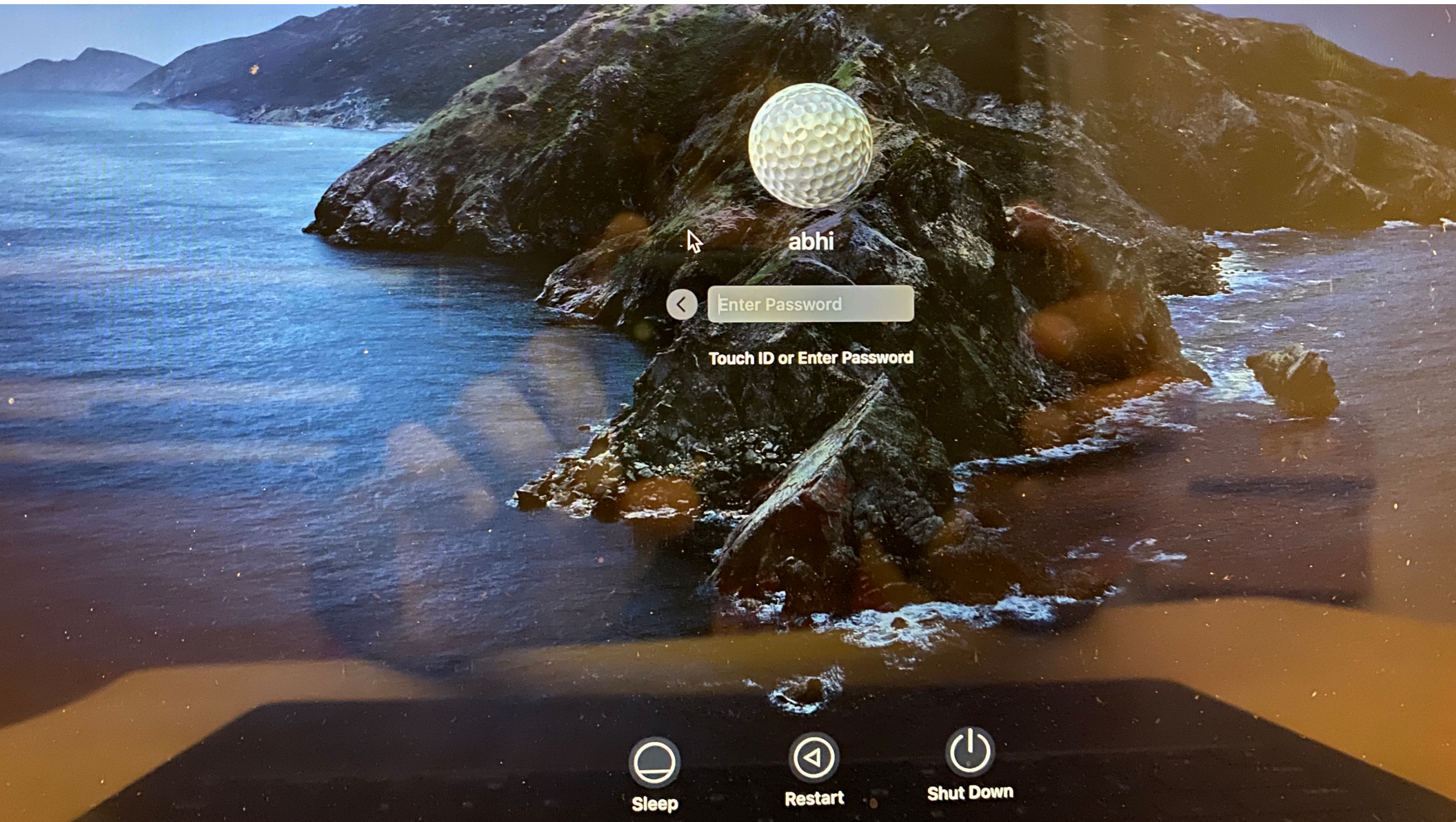


2550 Intro to cybersecurity L2

abhi shelat

What does it mean to attack a system?

