Keybase, a company that strives to provide everyone with GPG

CS 88S

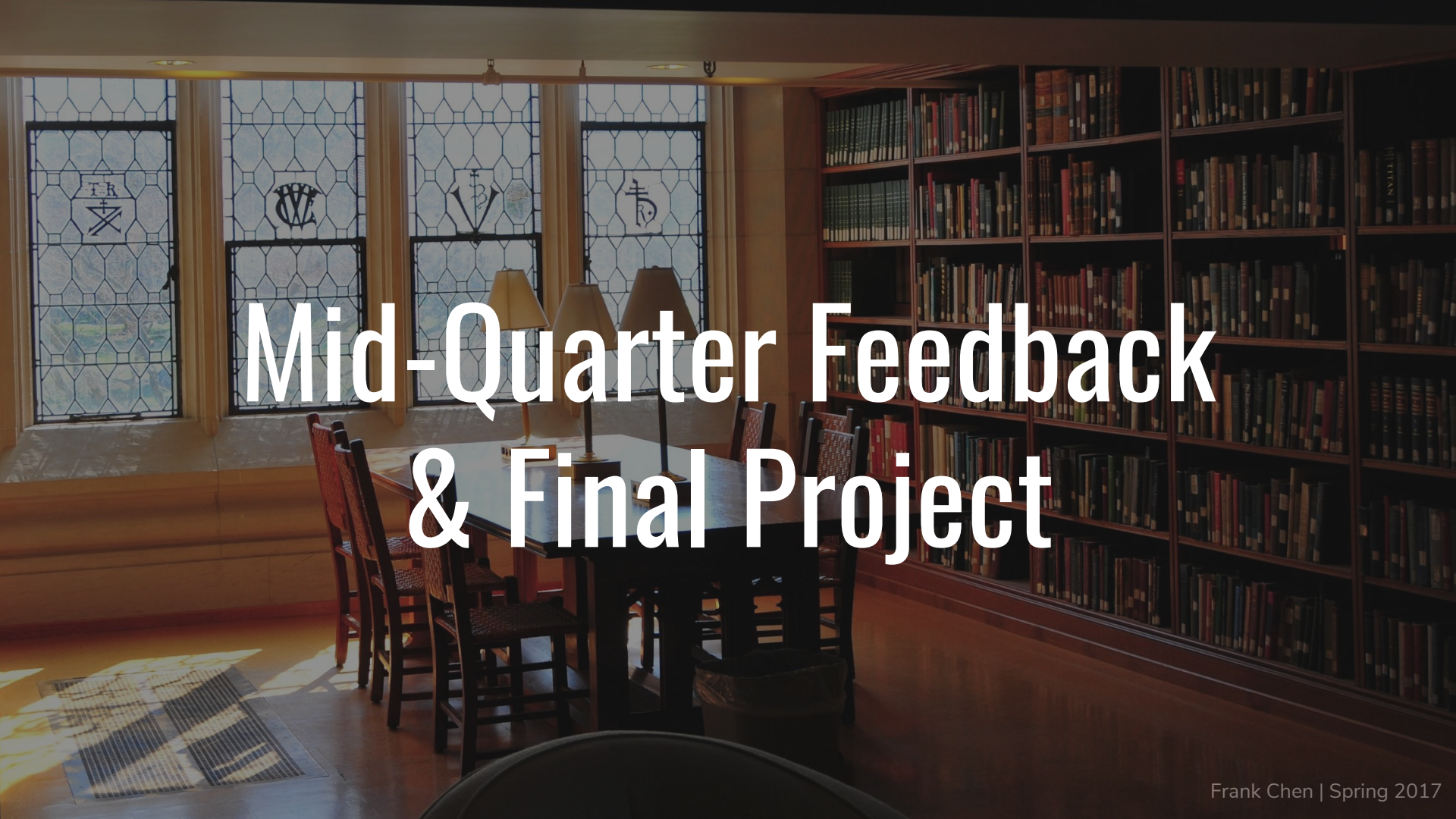
Web Browsing, Cryptography, VPN, PGP

Week 5

Frank Chen | Spring 2017

Agenda

- *Review last week's material*
- *How the Internet Works, abridged*
- *Cryptography/PGP*
- *How does a VPN Work?*
- *What is Proxy Browsing?*
- *Wireshark Demo*



