CS 88S

Password, Authentication, Password Managers

Week 4

Frank Chen | Spring 2017

Agenda

- *Review last week's material*
- *Some Definitions*
- *Password in the Cloud*
- *How Password Cracking Works*
- *Password Managers*

Demonstration

The power of
Google Analytics

Google Analytics

Agenda

- ***Review last week's material***
- *Some Definitions*
- *Password in the Cloud*
- *How Password Cracking Works*
- *Password Managers*

Phishing

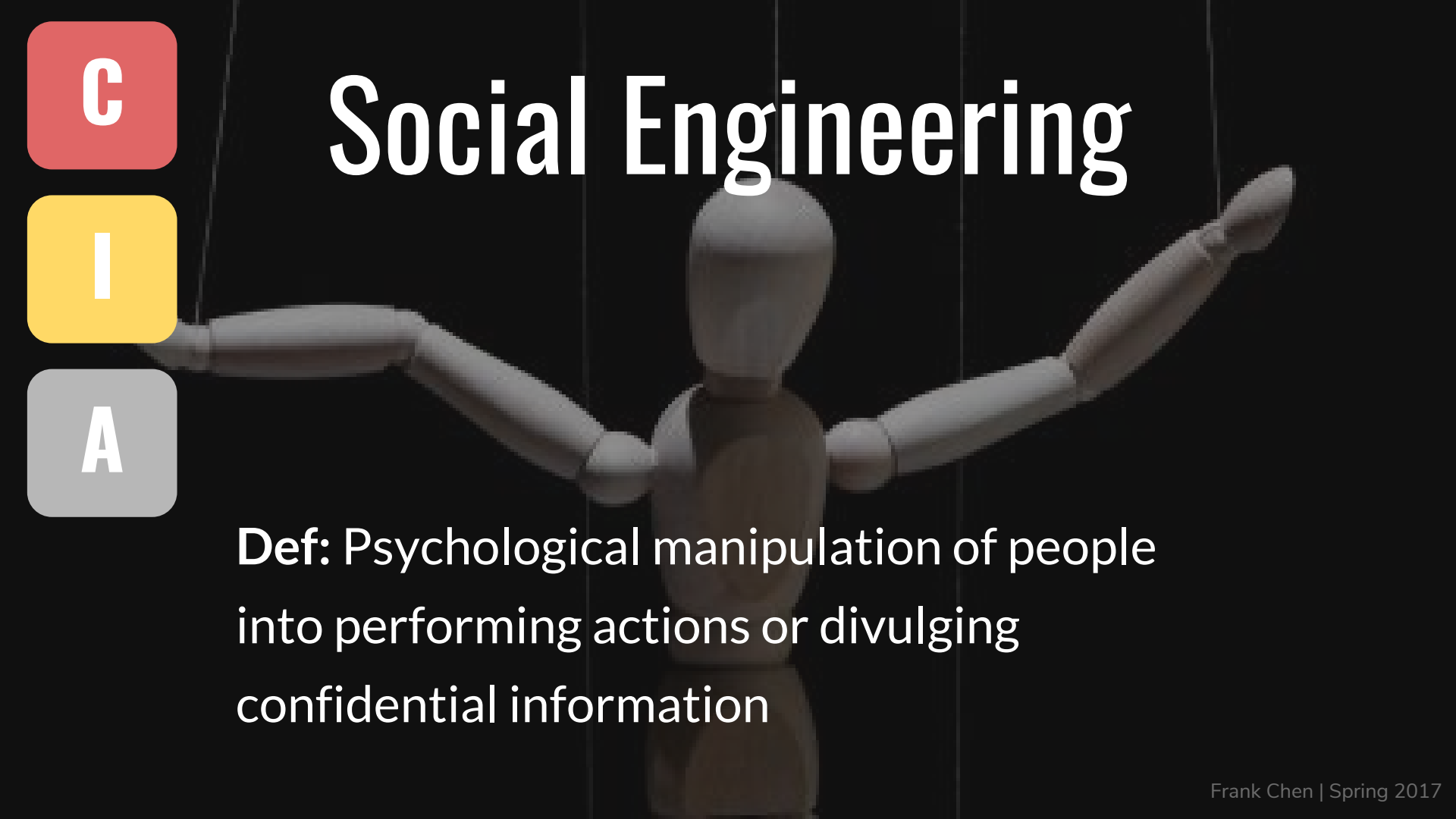
Def: The activity of **defrauding** an online account holder of financial information by posing as a **legitimate company**

C

I

A

Social Engineering



Def: Psychological manipulation of people into performing actions or divulging confidential information

Malwares

- *Adware*
- *Bot*
- *Ransomware*
- *Rootkit*
- *Spyware*
- *Trojan Horse*
- *Virus*
- *Worm*

Spam Email Classification

*Slide content credit to Prof. Ameet Talwalkar

Anti-Virus Software

Def: computer software used to **prevent, detect** and **remove** malicious software.

Agenda

- *Review last week's material*
- ***Some Definitions***
- *Password in the Cloud*
- *How Password Cracking Works*
- *Password Managers*

Password

Def: word or string of characters used to prove identity or gain access to a resource

Examples

OK Password:	Better Password:	Excellent Password:
kitty	1Kitty	**1Ki77y**
susan	Susan53	**.Susan53**
jellyfish	jelly22fish	**jelly22fi$h**
smellycat	sm3llycat	**$m3llycat**
allblacks	a11Blacks	**a11Black$**
usher	!usher	**!ush3r**