What are our expectations?



abhi



Enter Password

Touch ID or Enter Password



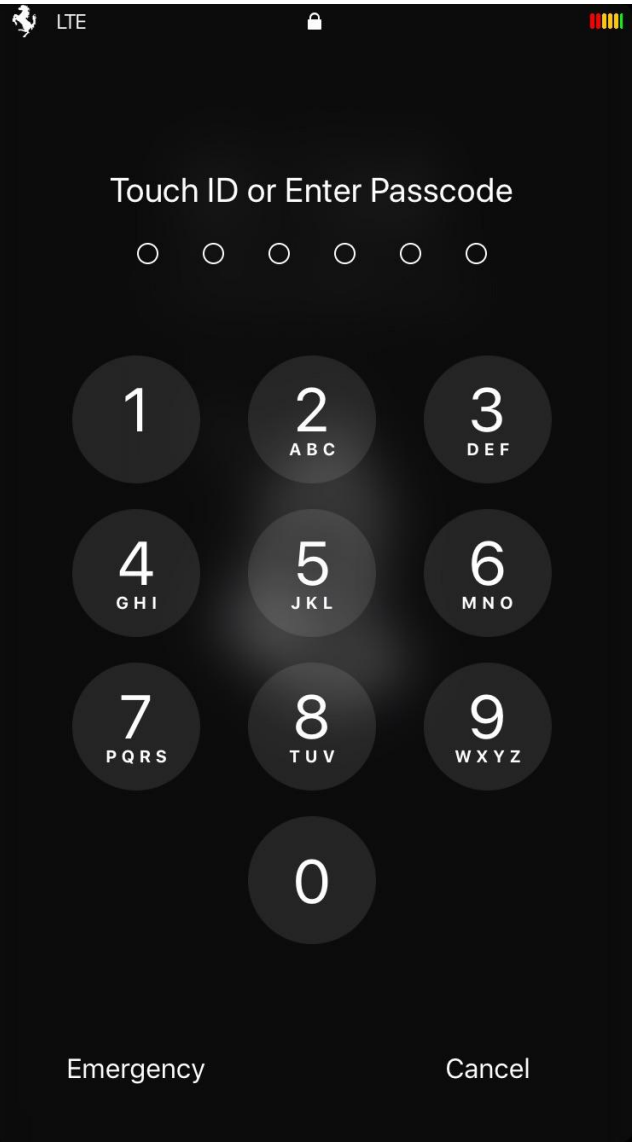
Sleep



Restart



Shut Down



Join "NUwave-guest"

 **Northeastern University**

Northeastern University Information Technology Services

Welcome to NUwave-guest

Log in to Northeastern's unsecured wireless network NUwave-guest using the username and password you received via text message.

Need to register? [Click here.](#)

One Day Conference Login [Click here.](#)

Have a myNEU login? You must log into NUwave - the secure wireless network.

NUwave-guest Login

Username:

Password:

< > clearpass-ri.nunet.neu.edu Cancel



Authentication

- **Authentication** is the process of verifying an actor's **identity**
- Critical for security of systems
 - Permissions, capabilities, and access control are all contingent upon knowing the identity of the actor
- Typically parameterized as a **username** and a **secret**
 - The secret attempts to limit unauthorized access
- Desirable properties of secrets include being *unforgeable*, *unguessable*, and *revocable*

