University of BRISTOL

Systems Security

COMSM1500

bristol.ac.uk

Question about the reflective section?

- Do send me draft for feedback
  - Last year, students who did so got significantly better grade
  - It will only affect your grade positively
  - Something is missing …
  - Something could be improved …
  - Something is not clear …
  - … I will tell you so, so it is there when you get graded

University of BRISTOL

Authentication

bristol.ac.uk

Authentication/identification:

who is this ?

≠

authorisation/access control:

are they allowed to do this ?

authentication

You can authenticate with something you ...

- ?
- ?
- ?

authentication

You can authenticate with something you ...

- *know* e.g. a password
- *have* e.g. an ID card
- *are* e.g. biometrics

p@s$w0rD

authentication

You can authenticate with ...

- *sth. you know* e.g. a password
- *sth. you have* e.g. an ID card
- *sth. you are* e.g. biometrics

- *your location*
- *your behaviour*

} extra factors, becoming much more widespread

University of BRISTOL

Passwords

bristol.ac.uk

What is a password?

- Secret shared between a user and a service
- Simplest implementation?

What is a password?

- Secret shared between a user and a service
- Simplest implementation?
  - Table: usr -> passwd

University of BRISTOL

Threat 1

Attacker have access to the table

bristol.ac.uk

What is a password?

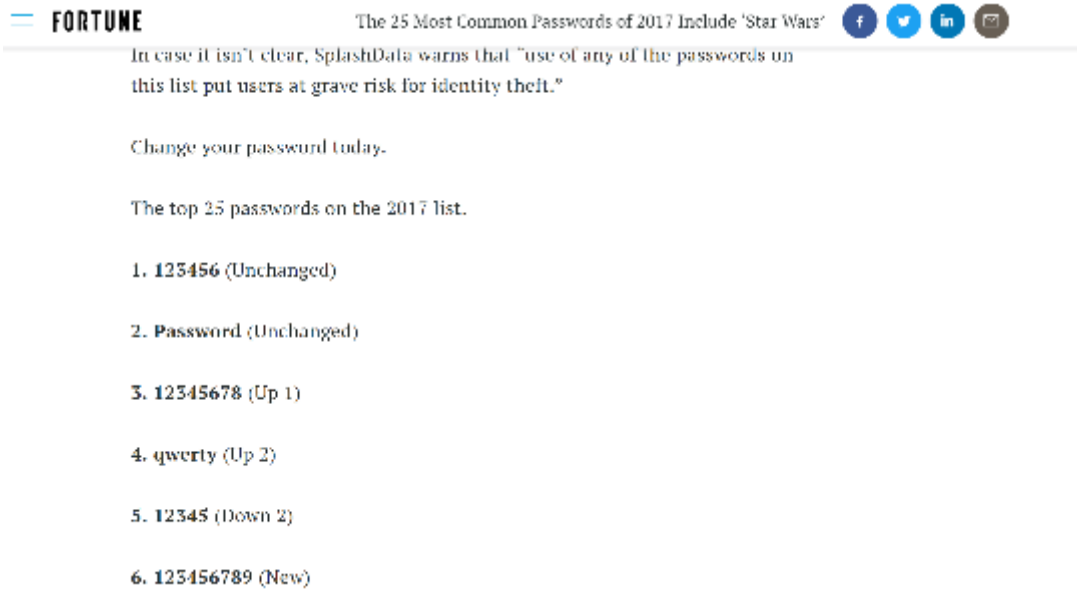
- Secret shared between a user and a service
- Simplest implementation?
  - Table: usr -> passwd
  - Not great
  - Table: usr -> Hash(passwd)
  - We assume hash cannot be reverted

University of BRISTOL

What is the problem?

bristol.ac.uk

Skewed distribution



FORTUNE

The 25 Most Common Passwords of 2017 Include 'Star Wars'

In case it isn't clear, SplashData warns that "use of any of the passwords on this list put users at grave risk for identity theft."

Change your password today.

The top 25 passwords on the 2017 list.

