## Common Threats and Solutions Password Managers

#### Irfan Kanat

Department of Digitization Copenhagen Business School

May 24, 2021

This work is licensed under a Creative Commons Attribution 4.0 International License.



Common Threats and Solutions

Irfan Kanat Dapartener af Digitization Copernages Bulents Schoo May 24, 2021

Common Threats and Solutions

This such is literard under a Creation Commune Attribution 6.0 in

In this video we will learn how to use a password manager.

Irfan Kanat (CBS)

Common Threats and Solutions

May 24, 2021

1/5

Possibilities...

2021-05-24

└A Strong Password

Common Threats and Solutions

A Strong Password

Possibilities...

Possibilities...

$$I = abc...xyz = 26$$



2021-05-24 └A Strong Password

Common Threats and Solutions

Possibilities... I = abc...xyz = 26

A Strong Password

Irfan Kanat (CBS)

Common Threats and Solutions

May 24, 2021 2 / 5

Possibilities...

$$I = abc...xyz = 26$$

$$III = 26 \times 26 \times 26 = 17$$

Irfan Kanat (CBS)

Common Threats and Solutions





 $III = 26 \times 26 \times 26 = 17576$ 

Common Threats and Solutions

└A Strong Password

A Strong Password

Possibilities... I = abc...xyz = 26  $NV = 26 \times 26 \times 26 = 17576$ 

Possibilities...

$$I = abc...xyz = 26$$

$$III = 26 \times 26 \times 26 = 17576$$

$$IIII = 26 \times 26 \times 26 \times 26 = 456976$$



Common Threats and Solutions Possibilities... I = abc...xyz = 26  $N = 26 \times 26 \times 26 = 17576$ NV = 26 × 26 × 26 × 26 = 456976 └A Strong Password

A Strong Password

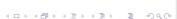
Possibilities...

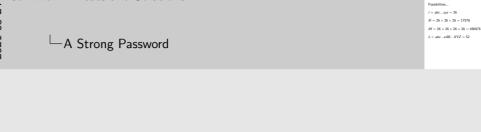
$$I = abc...xyz = 26$$

$$III = 26 \times 26 \times 26 = 17576$$

$$IIII = 26 \times 26 \times 26 \times 26 = 456976$$

$$L = abc...zAB...XYZ = 52$$





Common Threats and Solutions

A Strong Password

Possibilities...

$$I = abc...xyz = 26$$

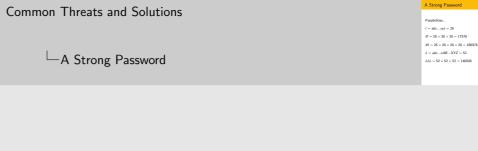
$$III = 26 \times 26 \times 26 = 17576$$

$$IIII = 26 \times 26 \times 26 \times 26 = 456976$$

$$L = abc...zAB...XYZ = 52$$

$$LLL = 52 \times 52 \times 52 = 140608$$

マロティタティミティミテーミ May 24, 2021



Possibilities...

$$I = abc...xyz = 26$$

$$III = 26 \times 26 \times 26 = 17576$$

$$IIII = 26 \times 26 \times 26 \times 26 = 456976$$

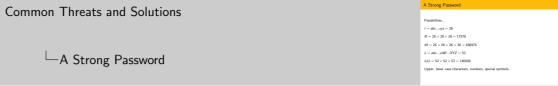
$$I = abc...zAB...XYZ = 52$$

$$III = 52 \times 52 \times 52 = 140608$$

Upper, lower case characters, numbers, special symbols...



May 24, 2021



The strength of the password can be estimated by how many possible tries it would take to guess the password. This is what a computer trying to **bruteforce** the password.

So two ways to increase the strength of the password. Size of the character set, and digits. So longer passwords made up of different types of characters (letters, numbers, symbols) are harder than shorter passwords made up of just one type of character.

Bruteforce is not the only way to crack a password. Trying all words in a dictionary, and combinations of words has also been done in the past. This is known as a **dictionary attack**. So don't use words in your password.

You can also just guess the password by using information about the person. So don't use personal facts as password.

Have You Been Pwned?

# ';--have i been pwned?

Check if your email or phone is in a data breach

email or phone (international format)

pwned?

Good news — no pwnage found!

No breached accounts and no pastes (subscribe to search sensitive breaches)



Common Threats and Solutions

Have You Been Pwned?



One way adversaries may get access to your accounts is by using your known passwords on other accounts.

So if your password was revealed in a data breach, all your other accounts using the same password is also in danger.

I highly recommend you go and check your e-mail address on haveibeenpwned.com

Irfan Kanat (CBS)

Common Threats and Solutions

## Good Password

No Personal Facts

Irfan Kanat (CBS)

No Words

Character Types

Long

Don't Reuse

◆□▶◆□▶◆豆▶◆豆> 豆 かなで

May 24, 2021 4 / 5

Common Threats and Solutions Good Password

Long Character Types No Personal Facts Don't Reuse

Good Password

#### **Password Managers**



#### ■ Encrypted

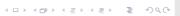
Complete database encryption using industry standard 256-bit AES. Fully compatible with KeePass Password Safe formats. Your password database works offline and requires no internet connection.

#### Cross-Platform

Every feature looks, feels, works, and is tested on Windows, macOS, and Linux. You can expect a seamless experience no matter which operating system you are using.

#### ♥ Open Source

The full source code is published under the terms of the GNU General Public License and made available on GitHub. Use, inspect, change, and share at will; contributions by everyone are welcome.



Common Threats and Solutions

Password Managers



A good password is not only hard to guess, it is also hard to remember for humans. So it is imperative you use a password manager.

There are various password managers out there. The most convenient ones are cloud based services like lastpass or 1password. Unfortunately these type of services run the risk of becoming paid after the fact. Last pass for example changed the terms of its free tier in 2020, putting their users in a difficult situation.

Therefore I recommend open source solutions. They are not as convenient, but it gives you more control.

Irfan Kanat (CBS)