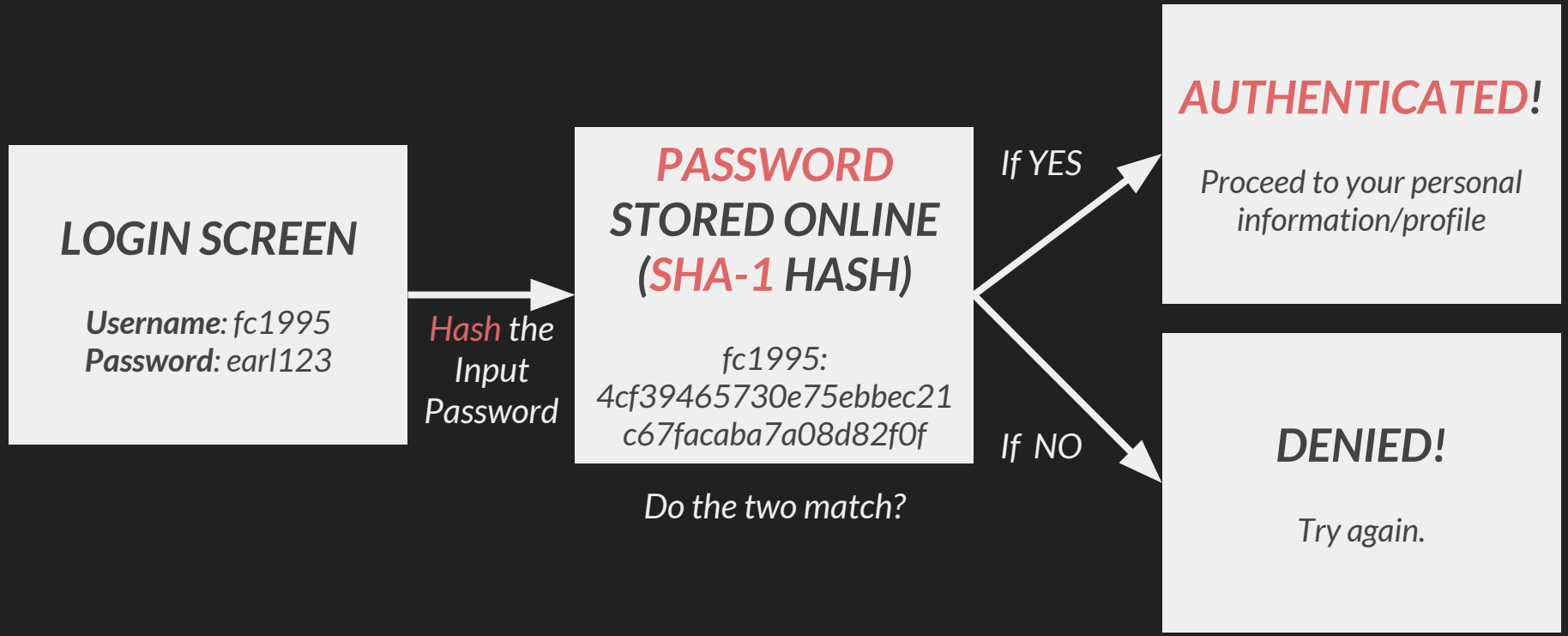
Mid-Quarter Feedback & Final Project

Frank Chen | Spring 2017

Agenda

- ***Review last week's material***
- *How the Internet Works, abridged*
- *Cryptography/PGP*
- *How does a VPN Work?*
- *What is Proxy Browsing?*
- *Wireshark Demo*

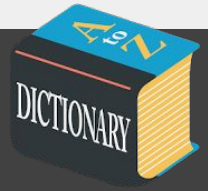
A typical Authentication Session



A typical Dictionary Attack

PASSWORD FROM DICTIONARY

...Dog, Dogs, Dogcatcher, Dogcatchers, Dogberry, Dogberries, Dogma, Dogmatic, Dogmatized, Dog1. Dog2, Dog3, Dog4...



Hash the Input Password

PASSWORD File (SHA-1 HASH)

fc1995: 4cf39465730e75ebbec21 c67facaba7a08d82f0f

Do the two hashes match?

If YES

RETRIEVED THE PASSWORD

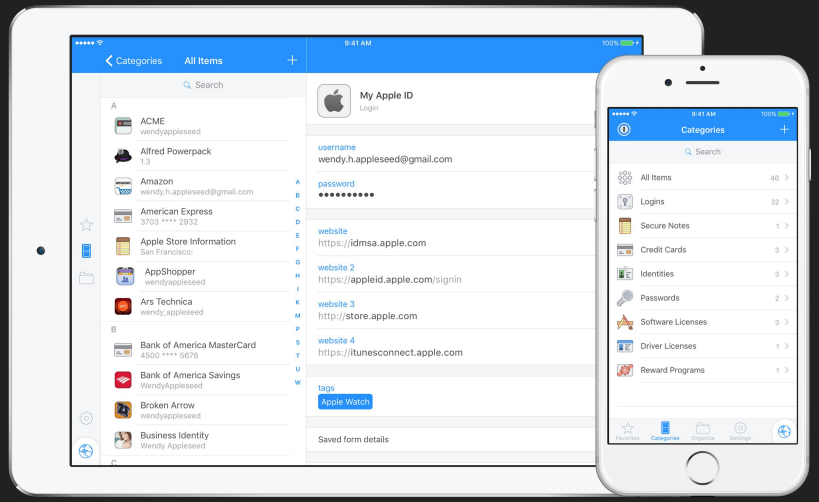
Proceed to use the password to login to your account

