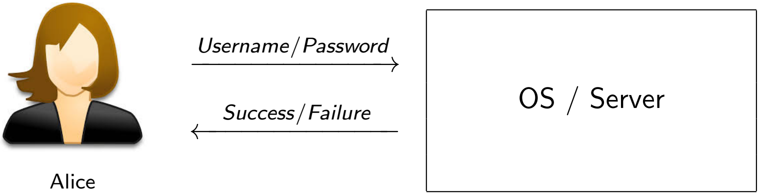
OS

Alice

Password authentication

- The question: “who is allowed to access the resources in a computer system?”
- How does the operating system securely identify its users?
- Authentication: determination of the identity of a user

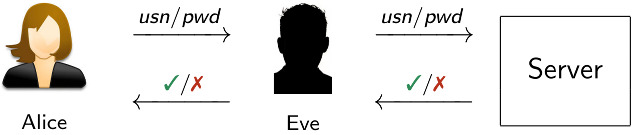
- Standard authentication mechanism: **username** and **password**



Usability vs. Security

Passwords need to be **hard to guess** yet **easy to remember**

Network attacks



Alice

usn/pwd →

✓/✗ ←

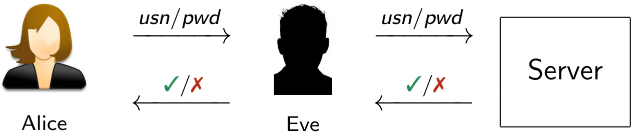
Eve

usn/pwd →

✓/✗ ←

Server

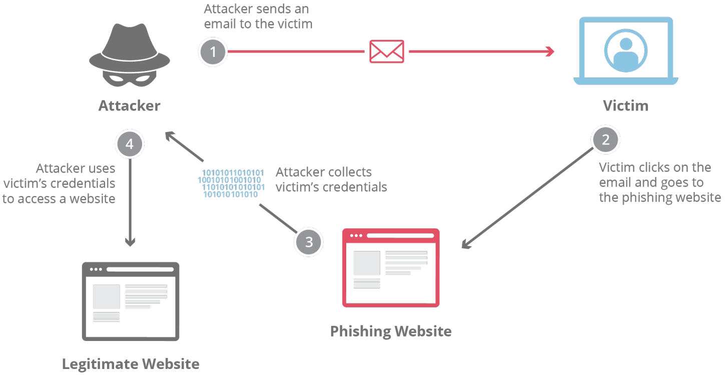
Network attacks



Defending against eaversdropers

Encrypt communication using *eg.* TLS

Social engineering & Phishing attacks



Attacker

1 Attacker sends an email to the victim

Victim

2 Victim clicks on the email and goes to the phishing website

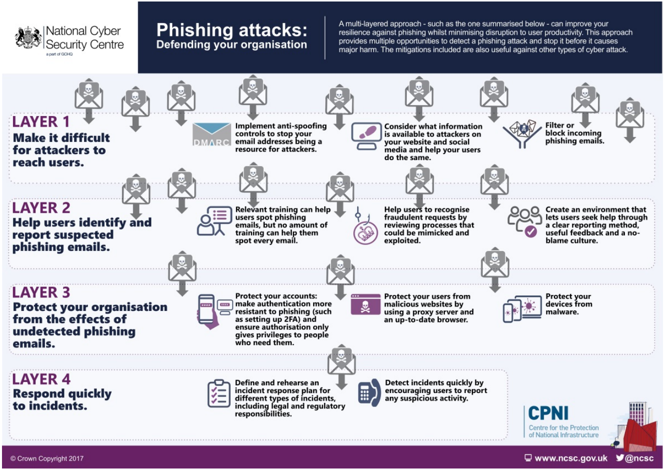
Phishing Website

3 Attacker collects victim's credentials

4 Attacker uses victim's credentials to access a website

Legitimate Website

Defending against phishing - NCSC guidance



National Cyber Security Centre
a part of GCHQ

Phishing attacks: Defending your organisation

A multi-layered approach - such as the one summarised below - can improve your resilience against phishing whilst minimising disruption to user productivity. This approach provides multiple opportunities to detect a phishing attack and stop it before it causes major harm. The mitigations included are also useful against other types of cyber attack.

