Yubikey, a physical key that provides 2-factor authentication

CS 88S

Protecting yourself: apps, methods, practices

Week 6

Frank Chen | Spring 2017

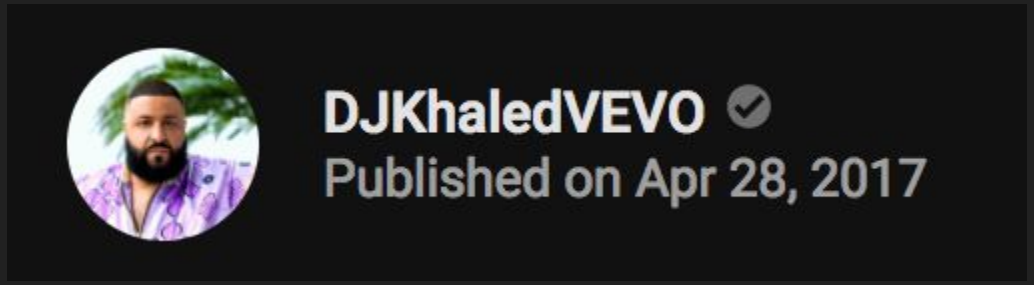
Agenda

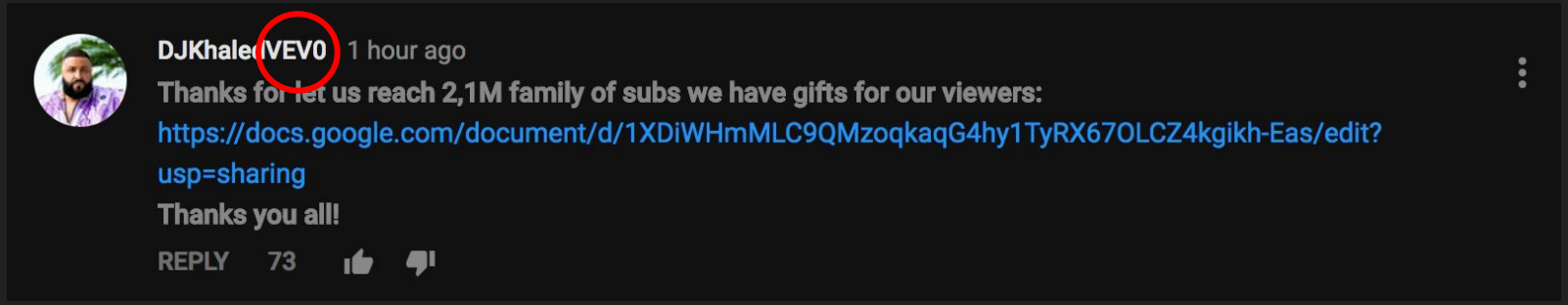
- *WireShark Demo, Final Project*
- *Review last week's material*
- *HTTPS, Safe Practices Online*
- *2 Factor Authentication*
- *Back up everything*
- *Use a Password Manager*

Agenda

- ***WireShark Demo, Final Project***
- *Review last week's material*
- *HTTPS, Safe Practices Online*
- *2 Factor Authentication*
- *Back up everything*
- *Use a Password Manager*