Passwords

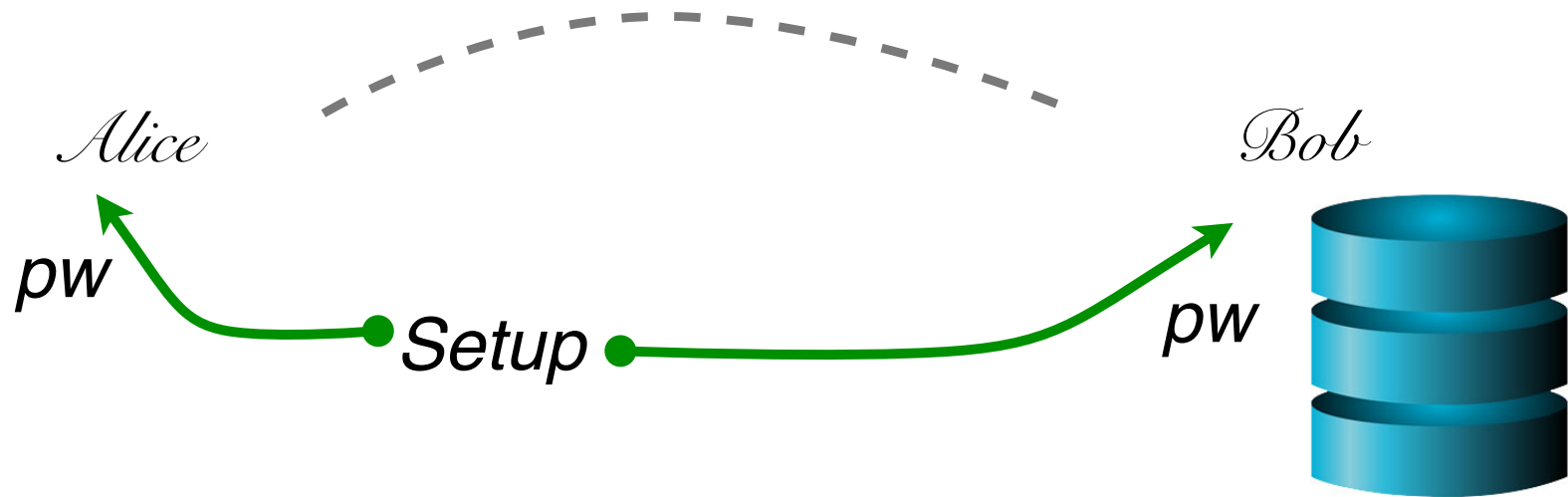
Main problem:

Alice



Bob

Passwords





Create your Google Account

First name

Last name

Username

@gmail.com

You can use letters, numbers & periods

[Use my current email address instead](#)

Password

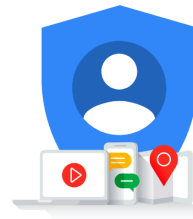
Confirm



Use 8 or more characters with a mix of letters, numbers & symbols

[Sign in instead](#)