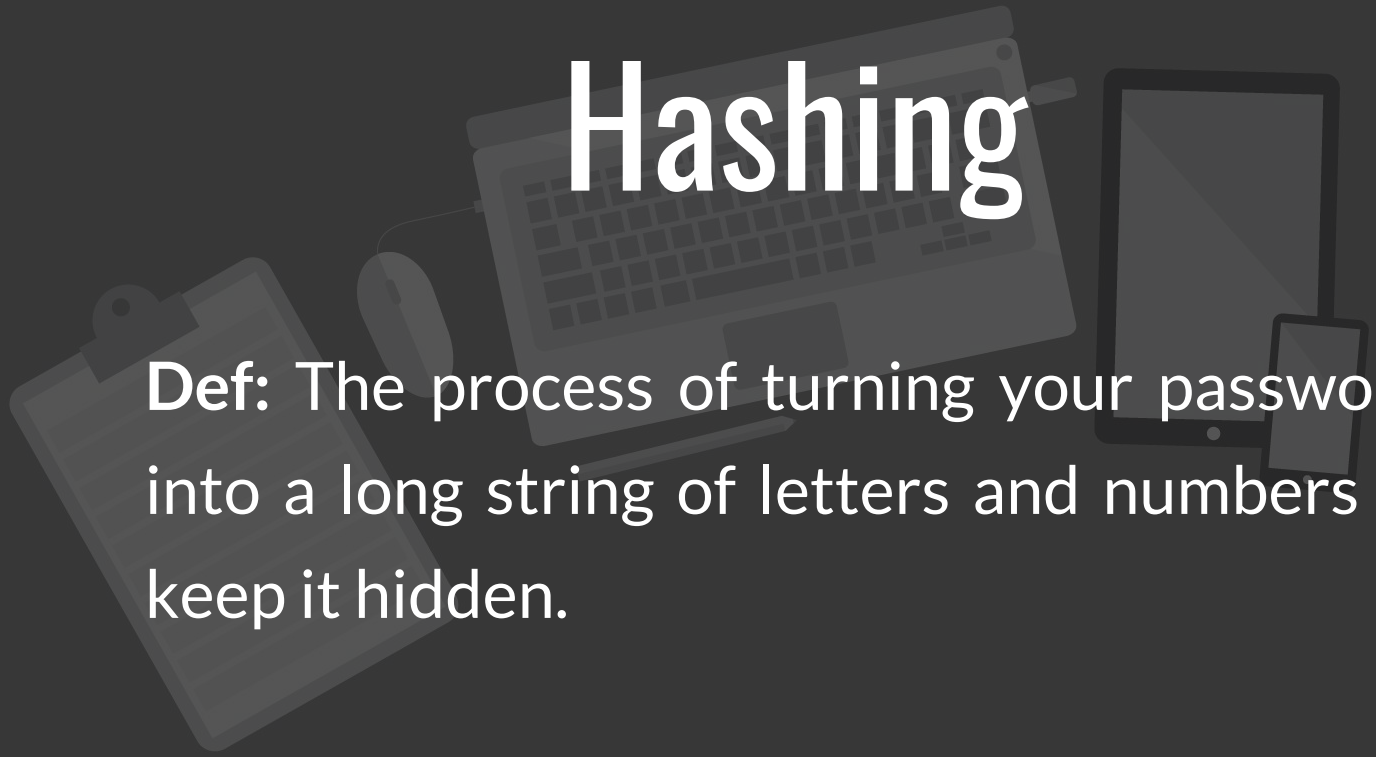
Source: http://bit.ly/2epzvkE

Plaintext

Def: Unencrypted text that is not computationally tagged, specially formatted, or written in code.

We don't want passwords to be stored in plaintext!

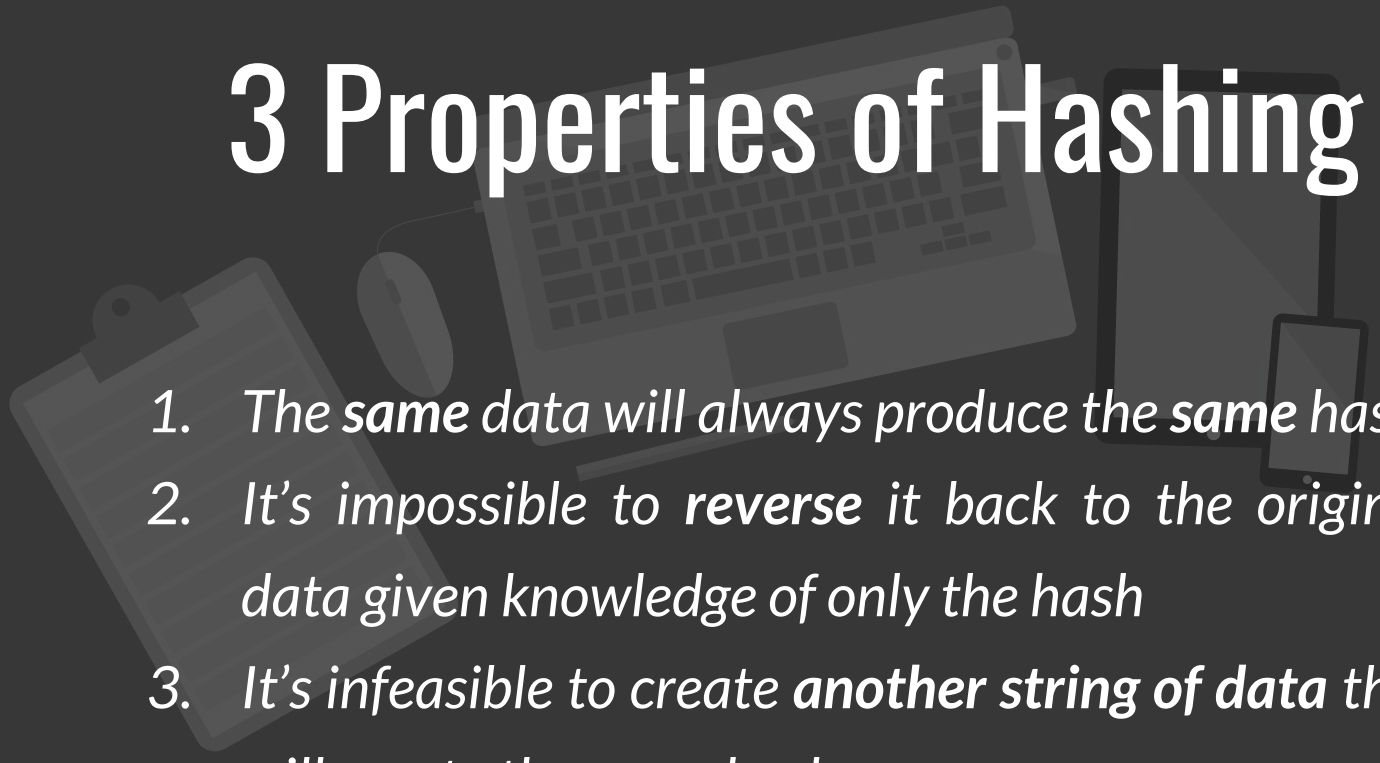
Hashing



Def: The process of turning your password into a long string of letters and numbers to keep it hidden.

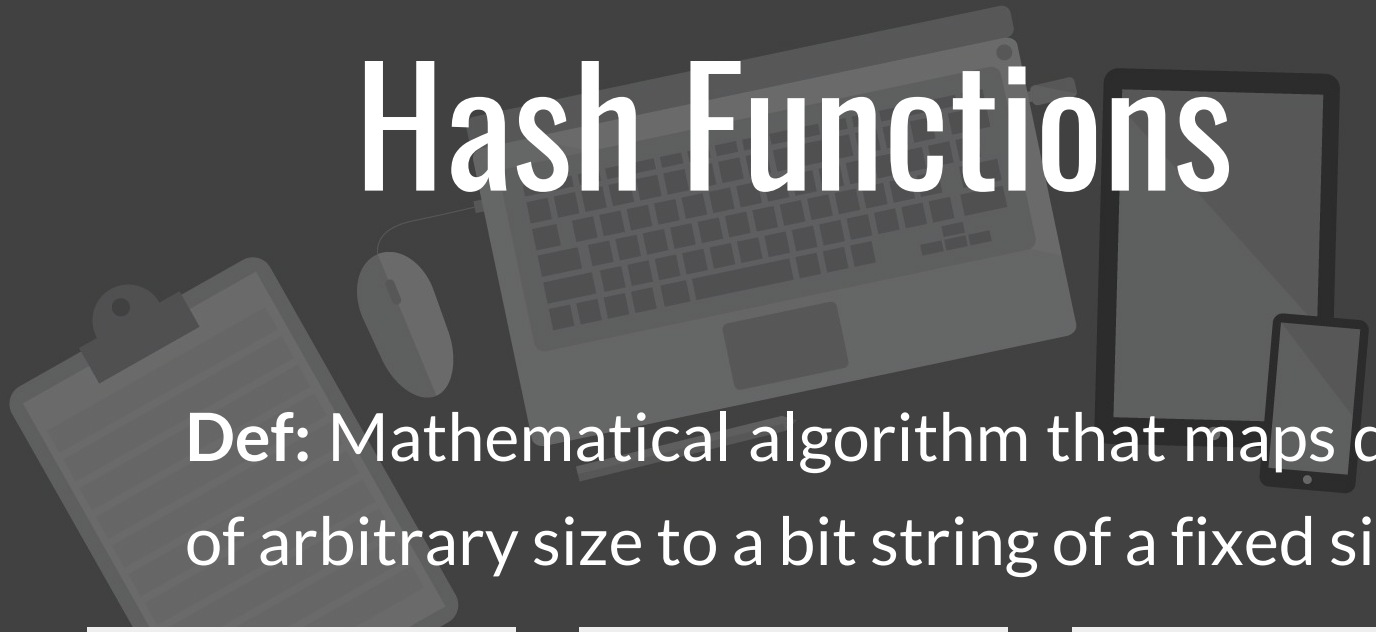
Hashing is a <u>one way street</u>.