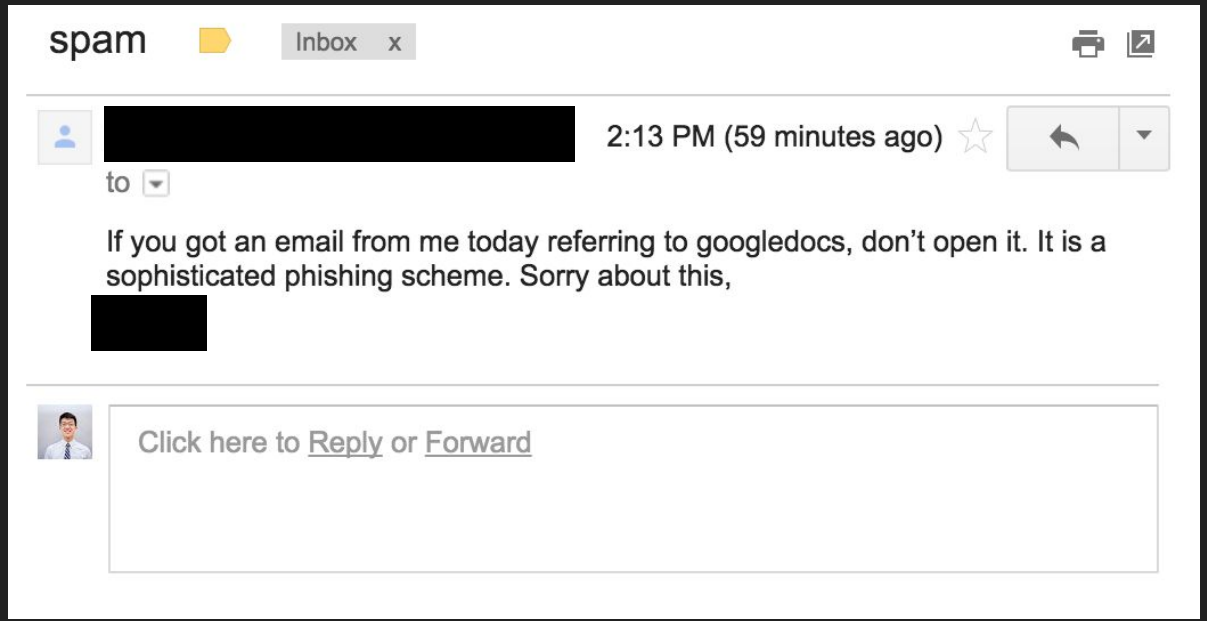
YouTube Phish





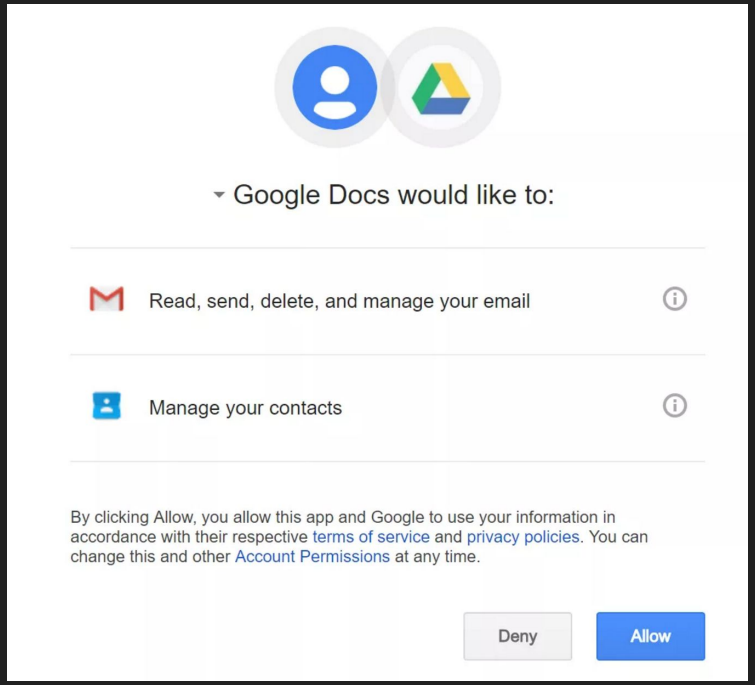
Source: http://bit.ly/2pIoWQW

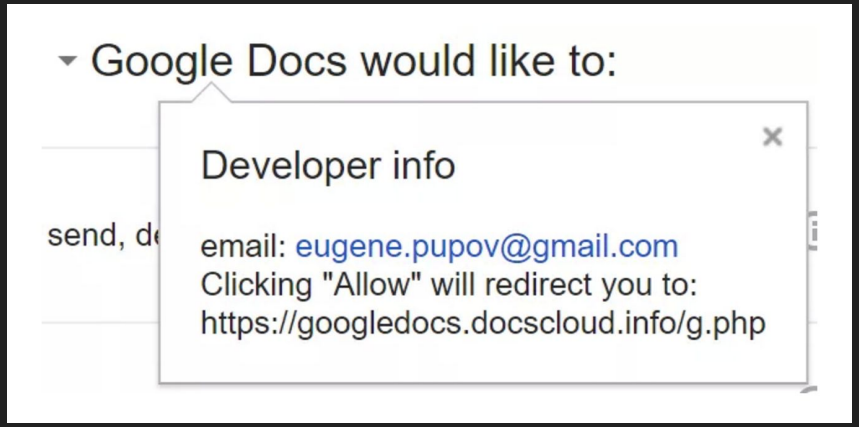
Google Docs Phish



Source: http://bit.ly/2pIoWQW

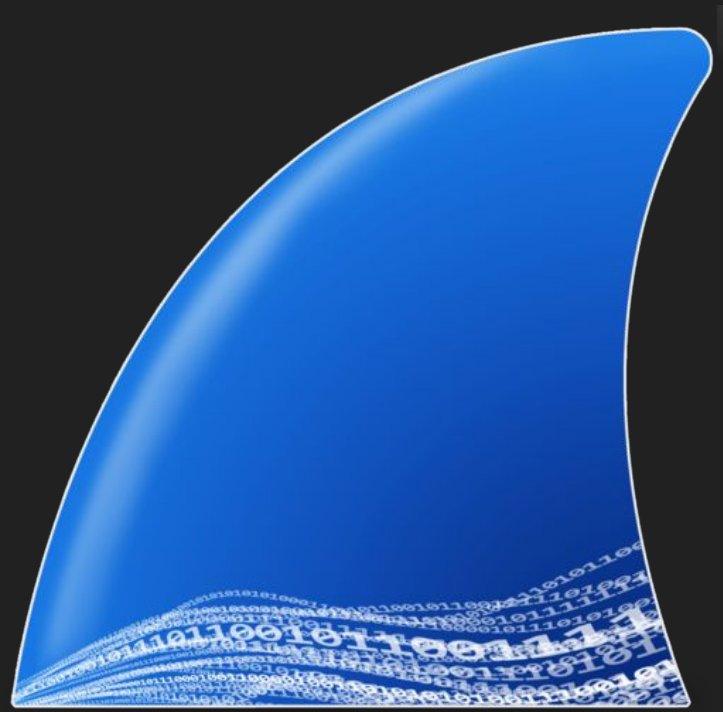
Google Docs Phish





Source: http://bit.ly/2pIoWQW

Wireshark Demo



Final Project

kfrankc.me/cs88s/final_project.pdf

Image Source: http://bit.ly/2pIoWQW

Agenda

- *WireShark Demo, Final Project*
- ***Review last week's material***
- *HTTPS, Safe Practices Online*
- *2 Factor Authentication*
- *Back up everything*
- *Use a Password Manager*

1 2 3 4 5 6 7

What happens when you type www.google.com?