Next

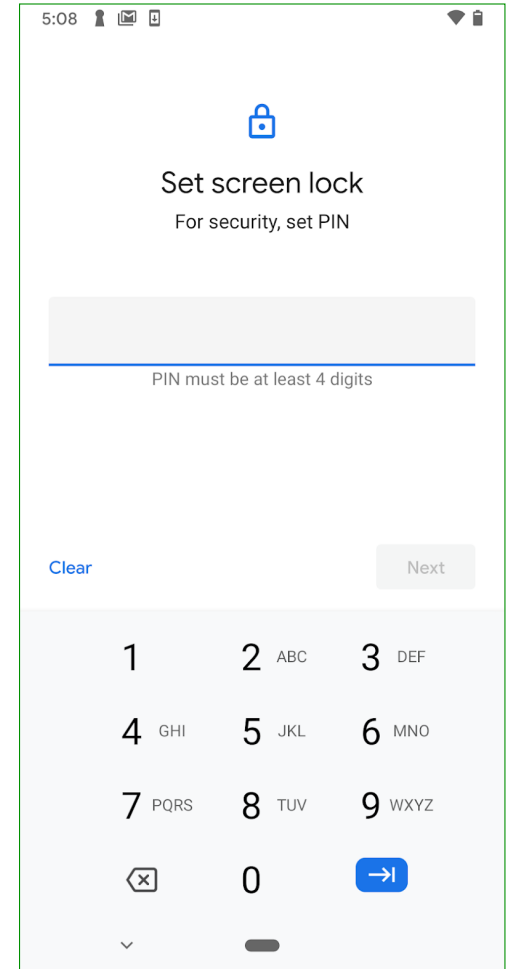
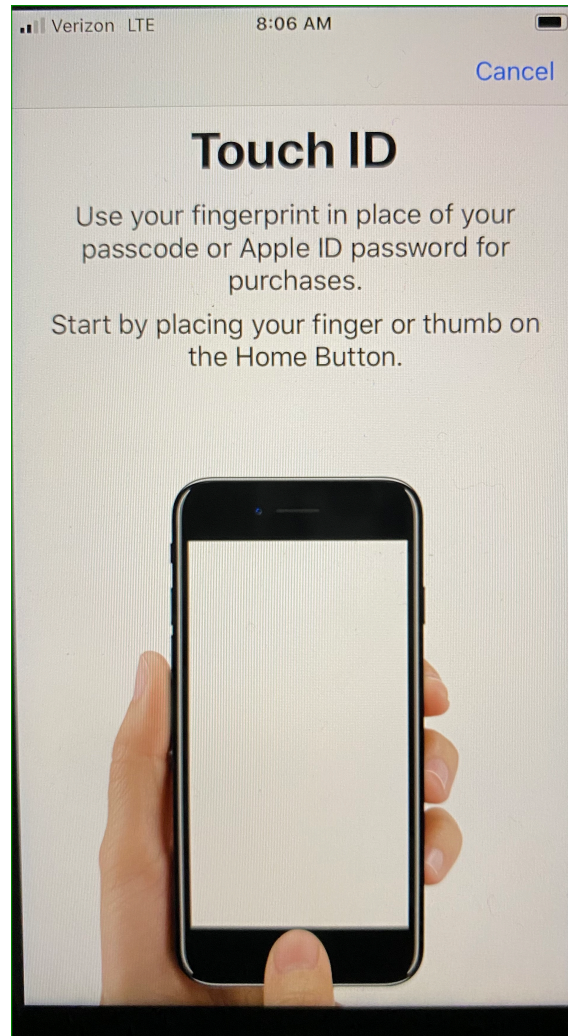
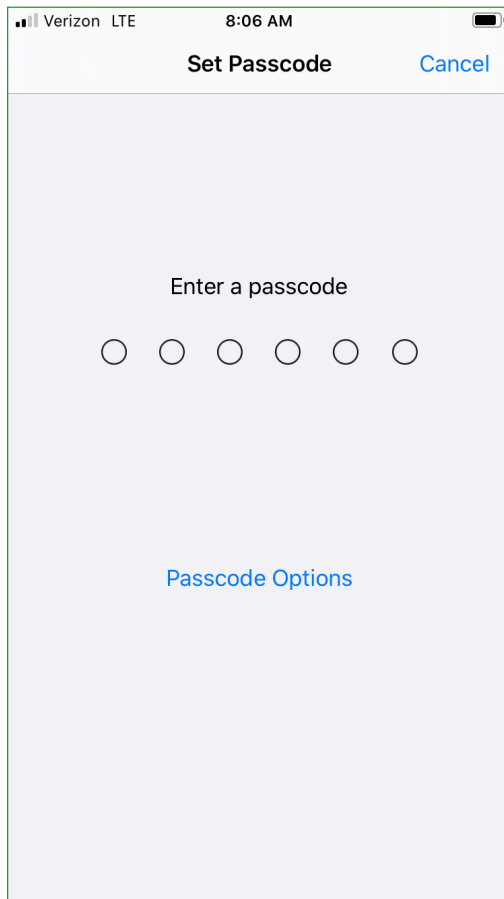


One account. All of Google working for you.