3 Properties of Hashing



1. *The **same** data will always produce the **same** hash*
2. *It's impossible to **reverse** it back to the original data given knowledge of only the hash*
3. *It's infeasible to create **another string of data** that will create the same hash*

Hash Functions



Def: Mathematical algorithm that maps data of arbitrary size to a bit string of a fixed size.

MD5
http://bit.ly/2pbzecq

SHA-1
http://bit.ly/2przKUs

SHA-2
http://bit.ly/2q5dDzB

For a list of hash functions
http://bit.ly/2pbAADN

Example: MD5 Hash

MD5("The quick brown fox jumps over the lazy dog")
= 9e107d9d372bb6826bd81d3542a419d6

MD5("The quick brown fox jumps over the lazy dog.")
= e4d909c290d0fb1ca068ffaddf22cbd0

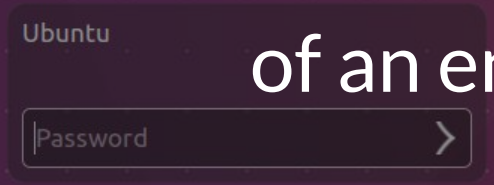
Source: `http://bit.ly/2pVq5pb`

Agenda

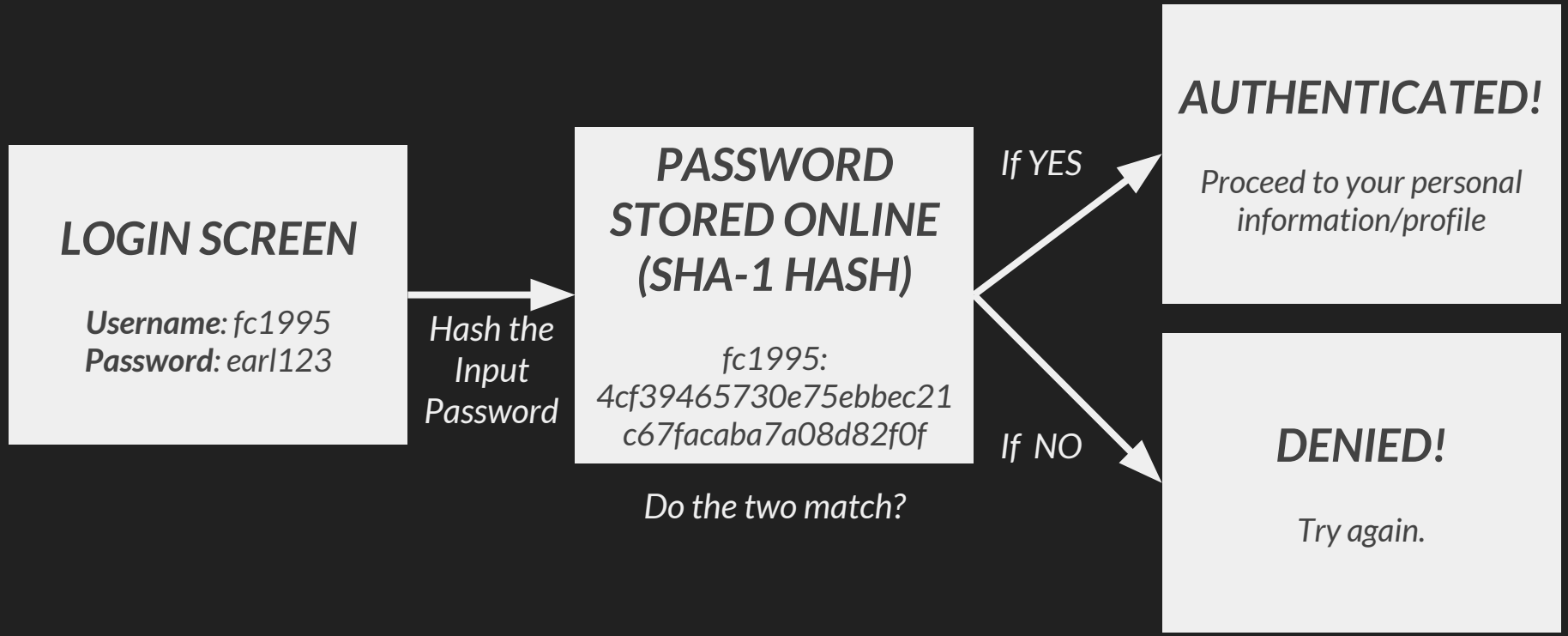
- *Review last week's material*
- *Some Definitions*
- ***Password in the Cloud***
- *How Password Cracking Works*
- *Password Managers*

Authentication

Def: The act of **confirming the truth** of an entered piece of data

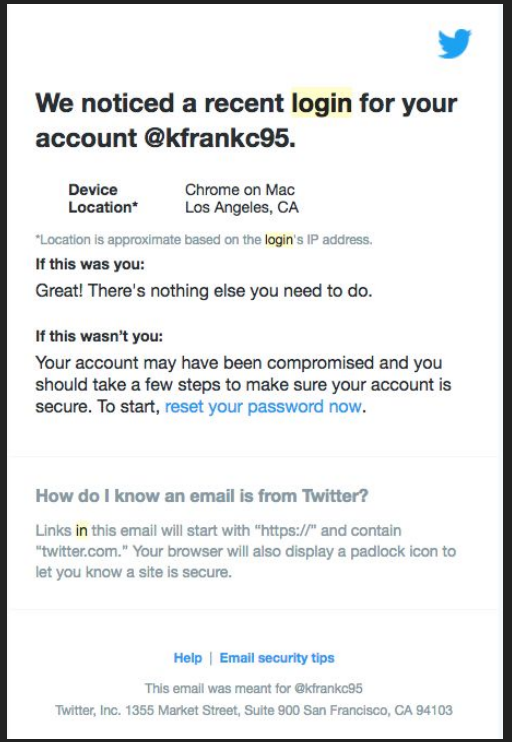


A typical Authentication Session



Additional Precautions

- *Timeout*
- *2 Factor Authentication*
- *Different Device Notifications*



We noticed a recent login for your account @kfrankc95.

