Class Notes

September 9th, 2021

Password creation policies are put in place because humans are bad at creating unique passwords for different services.

We want to be able to measure the increase in security between different passwords. If we have a way to measure it, such as the NIST score, it gives us a rough idea.

Y axis - % Passwords Cracked

X axis - # of Guesses

The NIST Score does not capture the human error of easy, guessable passwords. The NIST entropy score does not match the real world use cases. Which leads to a bad sense of security for people given a password policy.

**Credential Stuffing Attack:**

Take a password from a leak, with a given email address and try them on every possible site that you want to crack.

You can also do Mangling, which is attempting different combinations using the same password that was leaked, such as appending a 1 after it.

**Reasons Why Credential Stuffing Is Dangerous:**

* People tend to use the same passwords for multiple websites or slight variations
* Legit Usernames & Password pairs
* Easy to automate
* Low Effort for giant reward

**Password Managers**:

* Single Point of Failure (Users forget the password to the password manager)
* Autogenerate Strong Passwords, but you're not going to remember it

**Security Study in 2015 On Password Managers:**

What are the top 3 things you do to stay safe online? (Expert Responses)

1.) Keep System Software up to date for security patches (35%)

2.) Avoid Password Reuse (25%)

3.) 2FA (20% of experts)

Average Person Responses

1.) Having anti-virus software (42%)

2.) Strong Passwords

3.) Change Passwords

Pick friend or family member for videos:

Q1.) Tell them why they should use a password manager

Q2.) Pick a password manager, and make a tutorial for it.