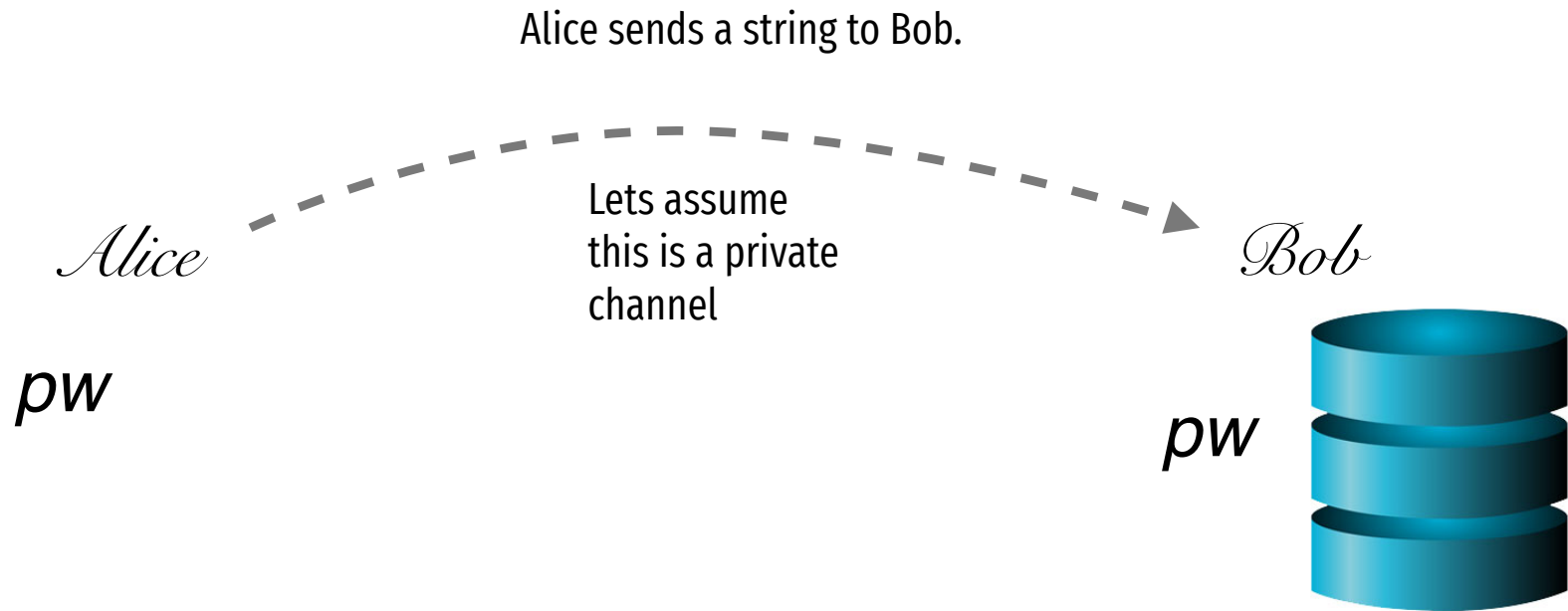
English (United States) ▼

[Help](#) [Privacy](#) [Terms](#)