Device	Chrome on Mac
Location*	Los Angeles, CA

*Location is approximate based on the login's IP address.

If this was you:

Great! There's nothing else you need to do.

If this wasn't you:

Your account may have been compromised and you should take a few steps to make sure your account is secure. To start, reset your password now.

How do I know an email is from Twitter?

Links in this email will start with "https://" and contain "twitter.com." Your browser will also display a padlock icon to let you know a site is secure.

Help | **Email security tips**

This email was meant for @kfrankc95

Twitter, Inc. 1355 Market Street, Suite 900 San Francisco, CA 94103

A lot of headlines...

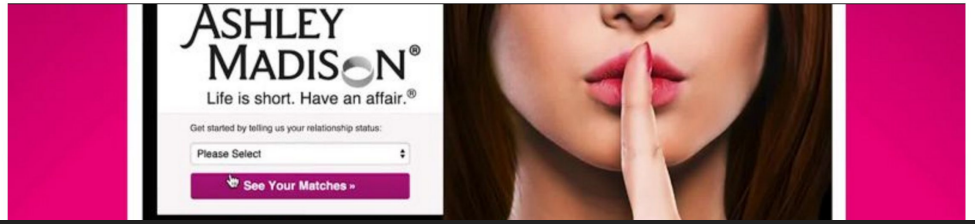
ANDY GREENBERG SECURITY 09.22.16 12:15 PM

HACK BRIEF: YAHOO BREACH HITS HALF A *BILLION* USERS

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

KIM ZETTER SECURITY 08.18.15 5:55 PM

HACKERS FINALLY POST STOLEN ASHLEY MADISON DATA



Source: http://bit.ly/1O1Md2G

Major Cloudflare bug leaked sensitive data from customers' websites

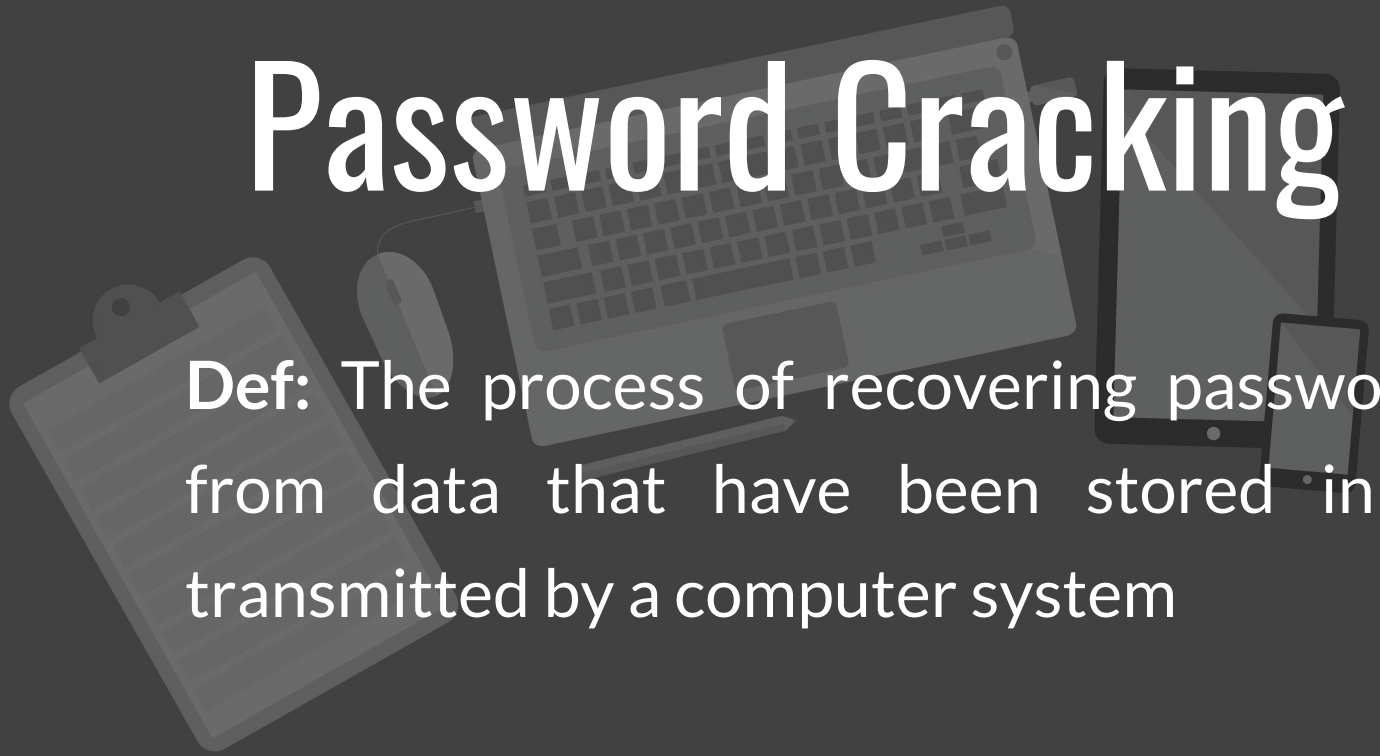
Posted Feb 23, 2017 by Kate Conger (@kateconger)

Source: http://tcrn.ch/2lLC3Pv

Agenda

- *Review last week's material*
- *Some Definitions*
- *Password in the Cloud*
- ***How Password Cracking Works***
- *Password Managers*

Password Cracking



Def: The process of recovering passwords from data that have been stored in or transmitted by a computer system

Examples (Revisited)

OK Password:	Better Password:	Excellent Password:
kitty	1Kitty	**1Ki77y**
susan	Susan53	**.Susan53**
jellyfish	jelly22fish	**jelly22fi$h**
smellycat	sm3llycat	**$m3llycat**
allblacks	a11Blacks	**a11Black$**
usher	!usher	**!ush3r**

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

What makes a Password Strong?

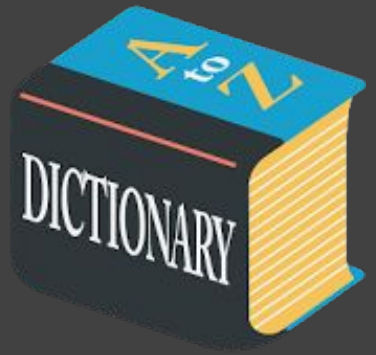
A STRONG password resists guessing.

The less that your password resembles regular English word patterns, the longer it will take for a repetition tool to guess it.

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

Dictionary Attack

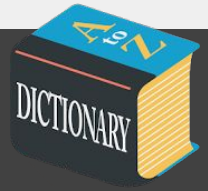
Def: an attempted illegal entry to a computer system that uses a dictionary list to generate possible passwords.



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!