Symmetric Key

Source: http://bit.ly/1I2YUeS

Public/Private Key

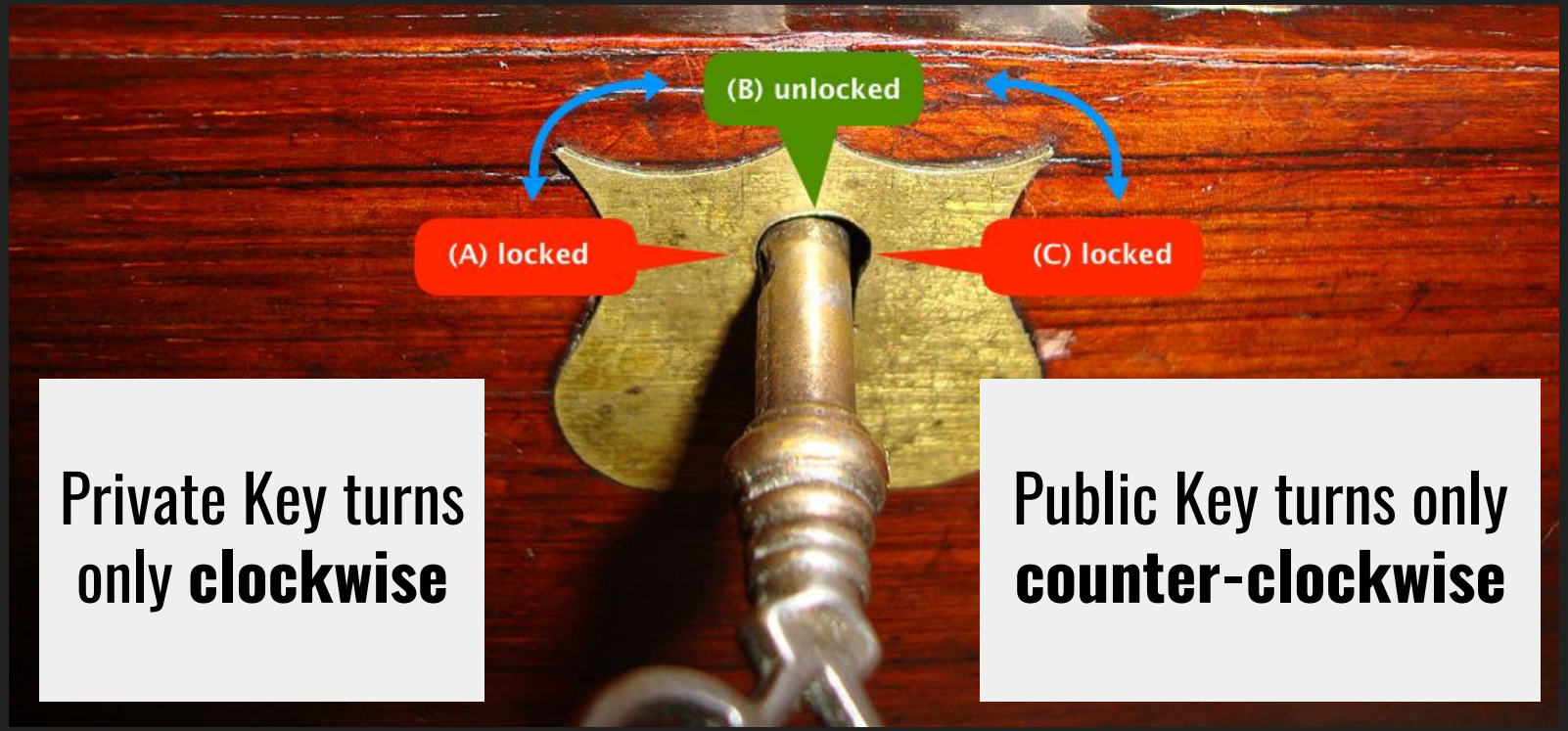
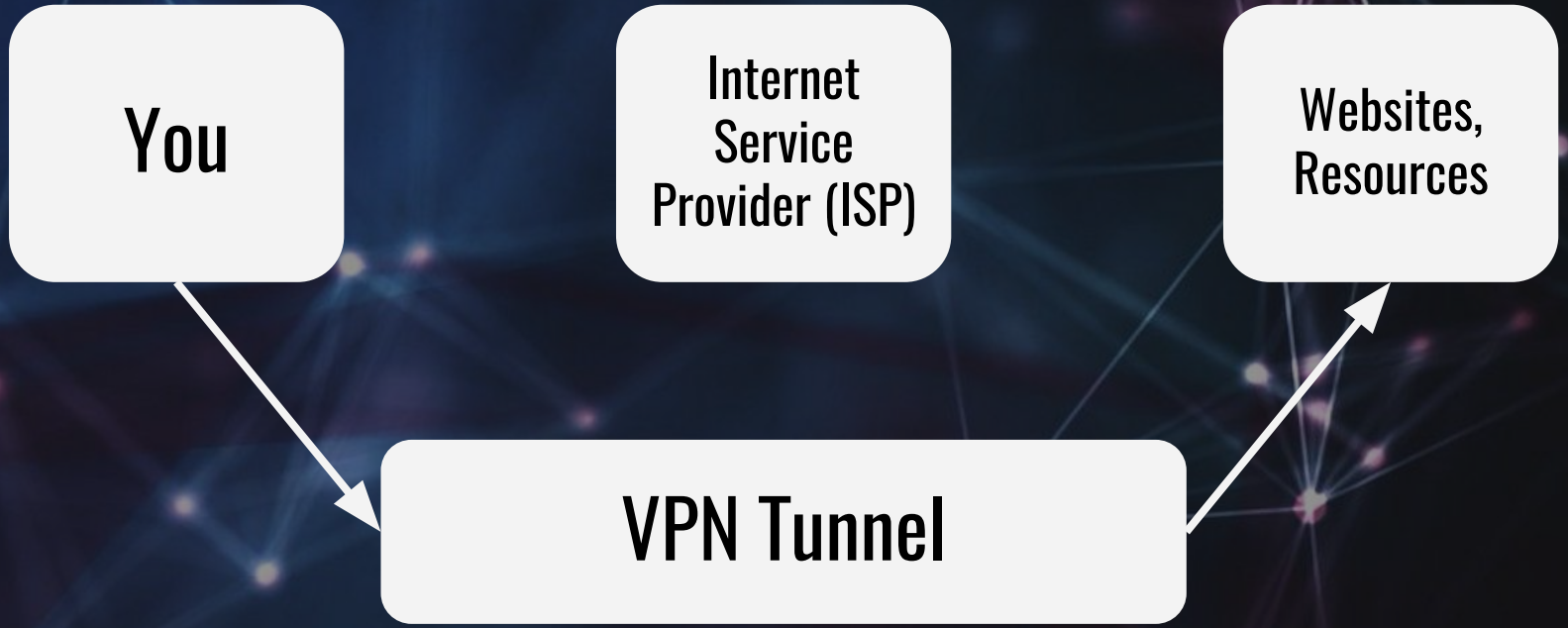