LAYER 1
Make it difficult for attackers to reach users.

Implement anti-spoofing controls to stop your email addresses being a resource for attackers.

Consider what information is available to attackers on your website and social media and help your users do the same.

Filter or block incoming phishing emails.

LAYER 2
Help users identify and report suspected phishing emails.

Relevant training can help users spot phishing emails, but no amount of training can help them spot every email.

Help users to recognise fraudulent requests by reviewing processes that could be mimicked and exploited.

Create an environment that lets users seek help through a clear reporting method, useful feedback and a no-blame culture.

LAYER 3
Protect your organisation from the effects of undetected phishing emails.

Protect your accounts: make authentication more resistant to phishing (such as setting up 2FA) and ensure authorisation only gives privileges to people who need them.

Protect your users from malicious websites by using a proxy server and an up-to-date browser.

Protect your devices from malware.

LAYER 4
Respond quickly to incidents.

Define and rehearse an incident response plan for different types of incidents, including legal and regulatory responsibilities.

Detect incidents quickly by encouraging users to report any suspicious activity.

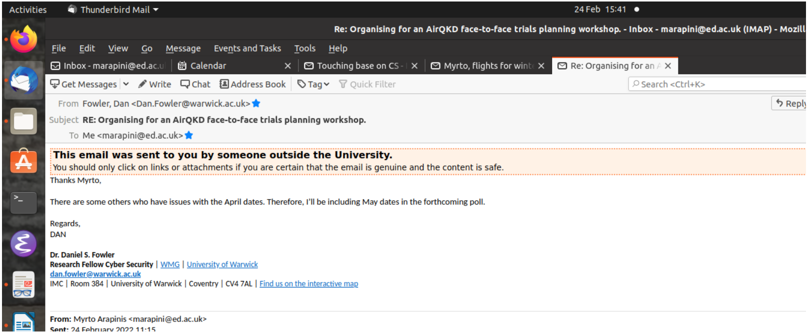
CPNI
Centre for the Protection of National Infrastructure

© Crown Copyright 2017

www.ncsc.gov.uk @ncsc

https://www.ncsc.gov.uk/guidance/phishing?fbclid=IwAR0cDtSZ7WdA7U2iB8zE91FoRuSWkS6daaRBhHU7btYIBxPp24J_LW3Lx88

Defending against phishing - UoE emails example



From Fowler, Dan <Dan.Fowler@warwick.ac.uk>
Subject **RE: Organising for an AirQKD face-to-face trials planning workshop.**
To Me <marapini@ed.ac.uk>

This email was sent to you by someone outside the University.
You should only click on links or attachments if you are certain that the email is genuine and the content is safe.

Thanks Myrto,

There are some others who have issues with the April dates. Therefore, I'll be including May dates in the forthcoming poll.

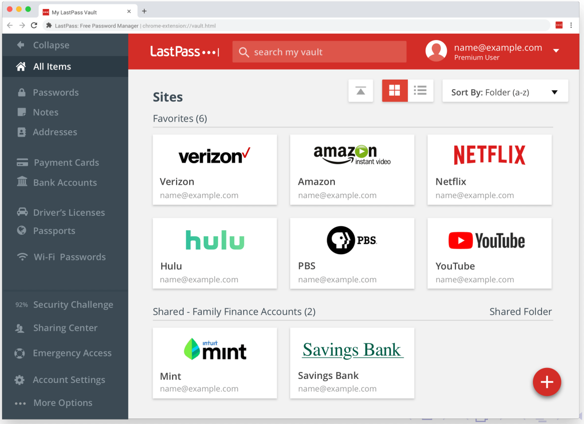
Regards,
DAN

Dr. Daniel S. Fowler
Research Fellow Cyber Security | WMG | University of Warwick
dan.fowler@warwick.ac.uk
IMC | Room 384 | University of Warwick | Coventry | CV4 7AL | Find us on the interactive map