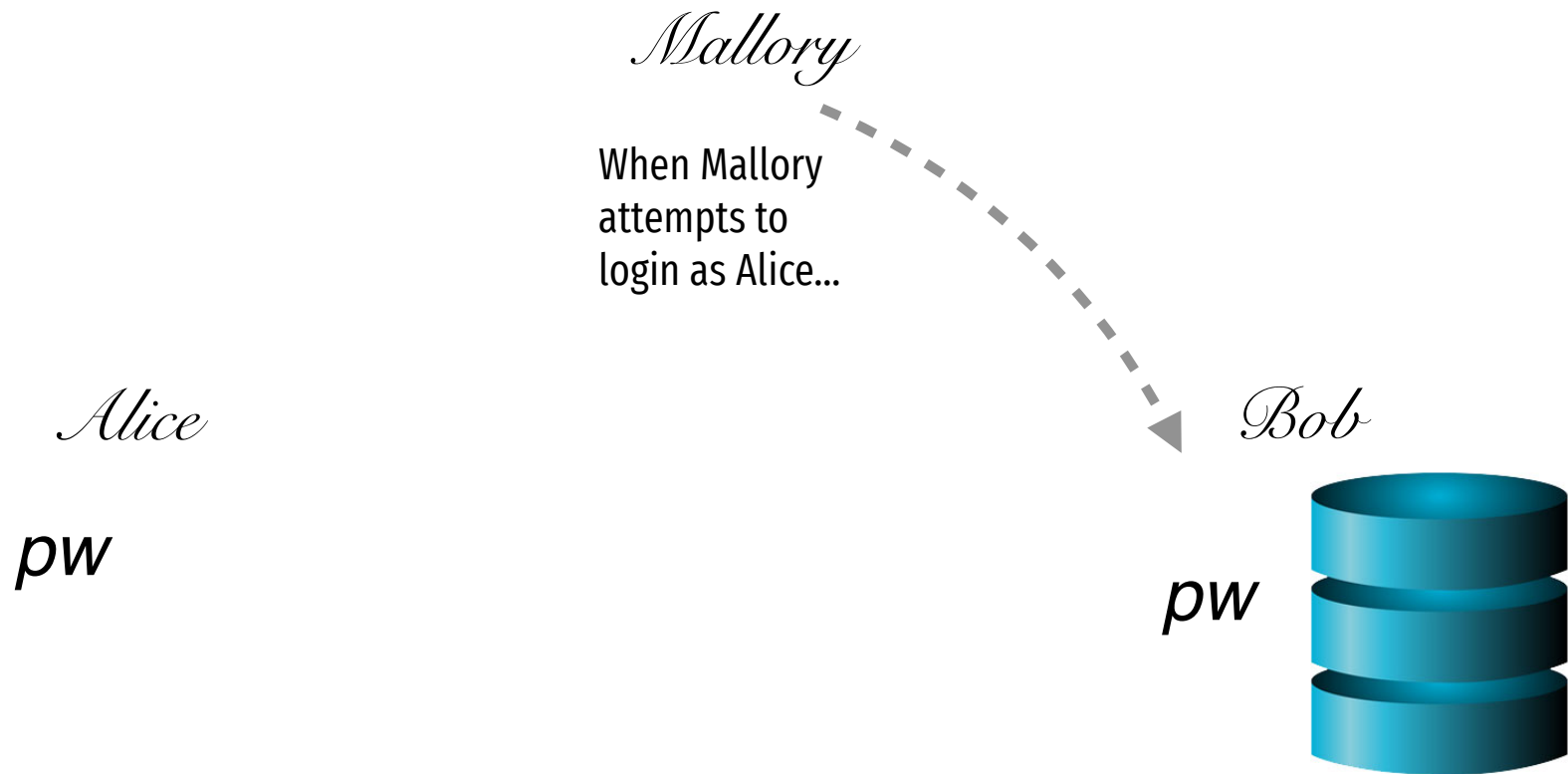
PIN setup



Passwords: Alice always succeeds



Passwords: Others do not succeed



Natural authenticators

First problem: How does Bob *check* Alice's password?



Checking Passwords

- System must validate passwords provided by users
- Thus, passwords must be *stored* somewhere
- Basic storage: plain text

password.txt	
Alice	p4ssw0rd
Eve	i heart doggies
Charlie	93Gd9#jv*0x3N
bob	security

Operating
Systems

R. Stockton Gaines
Editor

Password Security: A Case History

Robert Morris and Ken Thompson
Bell Laboratories

This paper describes the history of the design of the password security scheme on a remotely accessed time-sharing system. The present design was the result of countering observed attempts to penetrate the system. The result is a compromise between extreme security and ease of use.

Key Words and Phrases: operating systems, passwords, computer security

CR Categories: 2.41, 4.35

Communications
of
the ACM

November 1979
Volume 22
Number 11

"The UNIX system was first implemented with a password file **that contained the actual passwords of all the users, and for that reason the password file had to be heavily protected against being either read or written.** Although historically, this had been the technique used for remote-access systems, it was completely unsatisfactory for several reasons."