1. **123456** (Unchanged)

2. **Password** (Unchanged)

3. **12345678** (Up 1)

4. **qwerty** (Up 2)

5. **12345** (Down 2)

6. **123456789** (New)

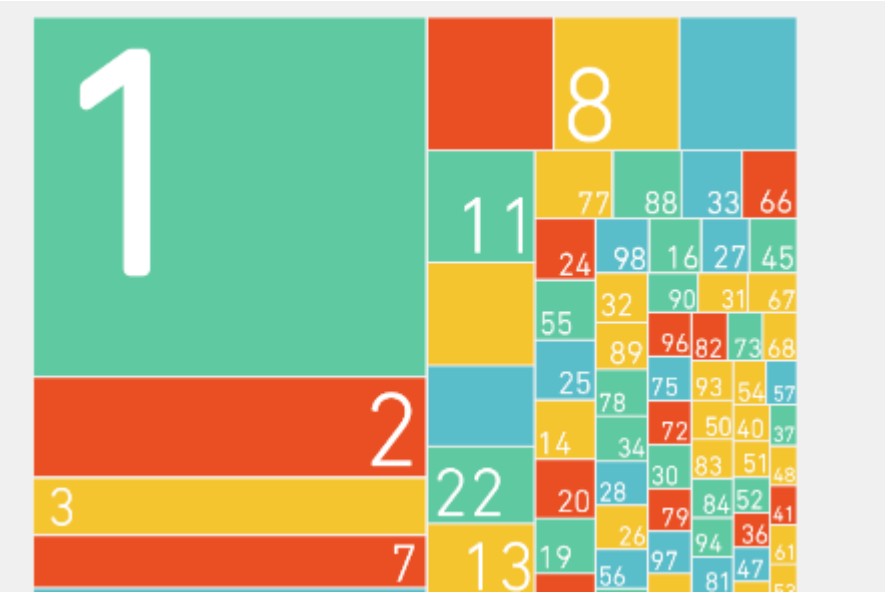
Skewed distribution

- Top 100,000 passwords
  - https://github.com/danielmiessler/SecLists/blob/master/Passwords/Common-Credentials/10-million-password-list-top-100000.txt
- >20% of users

Skewed distribution

Solution? (bad one)

- Ask the user to add some specific characters



Solution? (bad one)

- No word from the dictionary

How attacker use this?

- Dictionary attack
- Go through the list of most used password
- Check for a match

Solution? better hash

- usr -> hash(password)
- Hash -> low computational cost
- More costly hash
  - Eg.PBKDF2, Bcrypt etc…
- Still not a solution!

Rainbow table

- Attacker
  - password -> Hash1(password), Hash2(password) etc…
  - If your website use a framework the attacker knows the hash function
- Try to find a match in the service table
- Due to password distribution likely to get a match
- Computational cost is independent from the hash function
  - One time cost

Solution? Salt

- Hash(salt, password)
- Different salt per password (for and across users)
- Salt does not need to be a secret
  - Defeat rainbow table
  - Increase cost of dictionary attack
- Not a panacea
  - If your password is 1234
  - Arms race

University of BRISTOL

Threat 2

Password recovery

bristol.ac.uk

Password recovery

- We've seen example in previous weeks
- External knowledge
  - Social Media
  - Famous people
  - Environment vulnerability
  - etc…
- Social engineering
  - Fake e-mail
  - Fake website
  - Ask over the phone
  - etc…
- Entropy of recovery is very bad! Entropy = Min(Ent(password), Ent(Recovery))
  - e.g. what's your favorite color? (likely red or blue)
  - User selected questions are terrible (e.g. 2+3)

University of BRISTOL

Threat 3

Man in the middle

bristol.ac.uk

Transmit password

- In the clear?

Transmit password

- In the clear?
  - Just need to listen on network packet…

Transmit password

- In the clear?
- Over encrypted connection?

Transmit password

- In the clear?
- Over encrypted connection?
  - Man in the middle attack
  - Need to authenticate the server (e.g. Am I really talking to google?)

Transmit password

- In the clear?
- Over encrypted connection?
- Send the hash?

Transmit password

- In the clear?
- Over encrypted connection?
- Send the hash?
  - Does not make a difference!

Transmit password

- In the clear?
- Over encrypted connection?
- Send the hash?
- Challenge response protocol?

Transmit password

- In the clear?
- Over encrypted connection?
- Send the hash?
- Challenge response protocol?
  - Bob can verify Alice know the secret
  - If someone pretend to be Bob he cannot know the password

Transmit password

- In the clear?
- Over encrypted connection?
- Send the hash?
- Challenge response protocol?
  - Bob can verify Alice know the secret
  - If someone pretend to be Bob he cannot know the password
  - Naïve (check online)

University of BRISTOL

Threat 4

“Hammering” the login page

bristol.ac.uk

Anti-hammering defences

- Rate-limit
  - Number of guess, then password revoked
- Time-outs
  - e.g. prevent to login within the next hours
- Why is it important?

Anti-hammering defences

- Rate-limit
  - Number of guess, then password revoked
- Time-outs
  - e.g. prevent to login within the next hours
- Why is it important?
  - Password have very low entropy!
  - Need to prevent brute forcing

University of BRISTOL

Better than password?

bristol.ac.uk

Comparing authentication method

Comparing authentication method

- WARNING
  - Not an absolute
  - Open to discussion/debate
  - Help you think about the problem

Comparing authentication method

- WARNING
  - Not an absolute
  - Open to discussion/debate
  - Help you think about the problem
- Where to read the paper discussed during the lecture?