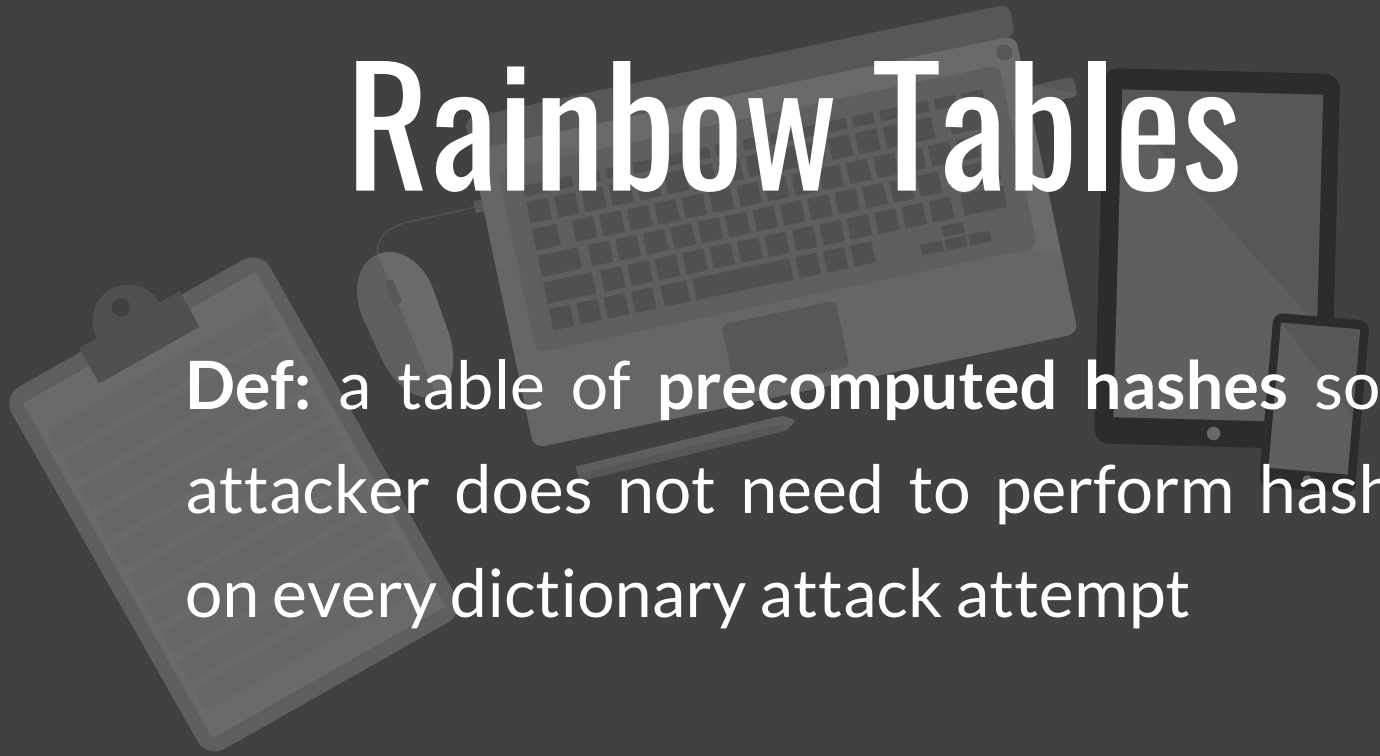
Dictionary Attacks can submit up to 1000 attempts per minute

John the Ripper

Password Cracker

Frank Chen | Spring 2017

Rainbow Tables

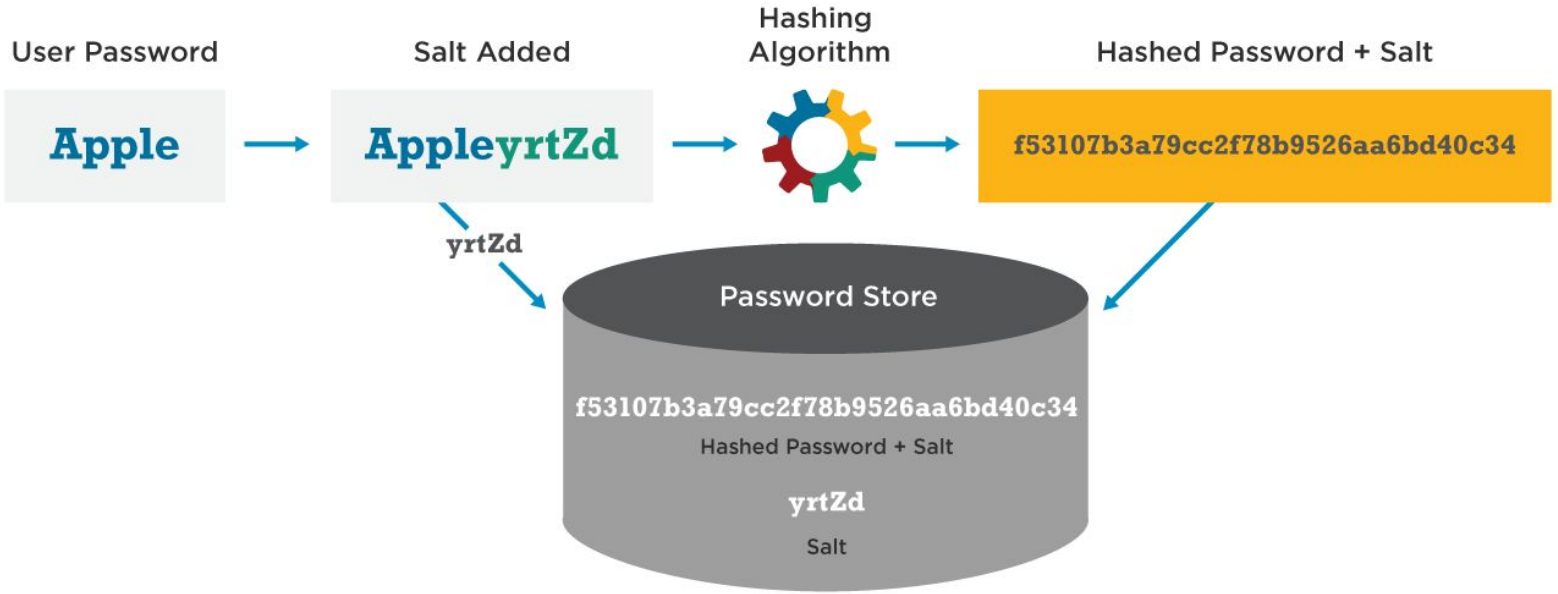


Def: a table of **precomputed hashes** so an attacker does not need to perform hashing on every dictionary attack attempt

Solution: Add Salt

Def: *salt* is random data that is used as an additional input to a one-way function that *hashes* a password or passphrase. Salt is added to the front of the password

Password Hash Salting



Wordfence™

wordfence.com/learn

Source: http://bit.ly/2p24ytZ

Case Study: eHarmony

eHarmony, Last.fm hit by same hackers that leaked LinkedIn passwords

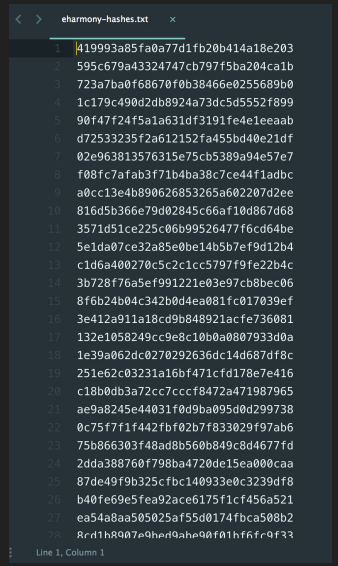
The breaches come as LinkedIn grapples with fall-out after 6.5 million of its passwords were posted online

eHarmony's homepage touts its trustworthiness, but its users' data has been compromised by hackers. Photograph: Screengrab

What does the leak mean?