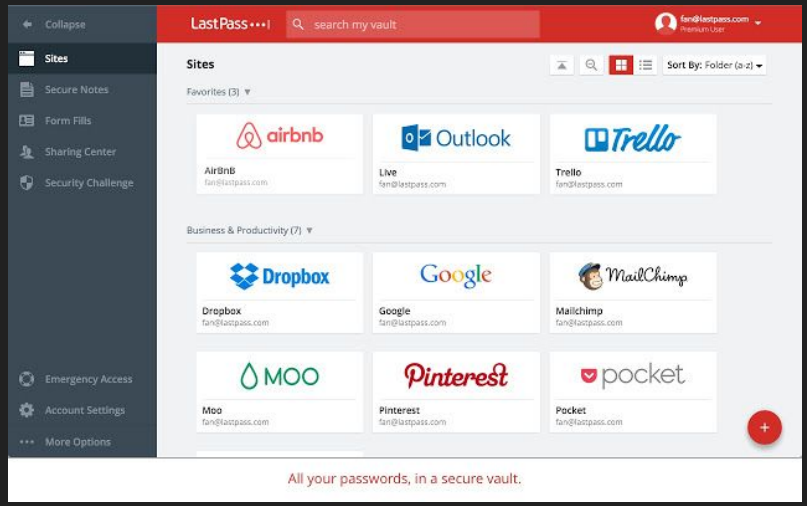
If NO

CONTINUE!

Dictionary Attacks can submit up to 1000 attempts per minute

Password Managers





Agenda

- *Review last week's material*
- ***How the Internet Works, abridged***
- *Cryptography/PGP*
- *How does a VPN Work?*
- *What is Proxy Browsing?*
- *Wireshark Demo*

What happens when you type www.google.com?

1 2 3 4 5 6 7

What happens when you type www.google.com?

Using a Browser

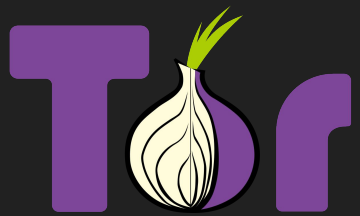
Def: A Program installed on your computer that allows you to visit websites.

Source: http://bit.ly/2oX9Gwr

There are many Browsers





Browser checks cache

Def: The browser cache is a temporary storage location on your computer for files downloaded by your browser to display websites.

Browser checks cache

Browser asks OS for IP Address

Def: Operating System (OS) is the software that supports a computer's basic functions

Browser asks OS for IP Address

Def: Internet Protocol (IP) Address is a unique string of numbers separated by periods that identifies each computer

Ex. 172.217.11.78 (Google's IP Address)

OS makes DNS Lookup for IP

Def: Domain Name System (DNS) Lookup translates the domain name into an IP address your browser can use

Video: http://bit.ly/1jld0uV

Browser sends HTTP request

Def: The Hypertext Transfer Protocol (HTTP) is the foundation of data communication for the World Wide Web

Note: *OSI Model-related subjects, TCP and UDP are out of scope for this course.*

Browser reads response from server

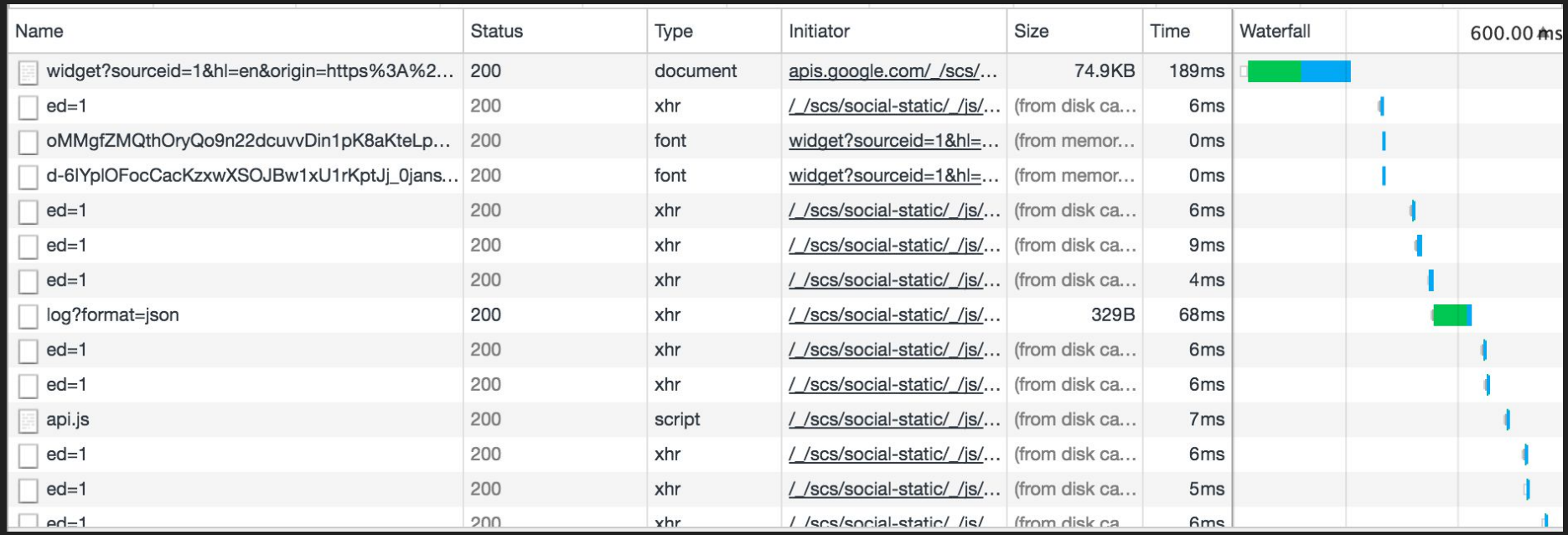
Def: Client/Server Model - A server host runs programs to share resource with clients. A client does not share resources, but requests a server's content or service function.