Image Source: http://bit.ly/1I2YUeS

Virtual Private Network (VPN)



Source: http://bit.ly/2qBrNZh

So Far...

cybersecurity ✔

protect myself ✘

hack ✔

privacy ✘

money, personal contact, identification ✔

extra (security in IoT devices) ✘

Agenda

- *WireShark Demo, Final Project*
- *Review last week's material*
- ***HTTPS, Safe Practices Online***
- *2 Factor Authentication*
- *Back up everything*
- *Use a Password Manager*

HTTP

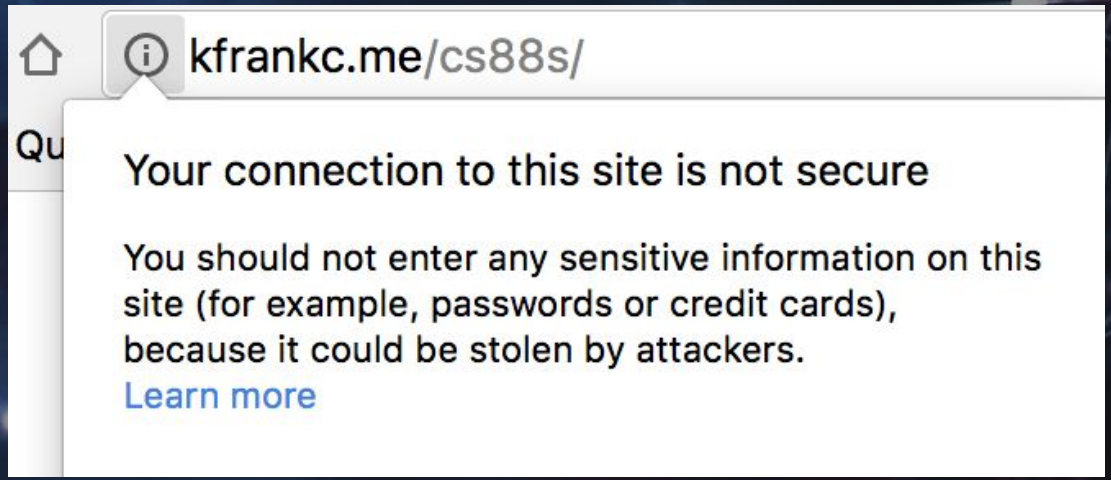
Def: *HTTP (Hypertext Transfer Protocol) is the procedure for exchanging information on the Internet*

It is ***easy to intercept***

How secure is HTTP?