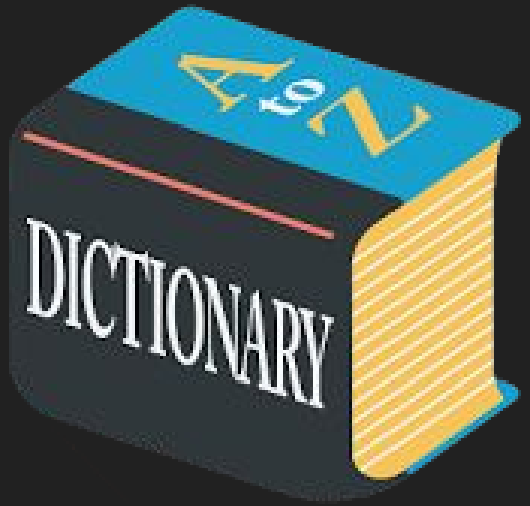
- *Most leaked files are **hashed***
- *Some are in **plaintext!?***
- *Others are hashed and **salted***

```
723a7ba0f68670f0b38466e0255689b0
1c179c490d2db8924a73dc5d5552f899
90f47f24f5a1a631df3191fe4e1eeaab
d72533235f2a612152fa455bd40e21df
02e963813576315e75cb5389a94e57e7
```



eHarmony password hash (md5 unsalted):
http://bit.ly/2nsJOZl

Dictionary Attack on CrackStation



1,493,677,782

medium dictionary entries

15,171,326,912

huge dictionary entries

Result of eHarmony Brute Force Attack

```
39007e310acd5cc5582c34c408ebf4cc :: RAWANN
c69f24b431852eb5b2db419860387dad :: SHELDURAY88
713f6fcbeeacbd3a78401382f88f5d1f :: KJ1017
86fc184cabcf0626c479927cc4e5e998 :: PUSSY310
c075be959b6831fb01d52591963d12b7 :: KARAAGE4
6c058fea843d5bff058c939fde3a6eb8 :: TH3EMPRESS
2dfecece2bf00698dd5fbae90e2f0860 :: ELLEGRA
e720578393bb68956f079c3db426d6ec :: 81PIRTER73
b0963f1a7fd94698a6e76e402daffcef :: KORRESHI
026d29ad37c6c672315e5a9c358d0a7c :: CLC47
7d01d8893e7ddbb18ceb40c59ef384c2 :: ROMELP
bf1a688689f82ba39b9efa236d09c539 :: OFTROY
dfcd9ad16c5358c1c420343a7b2b683b :: MVN2006
14f6609d95e3830b14709bce165041af :: MIKYONE
2b1841891df6de05b163d8dbbe79036c :: JAMFILE
9fe44d8eb7fbc5217fad2e54d09871ed :: TRIATA
961887ee6a084c02619f22f6b2e8a852 :: IAMTHATIS
fd9d9fa433c0d9385345355c17be13f4 :: PEACHKA1
fa22376fe0782fe9313385846e66b979 :: JAHAAD
095614e5971ad8a81d4f232c00bbf33d :: SARAHMIA1
f14c92dd1b2281cdf0f5999e595442de :: LEBIN
6e0f9ff4606b41705ea25bcbff1ac94b :: WINGK2
49cacc76a288058b68ded69f0c804269 :: CHARLIEXX
cbc7f37615111efe8e246d3316e24408 :: MB1229
81fc99cc34d28eec3c90109cab7ddfbe :: EMETI
e838f7db8ef56faa9b49e8215dfbbee7 :: KITABLAR
02ae65a2f3dac98a54290f09c39758ed :: JENGARY
3a7edcb86afee6b0853fba0a16672bcd :: GODSPELL2
22d541659b917e40146f4d4256b2a2e2 :: LETSTALK2
4e953e9a0a0f2503e8b8269b2c4a8057 :: 1MEMO1
```

275,860

(18.2%) of the passwords retrieved

23.47

Hours

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

How long would it take if the hashes were *salted* ?

```
39007e310acd5cc5582c34c408ebf4cc :: RAWANN
c69f24b431852eb5b2db419860387dad :: SHELDURAY88
713f6fcbeeacbd3a78401382f88f5d1f :: KJ1017
86fc184cabcf0626c479927cc4e5e998 :: PUSSY310
c075be959b6831fb01d52591963d12b7 :: KARAAGE4
6c058fea843d5bff058c939fde3a6eb8 :: TH3EMPRESS
2dfecece2bf00698dd5fbae90e2f0860 :: ELLEGRA
e720578393bb68956f079c3db426d6ec :: 81PIRTER73
b0963f1a7fd94698a6e76e402daffcef :: KORRESHI
026d29ad37c6c672315e5a9c358d0a7c :: CLC47
7d01d8893e7ddbb18ceb40c59ef384c2 :: ROMELP
bf1a688689f82ba39b9efa236d09c539 :: OFTROY
dfcd9ad16c5358c1c420343a7b2b683b :: MVN2006
14f6609d95e3830b14709bce165041af :: MIKYONE
2b1841891df6de05b163d8dbbe79036c :: JAMFILE
9fe44d8eb7fbc5217fad2e54d09871ed :: TRIATA
961887ee6a084c02619f22f6b2e8a852 :: IAMTHATIS
fd9d9fa433c0d9385345355c17be13f4 :: PEACHKA1
fa22376fe0782fe9313385846e66b979 :: JAHAAD
095614e5971ad8a81d4f232c00bbf33d :: SARAHMIA1
f14c92dd1b2281cdf0f5999e595442de :: LEBIN
6e0f9ff4606b41705ea25bcbff1ac94b :: WINGK2
49cacc76a288058b68ded69f0c804269 :: CHARLIEXX
cbc7f37615111efe8e246d3316e24408 :: MB1229
81fc99cc34d28eec3c90109cab7ddfbe :: EMETI
e838f7db8ef56faa9b49e8215dfbbee7 :: KITABLAR
02ae65a2f3dac98a54290f09c39758ed :: JENGARY
3a7edcb86afee6b0853fba0a16672bcd :: GODSPELL2
22d541659b917e40146f4d4256b2a2e2 :: LETSTALK2
4e953e9a0a0f2503e8b8269b2c4a8057 :: 1MEMO1
```

over **30** *years*

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

Let's look at some Math!