Comparing authentication method

- WARNING
  - Not an absolute
  - Open to discussion/debate
  - Help you think about the problem
- Where to read the paper discussed during the lecture?

Usability

Category	Password	Biometrics
Memory effortless	No	
Scalable for users	No	
Nothing to carry	Yes	
Physically effortless	No	
Easy to learn	Yes	
Infrequent error	~Yes	
Easy recovery from loss	Yes	

Deployability

Category	Password	Biometrics
Accessible	Yes	
Negligible cost per user	Yes	
Server-compatible	Yes	
Browser-compatible	Yes	
Non-propriotary	Yes	

Security (resilient to)

Category	Password	Biometrics
Physical observation	No	
Targeted impersonation	~Yes	
Throttled guessing	Yes	
Unthrottled guessing	No	
Internal observation	No	
Leak from other verifiers	No	
Phishing	No	

University of BRISTOL

Biometrics what do you think?

Think of fingerprint

bristol.ac.uk

Usability

Category	Password	Biometrics
Memory effortless	No	
Scalable for users	No	
Nothing to carry	Yes	
Physically effortless	No	
Easy to learn	Yes	
Infrequent error	~Yes	
Easy recovery from loss	Yes	

Deployability

Category	Password	Biometrics
Accessible	Yes	
Negligible cost per user	Yes	
Server-compatible	Yes	
Browser-compatible	Yes	
Non-propriotary	Yes	

Security (resilient to)

Category	Password	Biometrics
Physical observation	No	
Targeted impersonation	~Yes	
Throttled guessing	Yes	
Unthrottled guessing	No	
Internal observation	No	
Leak from other verifiers	No	
Phishing	No	

University of BRISTOL

Biometrics what do you think?

Answers (some of them are debatable, and that is part of the point)

bristol.ac.uk

Usability

Category	Password	Biometrics
Memory effortless	No	Yes
Scalable for users	No	Yes
Nothing to carry	Yes	Yes
Physically effortless	No	~Yes
Easy to learn	Yes	Yes
Infrequent error	~Yes	No
Easy recovery from loss	Yes	No

Deployability

Category	Password	Biometrics
Accessible	Yes	~Yes
Negligible cost per user	Yes	No
Server-compatible	Yes	No
Browser-compatible	Yes	No
Non-propriotary	Yes	No

Security (resilient to)

Category	Password	Biometrics
Physical observation	No	Yes
Targeted impersonation	~Yes	No
Throttled guessing	Yes	Yes
Unthrottled guessing	No	No
Internal observation	No	No
Leak from other verifiers	No	No
Phishing	No	No

Comparing authentication method

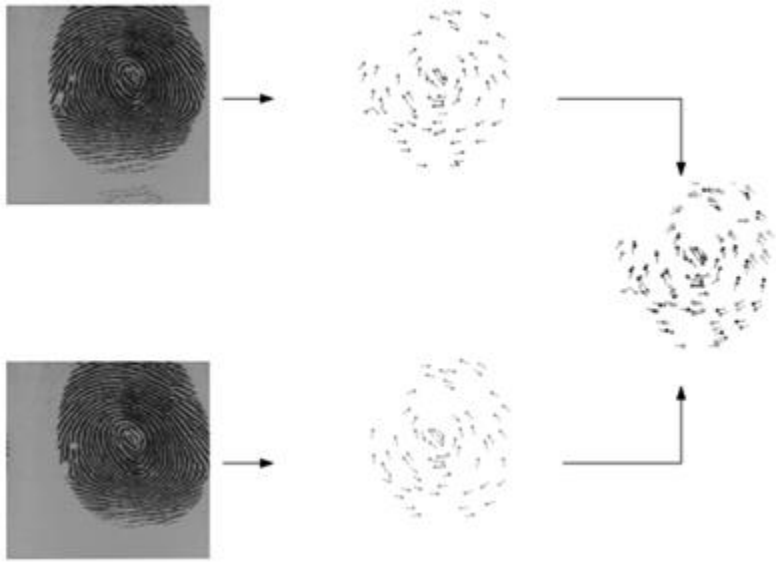
- It is a discussion
  - Need to understand the context
  - Need to understand the implementation
- It is not black and white
- If there were something undoubtfully better we would not use password

Entropy?

- Every fingerprint is unique?