Browser reads response from server

Def: The server's Response to the client includes the status code, such as 404 Not Found, or 200 Successful.

List of HTTP Status Code: http://bit.ly/2ptqwnG

1 2 3 4 5 6 7

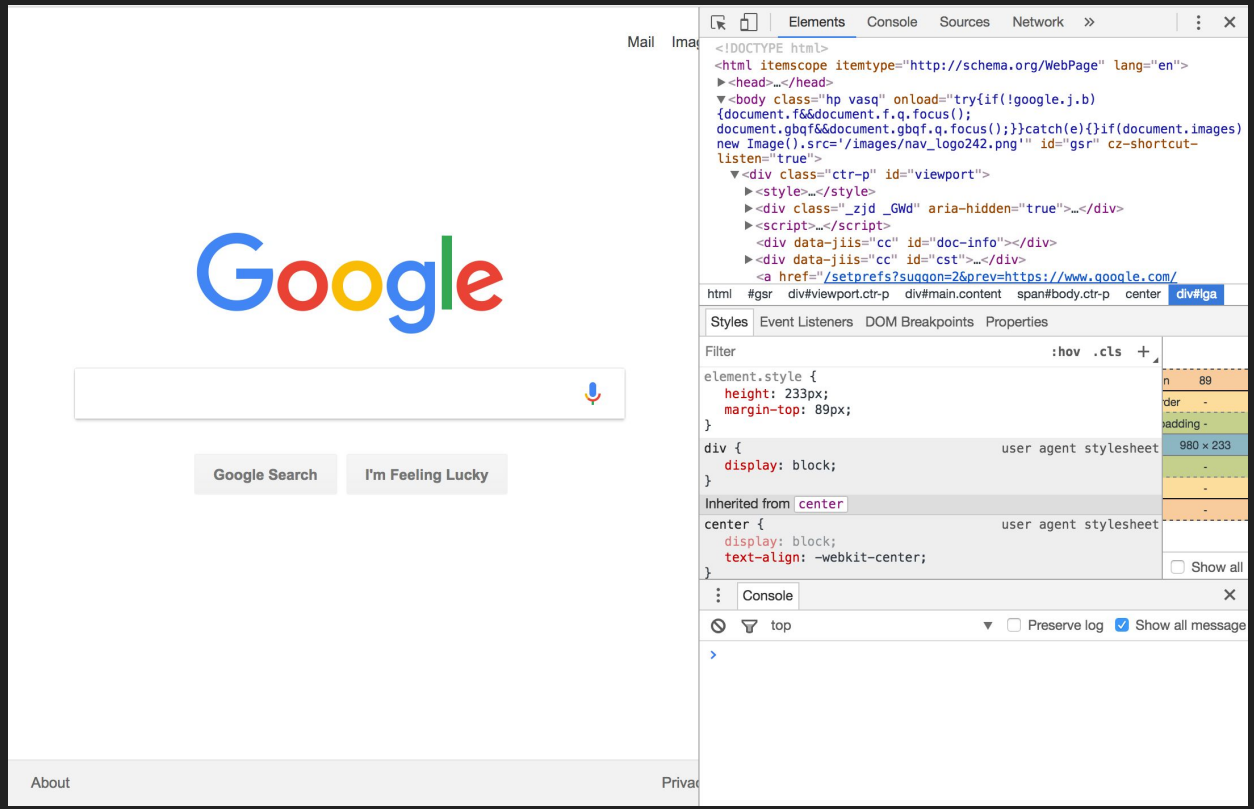


Name	Status	Type	Initiator	Size	Time	Waterfall 600.00 ms
widget?sourceid=1&hl=en&origin=https%3A%2…	200	document	apis.google.com/_/scs/…	74.9KB	189ms	
ed=1	200	xhr	/_/scs/social-static/_/js/…	(from disk ca…	6ms	
oMMgfZMQthOryQo9n22dcuvvDin1pK8aKteLp…	200	font	widget?sourceid=1&hl=…	(from memor…	0ms	
d-6lYplOFocCacKzxwXSOJBw1xU1rKptJj_0jans…	200	font	widget?sourceid=1&hl=…	(from memor…	0ms	
ed=1	200	xhr	/_/scs/social-static/_/js/…	(from disk ca…	6ms	
ed=1	200	xhr	/_/scs/social-static/_/js/…	(from disk ca…	9ms	
ed=1	200	xhr	/_/scs/social-static/_/js/…	(from disk ca…	4ms	
log?format=json	200	xhr	/_/scs/social-static/_/js/…	329B	68ms	
ed=1	200	xhr	/_/scs/social-static/_/js/…	(from disk ca…	6ms	
ed=1	200	xhr	/_/scs/social-static/_/js/…	(from disk ca…	6ms	
api.js	200	script	/_/scs/social-static/_/js/…	(from disk ca…	7ms	
ed=1	200	xhr	/_/scs/social-static/_/js/…	(from disk ca…	6ms	
ed=1	200	xhr	/_/scs/social-static/_/js/…	(from disk ca…	5ms	
ed=1	200	xhr	/_/scs/social-static/_/js/…	(from disk ca	6ms	

List of HTTP Status Code: http://bit.ly/2ptqwnG

Browser renders page to display

Def: The response from server contains HTML, CSS, Javascript, images, and all resources needed to render a webpage for the client.