If we allow the typical upper/lower case letters and digits/symbols, that gives us a set of $(26\ letters + 10\ digits) * 2\ cases = 72\ characters$

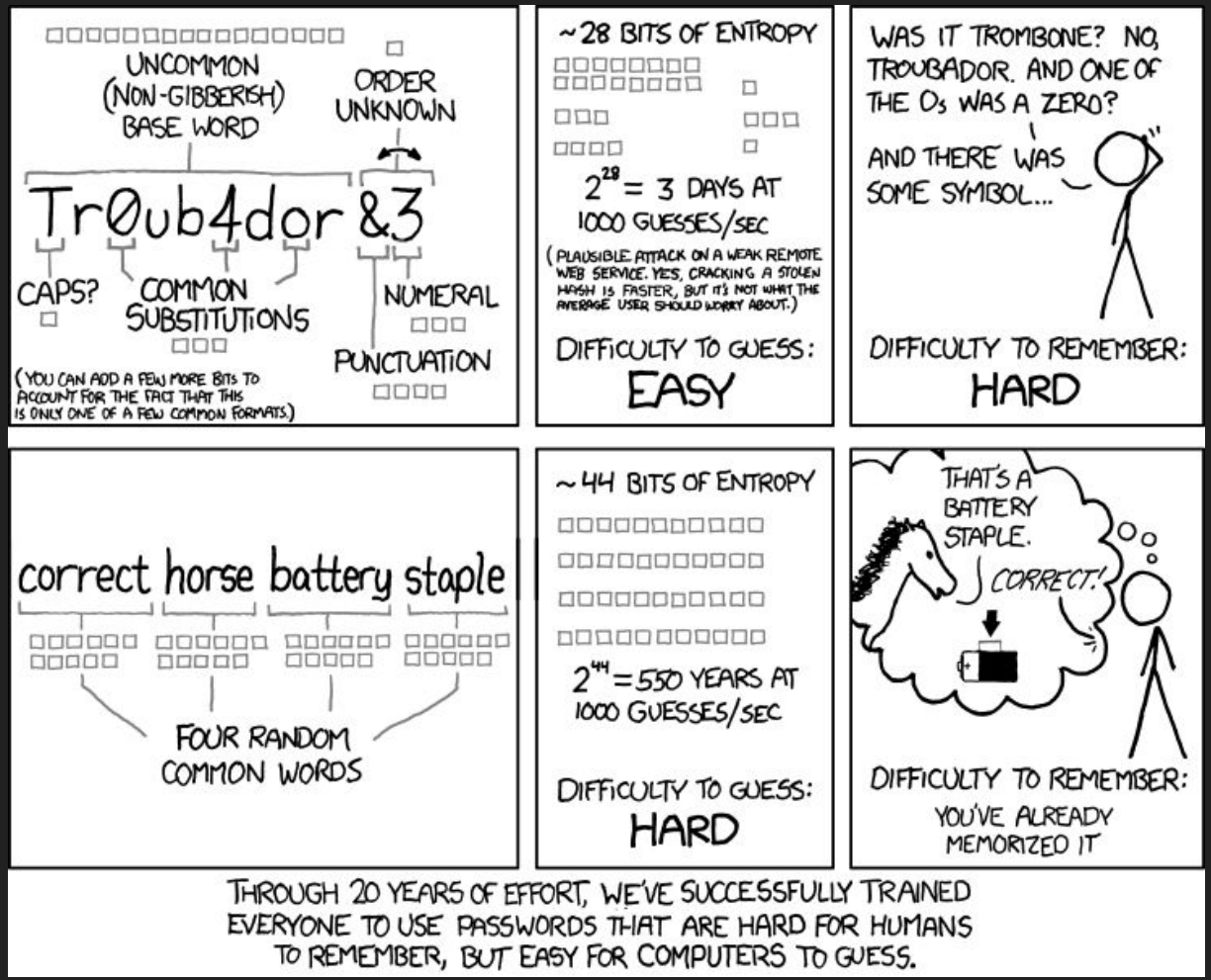
$72^{10} = 3,743,906,242,624,487,424$ potential passwords (~3.7 quadrillion). Fun fact: that's more than 34 million passwords for every person who has ever lived!

$$\frac{3,743,906,242,624,487,424\ hashes}{1\ password} \times \frac{1\ second}{115,840,000,000\ hashes} = \frac{32,319,632\ seconds}{1\ password}$$

$$\frac{32,319,632\ seconds}{1\ password} \times \frac{1\ hour}{3600\ seconds} = \frac{8,977.68\ hours}{1\ password}$$

$$\frac{8,977.68\ hours}{1\ password} \times \frac{1\ day}{24\ hours} = \frac{374\ days}{1\ password}$$

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



Source: http://bit.ly/1M88D3U

Tools

Source:
http://www.openwall.com/john/

Source:
https://www.aircrack-ng.org/

Source:
https://hashcat.net/hashcat/

Agenda

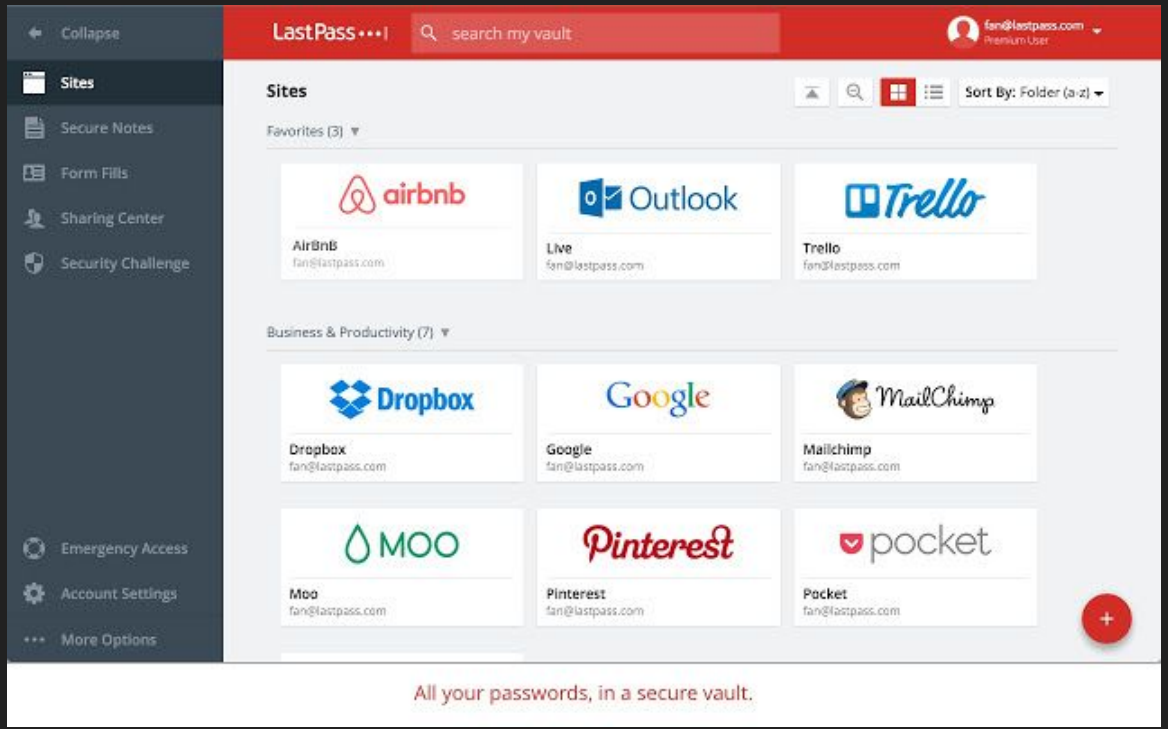
- *Review last week's material*
- *Some Definitions*
- *Password in the Cloud*
- *How Password Cracking Works*
- ***Password Managers***

Password Manager

Def: Software application or hardware that helps a user store and organize passwords.