- Authentication ✗
- Integrity ✗
- Privacy ✗

HTTPS, abridged



Source: http://bit.ly/2qEPNyc

HTTPS, abridged

Def: *HTTPS is HTTP over Secure Socket Layer.*

HTTPS ***encrypts*** *an HTTP message prior to transmission and* ***decrypts*** *a message upon arrival via* ***SSL Transaction.***

SSL Transaction

Source: http://bit.ly/2pTzoTY

****Note:** To further understand the relationship between SSL and HTTP, you'll first need to understand the OSI model of Computer Networks, which is out of the scope of this class.*

SSL Transaction

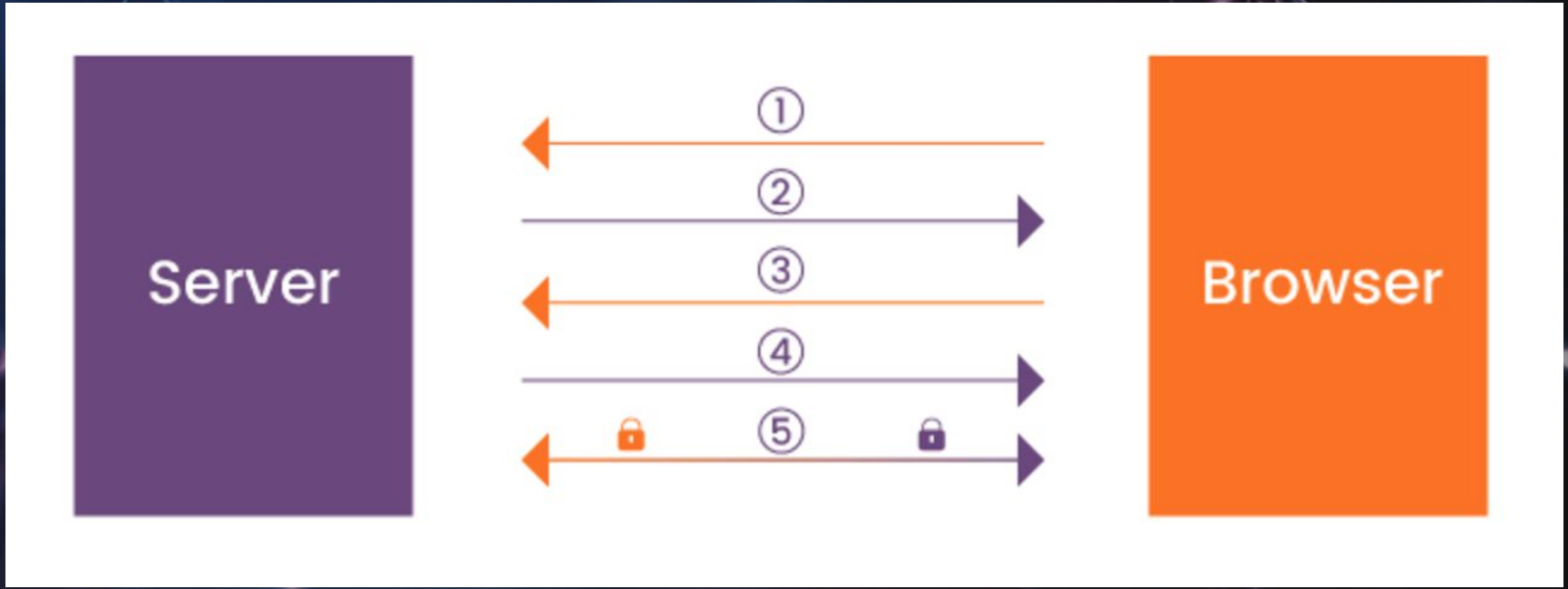


Image Source: http://bit.ly/2qoE6w9

How secure is HTTPS?

Authentication ✔

Integrity ✔

Privacy ✔

HTTPS Everywhere

- *Browser Extension*
- *Automatically redirect HTTP webpage into HTTPS webpage if possible*
- *Open Source*

Source: `http://bit.ly/2qcu3df`

Be Wary of Public Wi-Fi

Be Wary of Email Links

Agenda

- *WireShark Demo, Final Project*
- *Review last week's material*
- *HTTPS, Safe Practices Online*
- ***2 Factor Authentication***
- *Back up everything*
- *Use a Password Manager*

Authentication

What you **know**

What you **own**

Who you **are**

Authentication

What you **know**

What you **own**

Who you **are**

Which Password is more secure?