Mail
Google
Google Search
I'm Feeling Lucky
About
Elements
Console
Sources
Network
<!DOCTYPE html>
<html itemscope itemtype="http://schema.org/WebPage" lang="en">
<head>…</head>
<body class="hp vasq" onload="try{if(!google.j.b)
{document.f&&document.f.q.focus();
document.gbqf&&document.gbqf.q.focus();}}catch(e){}if(document.images)
new Image().src='/images/nav_logo242.png'" id="gsr" cz-shortcut-
listen="true">

<style>…</style>
…
<script>…</script>

…
<a href="/setprefs?suggon=2&prev=https://www.google.com/
html #gsr div#viewport.ctr-p div#main.content span#body.ctr-p center div#lga
Styles
Event Listeners
DOM Breakpoints
Properties
Filter
:hov .cls
element.style {
height: 233px;
margin-top: 89px;
}
div { user agent stylesheet
display: block;
}
Inherited from center
center { user agent stylesheet
display: block;
text-align: -webkit-center;
}
980 × 233
Show all
Console
top
Preserve log
Show all message

Agenda

- *Review last week's material*
- *How the Internet Works, abridged*
- ***Cryptography/PGP***
- *How does a VPN Work?*
- *What is Proxy Browsing?*
- *Wireshark Demo*

Cryptography

Def: Constructing and analyzing protocols that prevent third parties or the public from reading **private messages**

Symmetric Key Cryptography

Def: Algorithms for cryptography that use the same cryptographic keys for both **encryption** of plaintext and **decryption** of ciphertext

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

The Key Exchange Problem

The Trust Problem


Scalability

Public Key Cryptography

Def: Cryptographic system that uses pairs of keys: **public keys** which may be disseminated widely, and **private keys** which are known only to the owner.

Public Key Cryptography

Authentication
Public key is used to verify that a holder of the paired private key sent the message

Encryption
whereby only the holder of the paired private key can decrypt the message encrypted with the public key