Attacks against the Password Model

Mallory

Bob



{username: pwd}

password.txt

Alice	p4ssw0rd
Eve	i heart doggies
Charlie	93Gd9#jv*0x3N
bob	security

Problem: Password File Theft

- Attackers often compromise systems
- They may be able to steal the password file
 - Linux: /etc/shadow
 - Windows: c:\windows\system32\config\sam
- If the passwords are plain text, what happens?
 - The attacker can now log-in as any user, including root/administrator
- **Passwords should never be stored in plain text**

RockYou Hack: From Bad To Worse



Nik Cubrilovic



@nikcub / 2:42 am EST • December 15, 2009

Comment



Earlier today news spread that social application site [RockYou](#) had suffered a data breached that

resulted in the exposure of over 32 Million user accounts. To compound the severity of the security breach, it was found that **RockYou**  are storing all user account data in plain text in their database, exposing all that information to attackers. RockYou have yet to inform users of the breach, and their blog is eerily silent – but the details of the security breach are going from bad to worse.

Data UserAccount [32603388]

=====

1|jennaplanerunner@hotmail.com|mek*****|myspace|0|bebo.com
2|phdlance@gmail.com|mek*****|myspace|1|
3|jennaplanerunner@gmail.com|mek*****|myspace|0|
5|teamsmackage@gmail.com|pro*****|myspace|1|
6|ayul@email.com|kha*****|myspace|1|tagged.com
7|guera_n_negro@yahoo.com|emi*****|myspace|0|
8|beyootifulgirl@aol.com|hol*****|myspace|1|
9|keh2oo8@yahoo.com|cai*****|myspace|1|
10|mawabiru@yahoo.com|pur*****|myspace|1|
11|jodygold@gmail.com|att*****|myspace|1|
12|aryan_dedboy@yahoo.com|iri*****|myspace|0|
13|moe_joe_25@yahoo.com|725*****|myspace|1|
14|xxxnothingbutme@aol.com|1th*****|myspace|0|
15|meandcj069@yahoo.com|too*****|myspace|0|
16|stacey_chim@hotmail.com|cxn*****|myspace|1|
17|barne1en@cmich.edu|ilo*****|myspace|1|
18|reo154@hotmail.com|ecu*****|myspace|1|
19|natapappaslie@yahoo.com|tor*****|myspace|0|
20|ypiogirl@aol.com|tob*****|myspace|1|
21|brittanyleigh864@hotmail.com|bet*****|myspace|1|myspace.com
22|topenga68@aol.com|che*****|myspace|0|
23|marie603412@yahoo.com|cat*****|myspace|0|
24|mellowchick41@aol.com|chu*****|myspace|0|



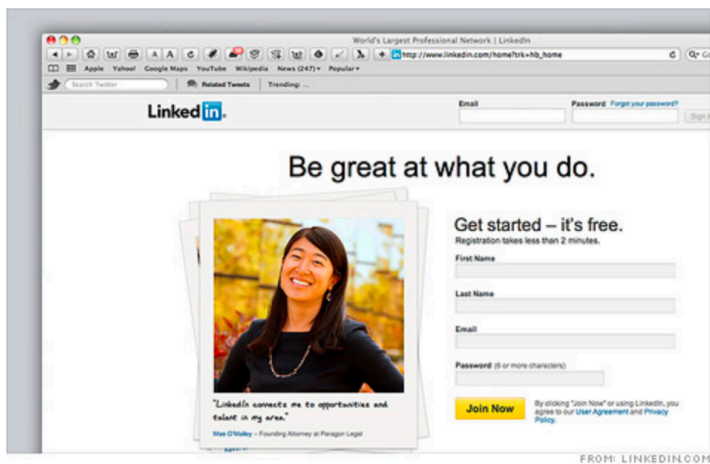
Pwd breaches



THE CYBERCRIME ECONOMY

More than 6 million LinkedIn passwords stolen

By David Goldman @CNNMoneyTech June 7, 2012: 9:34 AM ET



Researchers say a stash of what appear to be LinkedIn passwords were protected by a weak security scheme.