From: Myrto Arapinis <marapini@ed.ac.uk>
Sent: 24 February 2022 11:15

Defending against phishing - password managers

- Password managers often fill username & password for user based on URL
- The password manager will not enter credentials for `amazon.co.uk` or `barclays.co.uk` on any other attacker controled website :-)

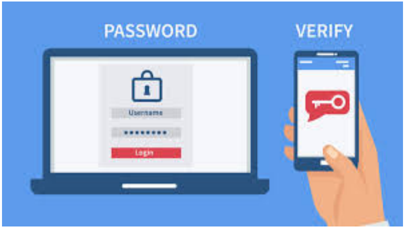


Malware attacks

- **Malware attack** - users will often have malware installed on their machine - this malware might contain a key-logger that records keyboard stroke and intercept passwords when typed

Malware attacks

- **Malware attack** - users will often have malware installed on their machine - this malware might contain a key-logger that records keyboard stroke and intercept passwords when typed
- Key-logger mitigation - use **two factor authentication** (2FA)

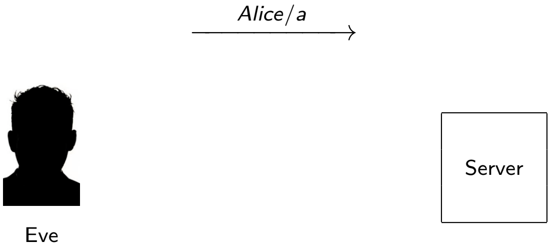


Online guessing attacks

Eve

Server

Online guessing attacks

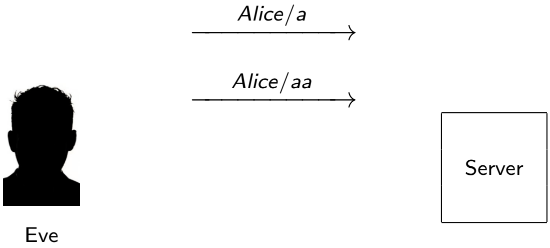


$Alice/a$

Eve

Server

Online guessing attacks



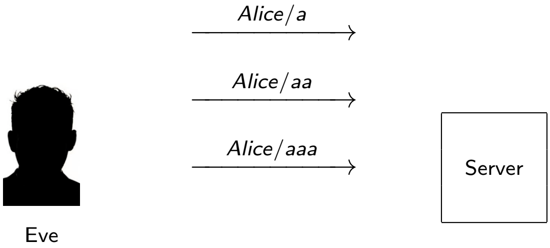
$Alice/a$

$Alice/aa$

Eve

Server

Online guessing attacks



Alice/*a*

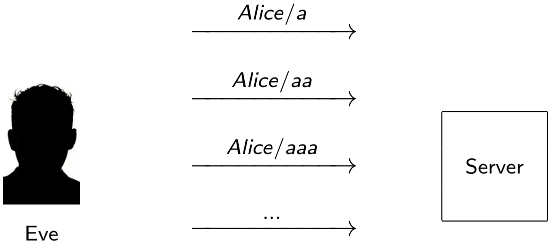
Alice/*aa*

Alice/*aaa*

Eve

Server

Online guessing attacks



Eve

Alice/*a*

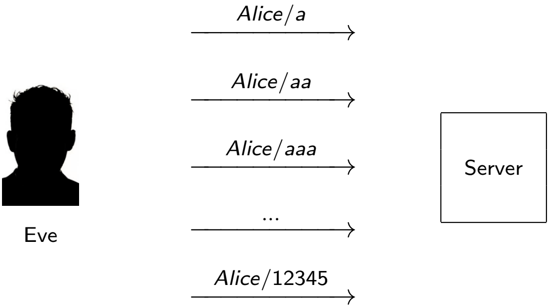
Alice/*aa*

Alice/*aaa*

...

Server

Online guessing attacks



Eve

Alice/*a*

Alice/*aa*

Alice/*aaa*

...

Alice/12345

Server

Defending against online guessing attacks

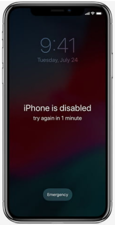
Defending against online guessing attacks

- **Choose a good password** - length, capital letters, symbol characters, not a word *etc*.