Symmetric Key

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

Public/Private Key

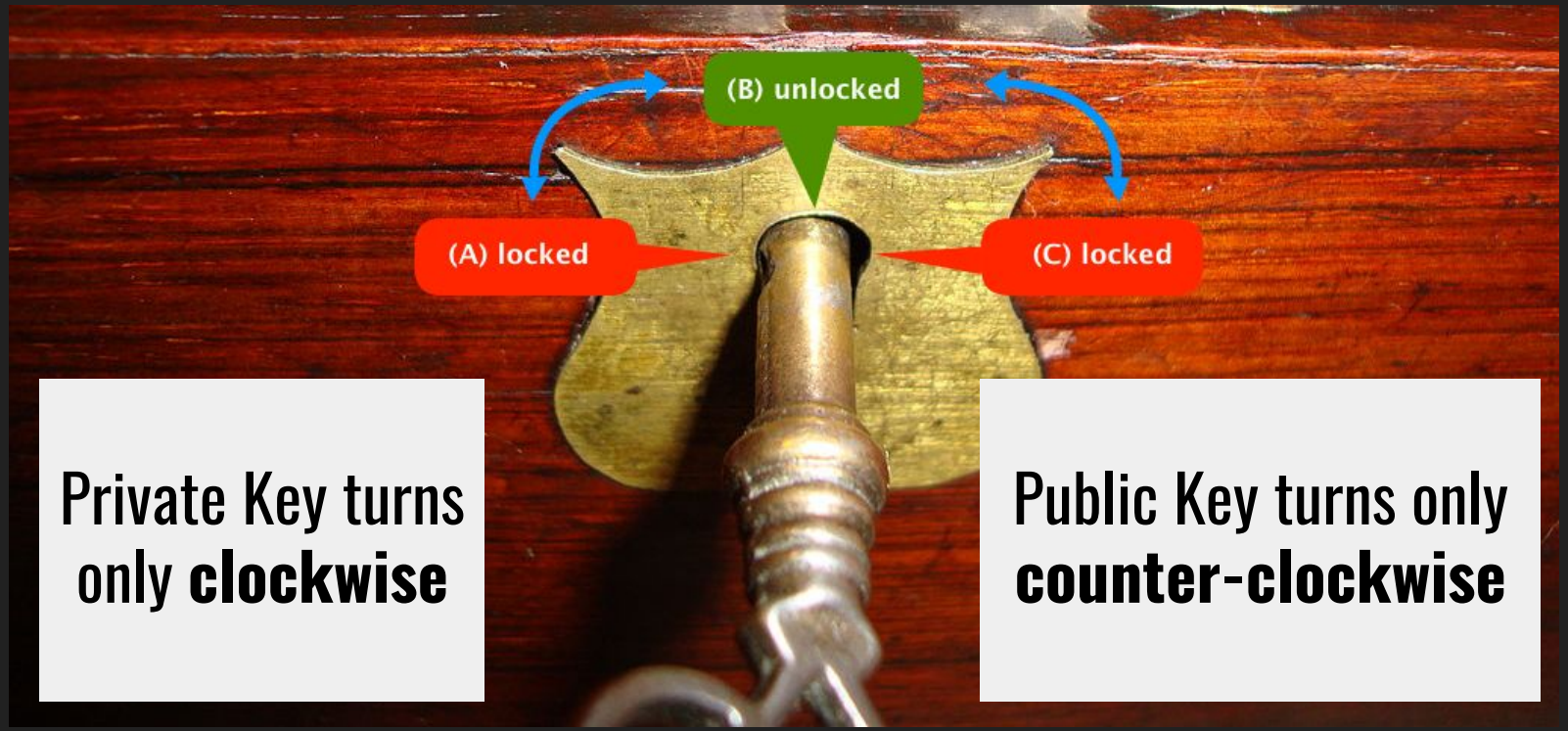


Image Source: http://bit.ly/1I2YUeS


How do you verify someone on the Internet?

Pretty Good Privacy (PGP)

Def: PGP is a program used for signing, encrypting, and decrypting texts, e-mails, files, directories, and whole disk partitions and to increase the security of e-mail communications

GnuPG is the free version of PGP

Source: `http://bit.ly/2pCWEp7`

Keybase

Demo

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

Agenda

- *Review last week's material*
- *How the Internet Works, abridged*
- *Cryptography/PGP*
- ***How does a VPN Work?***
- *What is Proxy Browsing?*
- *Wireshark Demo*

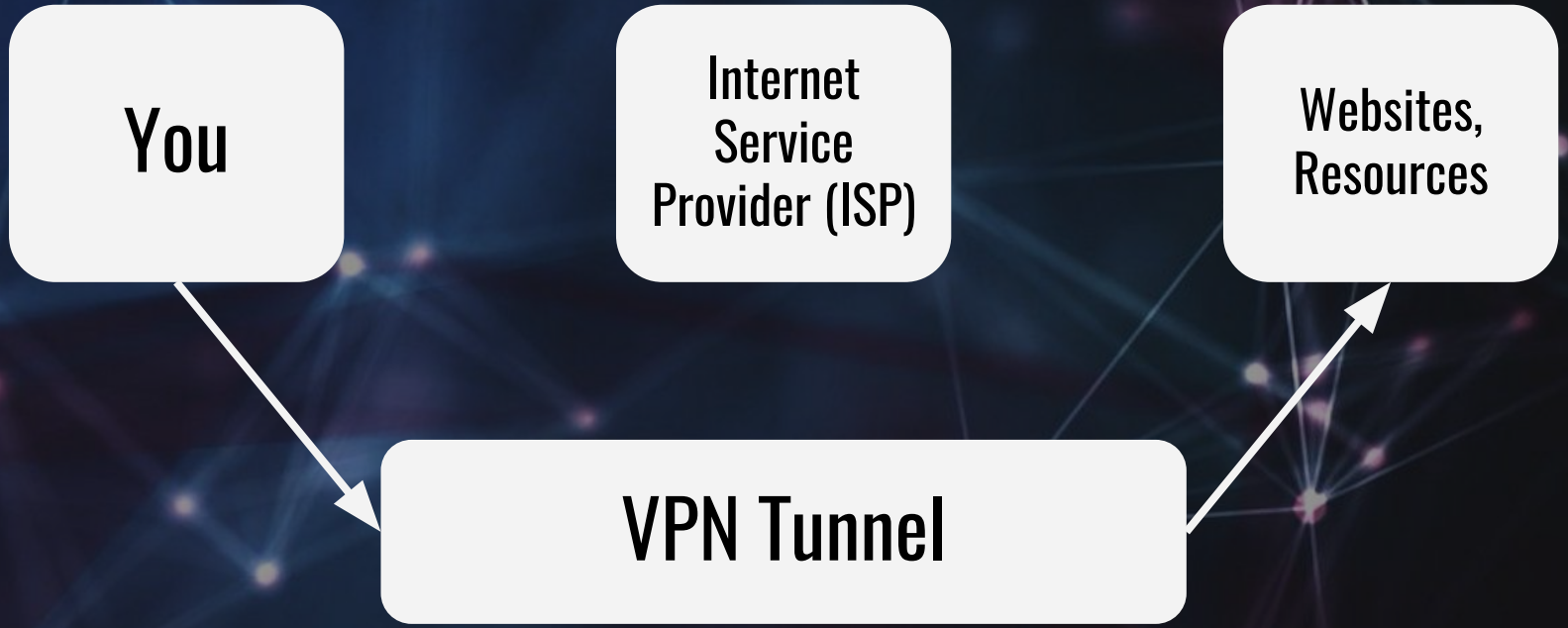
Virtual Private Network (VPN)

Def: VPNs allow users to securely access a private network and share data remotely through public networks.

Much like a firewall protects your data on your computer, VPNs protect it online.