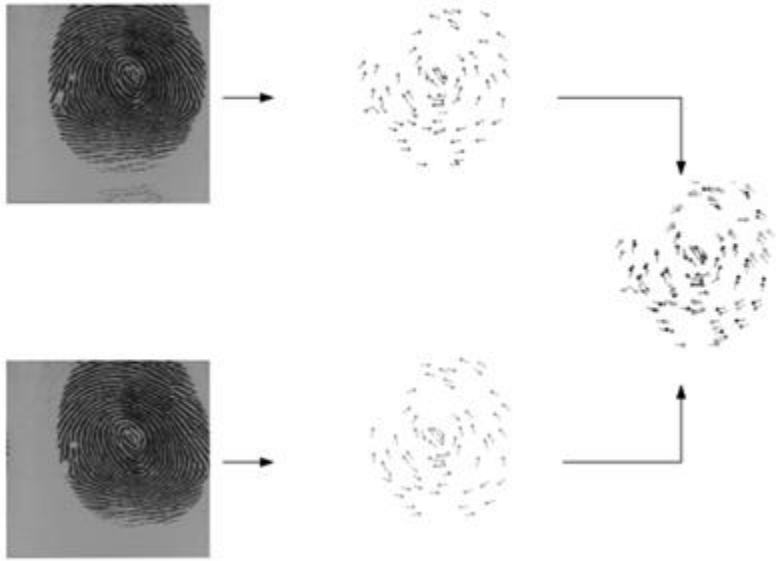
Entropy?

- Every fingerprint is unique?
- Feature extraction
- No exact match
  - X/Y match
- ~8.3 random characters password (again debatable, but not as good as you would assume)

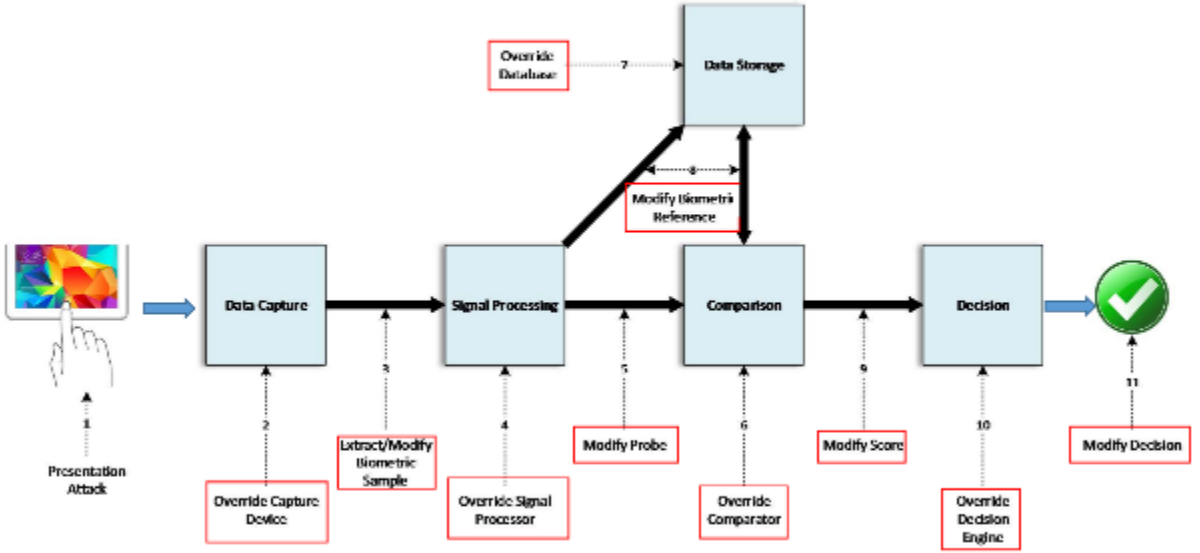


Entropy?

- Every fingerprint is unique?
- Feature extraction
- No exact match
  - X/Y match
- ~8.3 random characters password (again debatable, but not as good as you would assume)
- US NIST: biometrics is NOT OK for remote service authentication!



Potential vulnerability



24h after fingerprint iPhone

https://vimeo.com/75324765

24h after fingerprint iPhone

https://vimeo.com/75324765

- You can do the same from photo with high enough resolutions…

2FA

Two-factor authentication = use of at least two *different* factors such as ID card and password.

image credit: google

2FA

- More and more common
  - Steam
  - Google
  - Amazon
  - Twitter
  - Banks
- Optional on some services, mandatory for others
- By the way SMS authentication is deprecated (NIST)
  - There is proof of existing attack…
  - Still in use (e.g. twitter)

University of BRISTOL

Thank you

Office MVB 3.26

bristol.ac.uk