monkey-ocean-superior-pillow

3058472038475

They are about the same

Source: http://bit.ly/2pmNOuB

Which Password is more secure?

monkey-ocean-superior-pillow

4 common words: *$2000^4 \sim 2^{43.9}$ combinations*

3058472038475

13 random digits: *$10^{13} \sim 2^{43.2}$ combinations*

Source: http://bit.ly/2pmNOuB

Authentication

What you **know**

What you **own**

Who you **are**

Yubikey

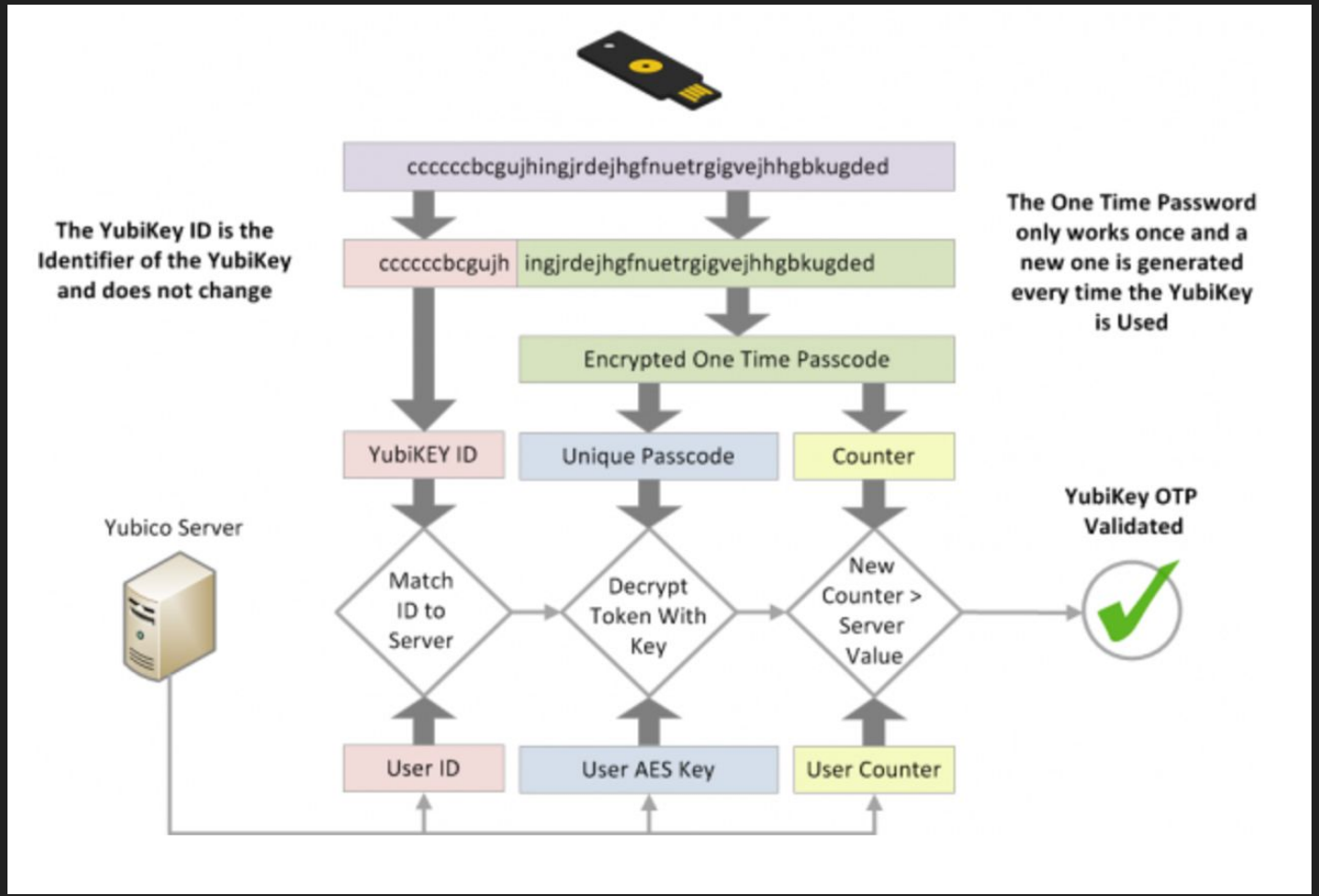
- *Physical 2-Factor Authentication Device*
- *Generates One-Time-Passwords (OTPs)*