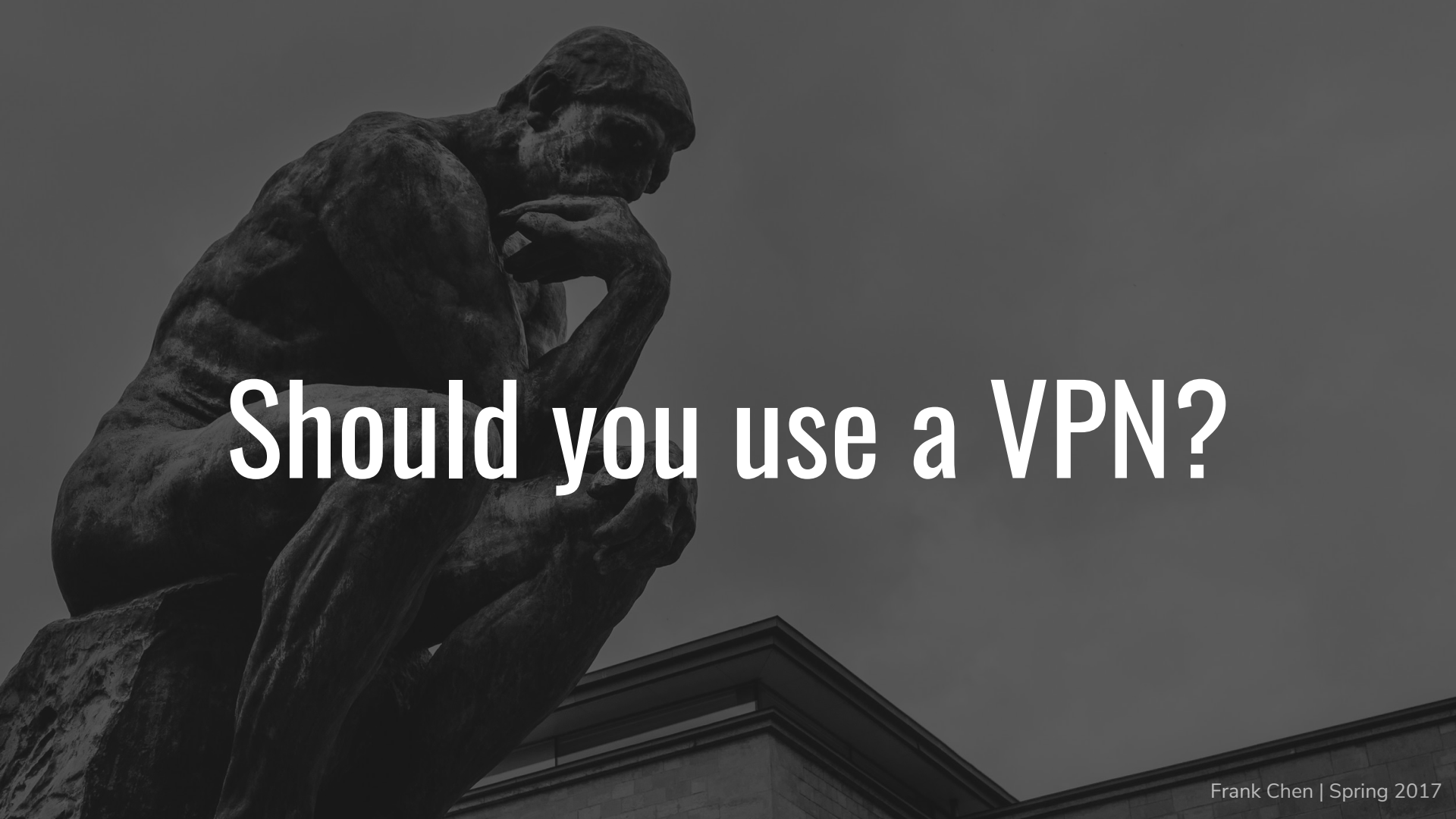
Virtual Private Network (VPN)

Virtual Private Network (VPN)



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

UCLA VPN Demo


Should you use a VPN?

Pro

- *ISPs cannot track you*
- *Good for protection in public Wi-Fi setting*
- *Network traffic always encrypted*

Con

- *Ads on free VPNs*
- *VPNs still log your activity*
- *Slow Internet Traffic*

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

Agenda

- *Review last week's material*
- *How the Internet Works, abridged*
- *Cryptography/PGP*
- *How does a VPN Work?*
- ***What is Proxy Browsing?***
- *Wireshark Demo*

Proxy Server

Def: A server set up as intermediary for the **client** and **server**

Using a Proxy can allow a user to spoof their IP address

Hide My Ass Demo

Source: https://www.hidemyass.com/proxy

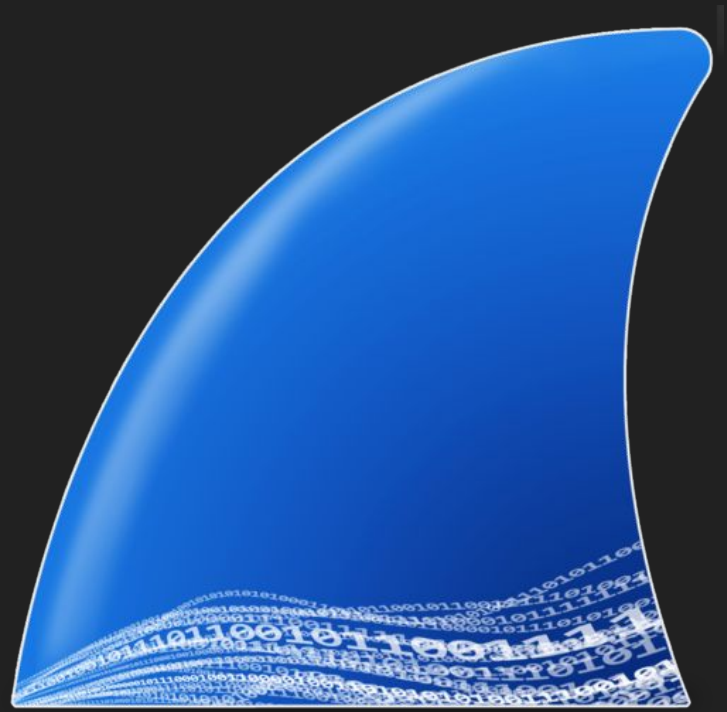
Difference between Proxy and VPN?