Defending against online guessing attacks

- **Choose a good password** - length, capital letters, symbol characters, not a word *etc*.

- **Rate limit** - impose a limit on the number of failed password attempts before locking the system for a set amount of time

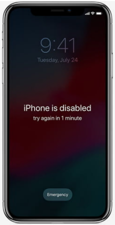


iPhone is disabled
try again in 1 minute

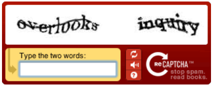
Defending against online guessing attacks

- **Choose a good password** - length, capital letters, symbol characters, not a word *etc*.

- **Rate limit** - impose a limit on the number of failed password attempts before locking the system for a set amount of time



- Include **captchas** - include a captcha puzzle to be solved along the submission of the username and password in order to prevent automated password guessing



overlooks inquiry

Type the two words:

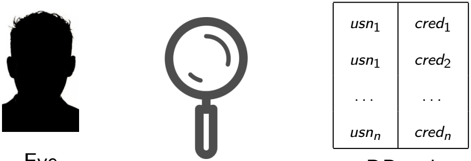
reCAPTCHA™ stop spam. read books.

Offline guessing attacks

- Most common password-related attacks target the server

Offline guessing attacks

- Most common password-related attacks target the server



usn_1	$cred_1$
usn_1	$cred_2$
$\dots$	$\dots$
usn_n	$cred_n$

DBpwd

Offline guessing attacks

- Most common password-related attacks target the server

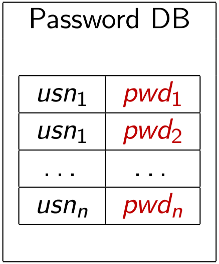
usn_1	$cred_1$
usn_1	$cred_2$
$\dots$	$\dots$
usn_n	$cred_n$

DBpwd

Our goal

Defend from attacks that leak the password database

Attempt #1: store passwords **unencrypted**



Password DB

usn_1	pwd_1
usn_1	pwd_2
$\dots$	$\dots$
usn_n	pwd_n

Attempt #1: store passwords **unencrypted**

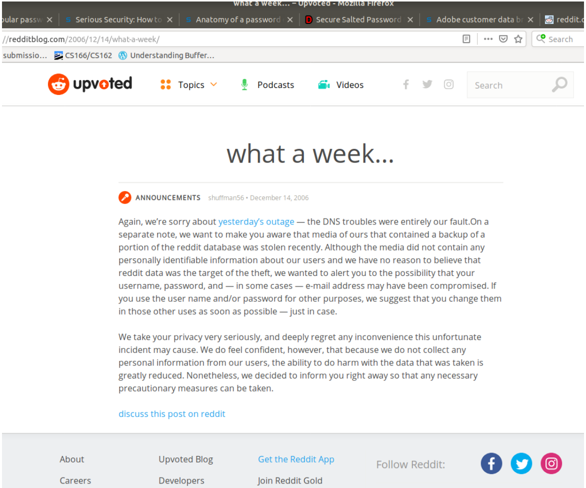
Password DB

usn_1	pwd_1
usn_1	pwd_2
$\dots$	$\dots$
usn_n	pwd_n

- Whoever accesses the password DB can login as any user

- Might leak user login information to other services/accounts

Reddit password leak (2006)



what a week…

ANNOUNCEMENTS shuffman56 • December 14, 2006

Again, we're sorry about yesterday's outage — the DNS troubles were entirely our fault.On a separate note, we want to make you aware that media of ours that contained a backup of a portion of the reddit database was stolen recently. Although the media did not contain any personally identifiable information about our users and we have no reason to believe that reddit data was the target of the theft, we wanted to alert you to the possibility that your username, password, and — in some cases — e-mail address may have been compromised. If you use the user name and/or password for other purposes, we suggest that you change them in those other uses as soon as possible — just in case.