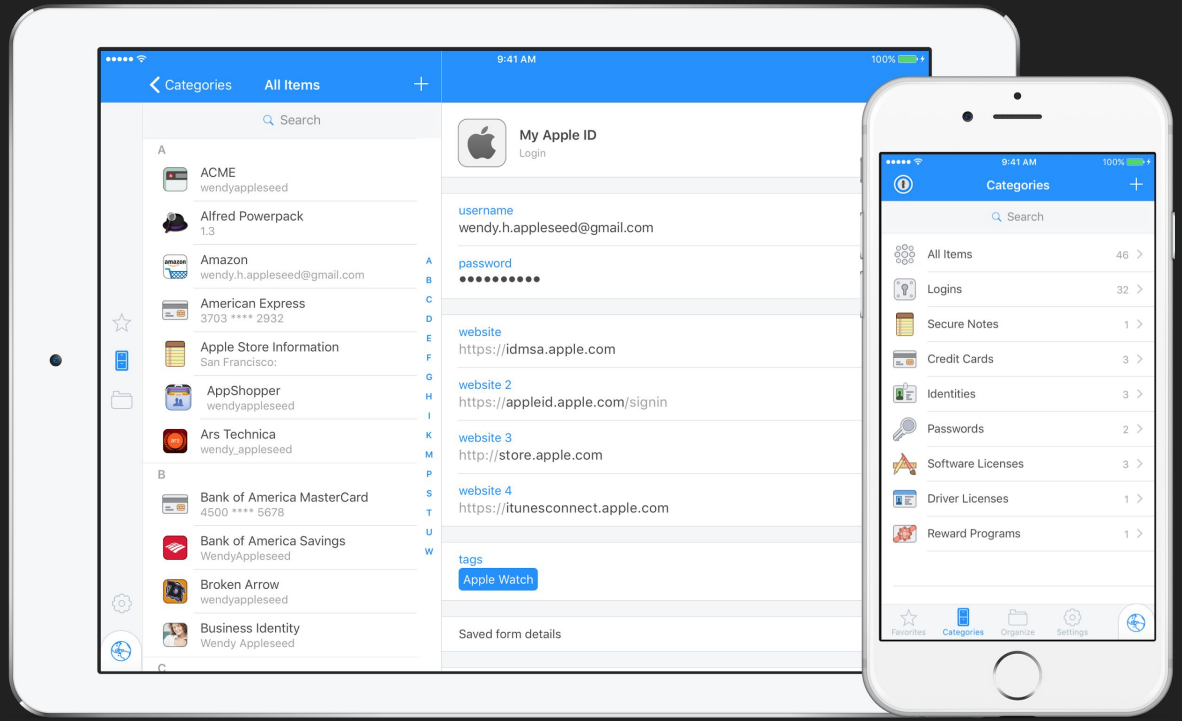
Password managers usually store passwords encrypted, requiring the user to create a **master password**

Lastpass



Password Managers can be hacked! http://bit.ly/2q38isq

1Password



Source: https://1password.com/

Should you use a Password Manager?

PROS

- *Balance of convenience and security*
- *Portability*
- *Secure Storage*
- *Not just for passwords*

CONS

- *Single point of failure*
- *Trusting in the Cloud*
- *Not necessary for some people*

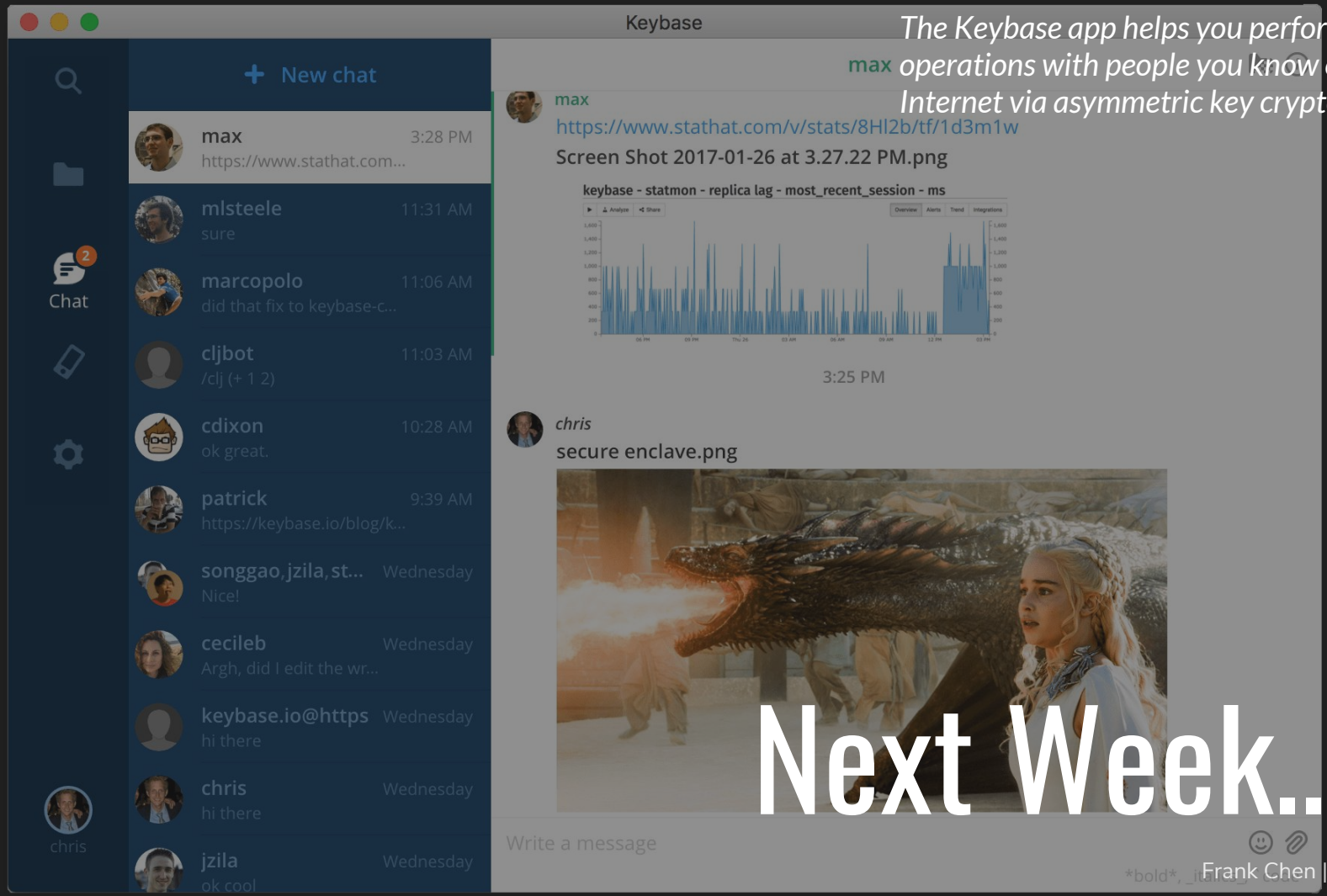
Source: http://bit.ly/2pZCcPc

Safety in the Cloud Tip

Manage your password well!

https://haveibeenpwned.com/

The Keybase app helps you perform secure operations with people you know on the Internet via asymmetric key cryptography



Next Week...