Source: http://bit.ly/2pS9liS

Agenda

- *Review last week's material*
- *How the Internet Works, abridged*
- *Cryptography/PGP*
- *How does a VPN Work?*
- *What is Proxy Browsing?*
- ***Wireshark Demo***

Wireshark



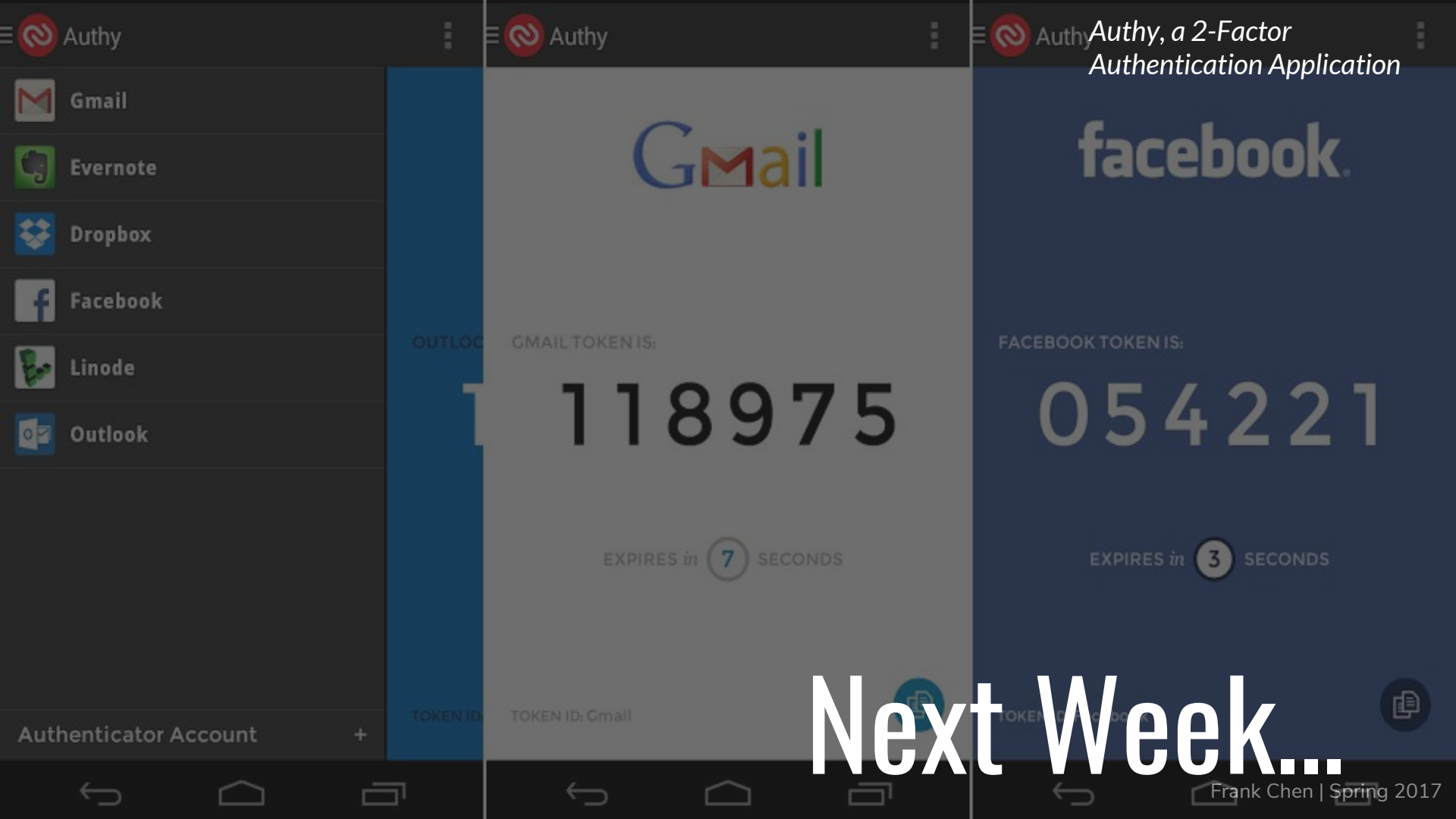
Safety in the Cloud Tip

Source:
http://bit.ly/2p5R4KX

Always use **HTTPS** or **VPN**

Source:
https://www.eff.org/https-everywhere

Authy, a 2-Factor Authentication Application



Next Week...