We take your privacy very seriously, and deeply regret any inconvenience this unfortunate incident may cause. We do feel confident, however, that because we do not collect any personal information from our users, the ability to do harm with the data that was taken is greatly reduced. Nonetheless, we decided to inform you right away so that any necessary precautionary measures can be taken.

discuss this post on reddit

Attempt #2: **encrypt** passwords

Password DB

$\boxed{k}$

usn_1	$c_1 = E(k, pwd_1)$
usn_2	$c_2 = E(k, pwd_2)$
$\ldots$	$\ldots$
usn_n	$c_n = E(k, pwd_n)$

Attempt #2: **encrypt** passwords

Password DB

$\boxed{k}$

usn_1	$c_1 = E(k, pwd_1)$
usn_2	$c_2 = E(k, pwd_2)$
$\dots$	$\dots$
usn_n	$c_n = E(k, pwd_n)$

- Stolen encrypted passwords cannot be decrypted.
- Only admins have the key. If a user forgets their password, admins can just look it up for him.

Attempt #2: **encrypt** passwords

Password DB

$\boxed{k}$

usn_1	$c_1 = E(k, pwd_1)$
usn_2	$c_2 = E(k, pwd_2)$
...	...
usn_n	$c_n = E(k, pwd_n)$

+ Stolen encrypted passwords cannot be decrypted.
+ Only admins have the key. If a user forgets their password, admins can just look it up for him.

– If attacker managed to steal passwords, why assume the key cannot be stolen?
– Anyone with the key (admins) can view passwords.

Adobe password leak (2013)

- Information on 38 million user accounts leaked
- Adobe pays US $1.2M plus settlements to end breach class action

https://nakedsecurity.sophos.com/2013/11/04/anatomy-of-a-password-disaster-adobes-giant-sized-cryptographic-blunder/

Attempt #3: **hash** passwords

Password DB

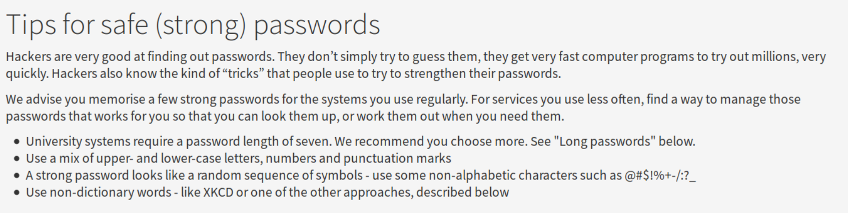
usn_1	$d_1 = H(pwd_1)$
usn_2	$d_2 = H(pwd_2)$
$\ldots$	$\ldots$
usn_n	$d_n = H(pwd_n)$

Brute force attack

- Try all passwords in a given space
  - κ: number of possible characters
  - ℓ: password length
  - ⇝ κ^ℓ possible passwords

Brute force attack

- Try all passwords in a given space
  - κ: number of possible characters
  - ℓ: password length
  - $\rightsquigarrow$ κ^{ℓ} possible passwords



Tips for safe (strong) passwords

Hackers are very good at finding out passwords. They don't simply try to guess them, they get very fast computer programs to try out millions, very quickly. Hackers also know the kind of "tricks" that people use to try to strengthen their passwords.

We advise you memorise a few strong passwords for the systems you use regularly. For services you use less often, find a way to manage those passwords that works for you so that you can look them up, or work them out when you need them.

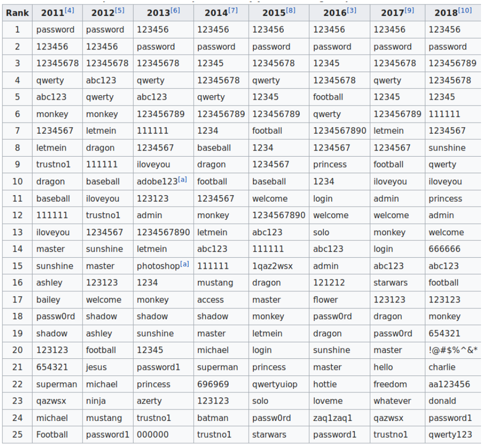
- University systems require a password length of seven. We recommend you choose more. See "Long passwords" below.
- Use a mix of upper- and lower-case letters, numbers and punctuation marks
- A strong password looks like a random sequence of symbols - use some non-alphabetic characters such as @#$!%+-/:?_
- Use non-dictionary words - like XKCD or one of the other approaches, described below

UoE password guidelines

$\rightsquigarrow$ Assuming a standard 94 characters keyboard, there are $94^7 = 6.4847759e^{+13}$ possible passwords.

