University of BRISTOL

Computer Systems B

COMS20012

Introduction to Operating Systems and Security

bristol.ac.uk

University of BRISTOL

Passwords

bristol.ac.uk

What is a password?

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

bristol.ac.uk

What is a password?

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

bristol.ac.uk

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

bristol.ac.uk

University of BRISTOL

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)

bristol.ac.uk

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

bristol.ac.uk

Skewed distribution

bristol.ac.uk

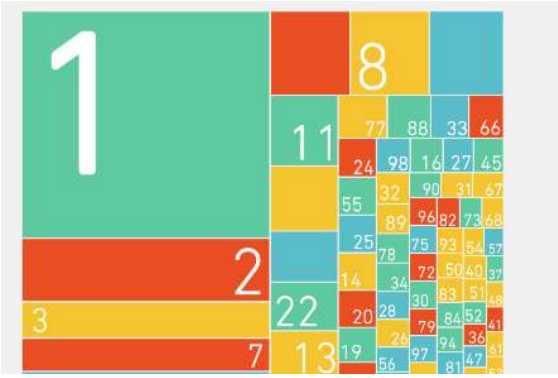
How attacker use this?

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

bristol.ac.uk

Solution? (bad one)

- Ask the user to add some specific characters



bristol.ac.uk

Solution? (bad one)

- No word from the dictionary

bristol.ac.uk

Solution? better hash

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

bristol.ac.uk

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

bristol.ac.uk

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

bristol.ac.uk

University of BRISTOL

Thank you

bristol.ac.uk