Yubikey's OTP

cccjgjgkhcbb irdrfdnlnghhfgrtnnlgedjlftrbdeut

cccjgjgkhcbb gefdkbbditfjrlniggevfhenublfnrev

cccjgjgkhcbb cvchfkfhiiuunbtnvgihdfiktncvlhck



Source: http://bit.ly/2qP6yUb

Yubikey Demonstration

2-Factor OTP Generators

Authentication

What you **know**

What you **own**

Who you **are**

Fingerprint Scanner

Source: http://apple.co/1En9Tz7

Single Sign-On

Source: https://shibboleth.net/

Source:https://www.okta.com/

Agenda

- *WireShark Demo, Final Project*
- *Review last week's material*
- *HTTPS, Safe Practices Online*
- *2 Factor Authentication*
- ***Back up everything***
- *Use a Password Manager*

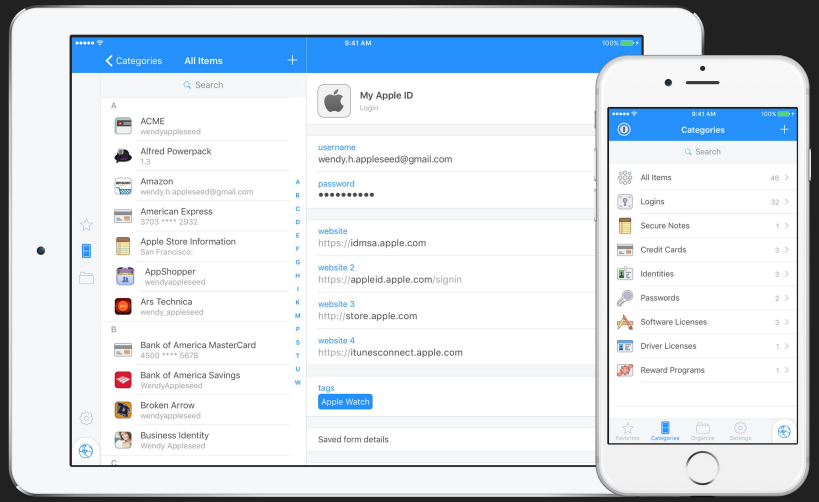
Cloud Storage

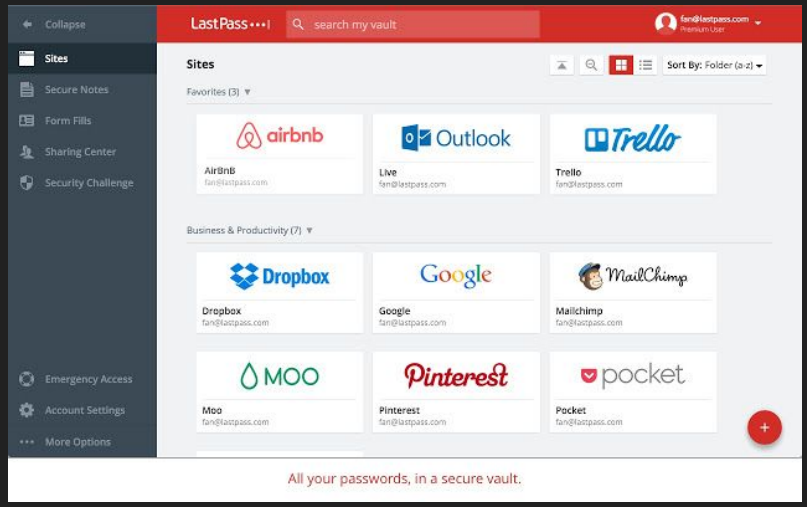
External Hard Drive

Agenda

- *WireShark Demo, Final Project*
- *Review last week's material*
- *HTTPS, Safe Practices Online*
- *2 Factor Authentication*
- *Back up everything*
- ***Use a Password Manager***

Password Managers





Safety in the Cloud Tip

Follow **at least one** of the Practices listed today!

Facebook's massive data center in Luleå

Next Week...