Do we need to try all κ^ℓ passwords?

Do we need to try all κ^ℓ passwords?



Rank	2011[4]	2012[5]	2013[6]	2014[7]	2015[8]	2016[3]	2017[9]	2018[10]
1	password	password	123456	123456	123456	123456	123456	123456
2	123456	123456	password	password	password	password	password	password
3	12345678	12345678	12345678	12345	12345678	12345	12345678	123456789
4	qwerty	abc123	qwerty	12345678	qwerty	12345678	qwerty	12345678
5	abc123	qwerty	abc123	qwerty	12345	football	12345	12345
6	monkey	monkey	123456789	123456789	123456789	qwerty	123456789	111111
7	1234567	letmein	111111	1234	football	1234567890	letmein	1234567
8	letmein	dragon	1234567	baseball	1234	1234567	1234567	sunshine
9	trustno1	111111	iloveyou	dragon	1234567	princess	football	qwerty
10	dragon	baseball	adobe123[a]	football	baseball	1234	iloveyou	iloveyou
11	baseball	iloveyou	123123	1234567	welcome	login	admin	princess
12	111111	trustno1	admin	monkey	1234567890	welcome	welcome	admin
13	iloveyou	1234567	1234567890	letmein	abc123	solo	monkey	welcome
14	master	sunshine	letmein	abc123	111111	abc123	login	666666
15	sunshine	master	photoshop[a]	111111	1qaz2wsx	admin	abc123	abc123
16	ashley	123123	1234	mustang	dragon	121212	starwars	football
17	bailey	welcome	monkey	access	master	flower	123123	123123
18	passw0rd	shadow	shadow	shadow	monkey	passw0rd	dragon	monkey
19	shadow	ashley	sunshine	master	letmein	dragon	passw0rd	654321
20	123123	football	12345	michael	login	sunshine	master	!@#$%^&*
21	654321	jesus	password1	superman	princess	master	hello	charlie
22	superman	michael	princess	696969	qwertyuiop	hottie	freedom	aa123456
23	qazwsx	ninja	azerty	123123	solo	loveme	whatever	donald
24	michael	mustang	trustno1	batman	passw0rd	zaq1zaq1	qazwsx	password1
25	Football	password1	000000	trustno1	starwars	password1	trustno1	qwerty123

- (2016) the 25 most common passwords made up more than 10% of surveyed passwords.
- Most common password of 2016, "123456", makes up 4% of surveyed passwords.
- 30% of password surveyed in top 10000

Dictionary attack

- Try the top N most common passwords,
- Try words in English dictionary,
- Try names, places, notable dates,
- Try Combinations of the above,
- Try the above replacing some characters with digits and symbols e.g. : iloveyou, il0vey0u, i10v3y0u, ...

Dictionary attack

- Try the top N most common passwords,
- Try words in English dictionary,
- Try names, places, notable dates,
- Try Combinations of the above,
- Try the above replacing some characters with digits and symbols e.g. : iloveyou, il0vey0u, i10v3y0u, ...
- UoE: password guidelines `https://www.ed.ac.uk/infosec/how-to-protect/lock-your-devices/passwords`

Attempt #3: **hash** passwords

Password DB

usn_1	$d_1 = H(pwd_1)$
usn_2	$d_2 = H(pwd_2)$
$\ldots$	$\ldots$
usn_n	$d_n = H(pwd_n)$

Attempt #3: **hash** passwords

Password DB

usn_1	$d_1 = H(pwd_1)$
usn_2	$d_2 = H(pwd_2)$
$\ldots$	$\ldots$
usn_n	$d_n = H(pwd_n)$

? Stolen hashed passwords cannot easily be cracked (?!)

- Once a hash is cracked, the password is know for all accounts using the same password
- Humans tend to pick weak/guessable passwords
  - Frequency analysis
  - Dictionary attack

LinkedIn password leak (2012)

- In June 2012, it was announced that almost 6.5 million linked in passwords were leaked and posted on a hacker website

Attempt #4: **salt and hash** passwords

Password DB

usn_1	s_1	$d_1 = H(s_1 \| \| pwd_1)$
usn_2	s_2	$d_2 = H(s_2 \| \| pwd_2)$
$\ldots$	$\ldots$	
usn_n	s_n	$d_n = H(s_n \| \| pwd_n)$

Attempt #4: **salt and hash** passwords

Password DB

usn_1	s_1	$d_1 = H(s_1 \| \| pwd_1)$
usn_2	s_2	$d_2 = H(s_2 \| \| pwd_2)$
$\dots$	$\dots$	
usn_n	s_n	$d_n = H(s_n \| \| pwd_n)$

+ Since every user has different salt, identical passwords will not have identical hashes

+ No frequency analysis

+ No precomputation: when salting one cannot use preexisting tables to crack passwords easily

Attempt #4: **salt and hash** passwords

Password DB

usn_1	s_1	$d_1 = H(s_1 \| pwd_1)$
usn_2	s_2	$d_2 = H(s_2 \| pwd_2)$
$\ldots$	$\ldots$	
usn_n	s_n	$d_n = H(s_n \| pwd_n)$

+ Since every user has different salt, identical passwords will not have identical hashes

+ No frequency analysis

+ No precomputation: when salting one cannot use preexisting tables to crack passwords easily

- store **salted hashes** of passwords

Attempt #4: **salt and hash** passwords

Password DB

usn_1	s_1	$d_1 = H(s_1 \| \| pwd_1)$
usn_2	s_2	$d_2 = H(s_2 \| \| pwd_2)$
$\dots$	$\dots$	
usn_n	s_n	$d_n = H(s_n \| \| pwd_n)$

+ Since every user has different salt, identical passwords will not have identical hashes
+ No frequency analysis
+ No precomputation: when salting one cannot use preexisting tables to crack passwords easily

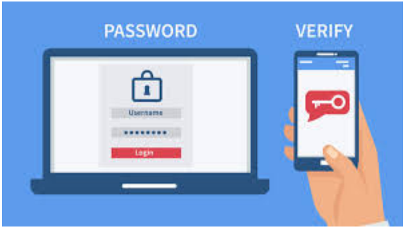
- store **salted hashes** of passwords
- use a **slow hash function** - *eg.* $H(pwd) = h^{1000}(pwd)$

Two factor authentication

- **Defending against compromised/stolen password** - even if Alice's password is stolen (offline attack, dictionary attack, malware attack, *etc*)

Two factor authentication

- **Defending against compromised/stolen password** - even if Alice's password is stolen (offline attack, dictionary attack, malware attack, *etc*)
- Password compromise mitigation - use **two factor authentication** (2FA)

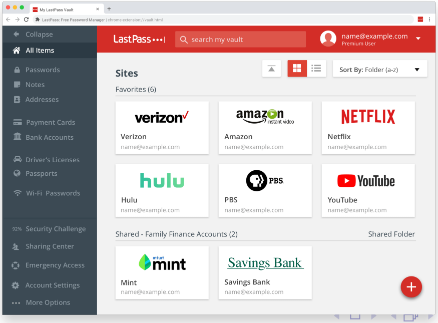


Password manager

- **Strong passwords are not easy to remember** - users are expected to memorise tens of different hard to guess passwords and humans are not good at this

Password manager

- **Strong passwords are not easy to remember** - users are expected to memorise tens of different hard to guess passwords and humans are not good at this
- Weak passwords mitigation - use a **password manager** - pick and memorise a single strong password to the password managers which takes care of storing and managing all the other passwords



Take aways

1. Password authentication
    - principles
    - network attacks
    - phishing attacks
    - keylogger attacks
    - offline attacks
    - online attacks
2. Password cracking
    - Brute force attack
    - Dictionary attack
3. How to store passwords:
    - store salted hashes of passwords
    - use a slow hash function
4. Enable 2FA
5. Use a password manager