NEW YORK (CNNMoney) -- Russian hackers released a giant list of passwords this week, and on Wednesday security researchers identified their likely source: business social networking site LinkedIn.

Operating
Systems

R. Stockton Gaines
Editor

Password Security: A Case History

Robert Morris and Ken Thompson
Bell Laboratories

This paper describes the history of the design of the password security scheme on a remotely accessed time-sharing system. The present design was the result of countering observed attempts to penetrate the system. The result is a compromise between extreme security and ease of use.

Key Words and Phrases: operating systems, passwords, computer security

CR Categories: 2.41, 4.35

Communications
of
the ACM

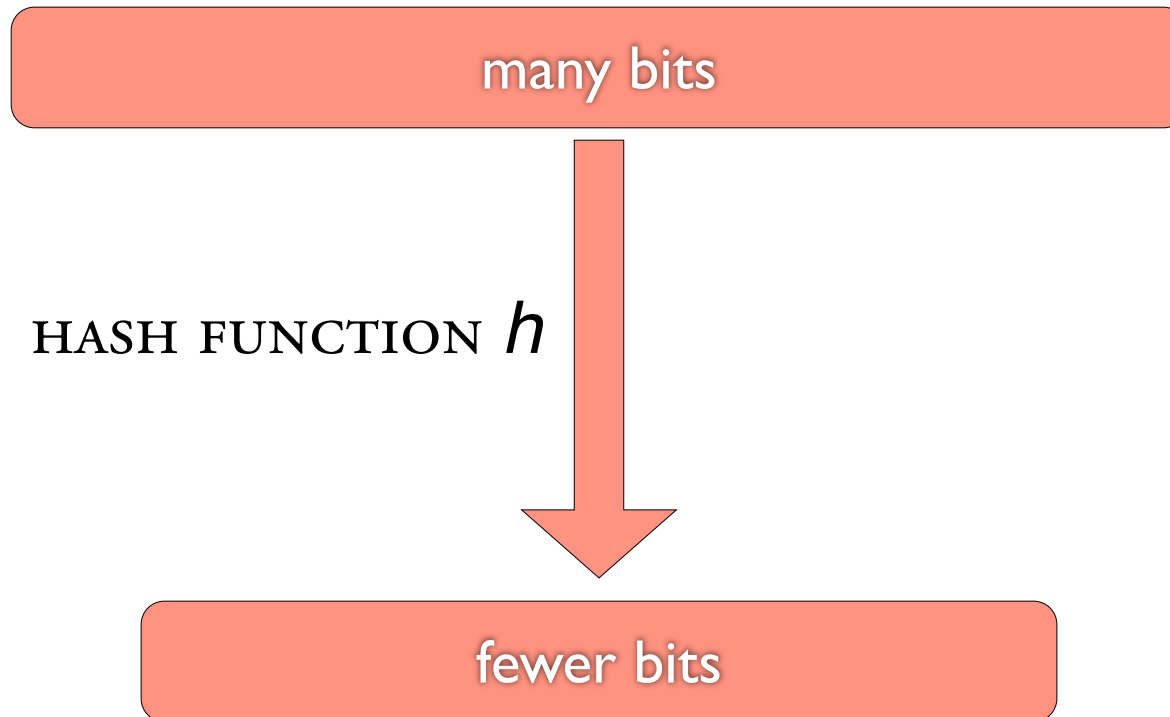
November 1979
Volume 22
Number 11

“The obvious solution is to arrange that the passwords not appear in the system at all, and it is not difficult to decide that this can be done by encrypting each user's password, putting only the encrypted form in the password file, and throwing away his original password (the one that he typed in). When the user later tries to log in to the system, the password that he types is encrypted and compared with the encrypted version in the password file. If the two match, his login attempt is accepted.”

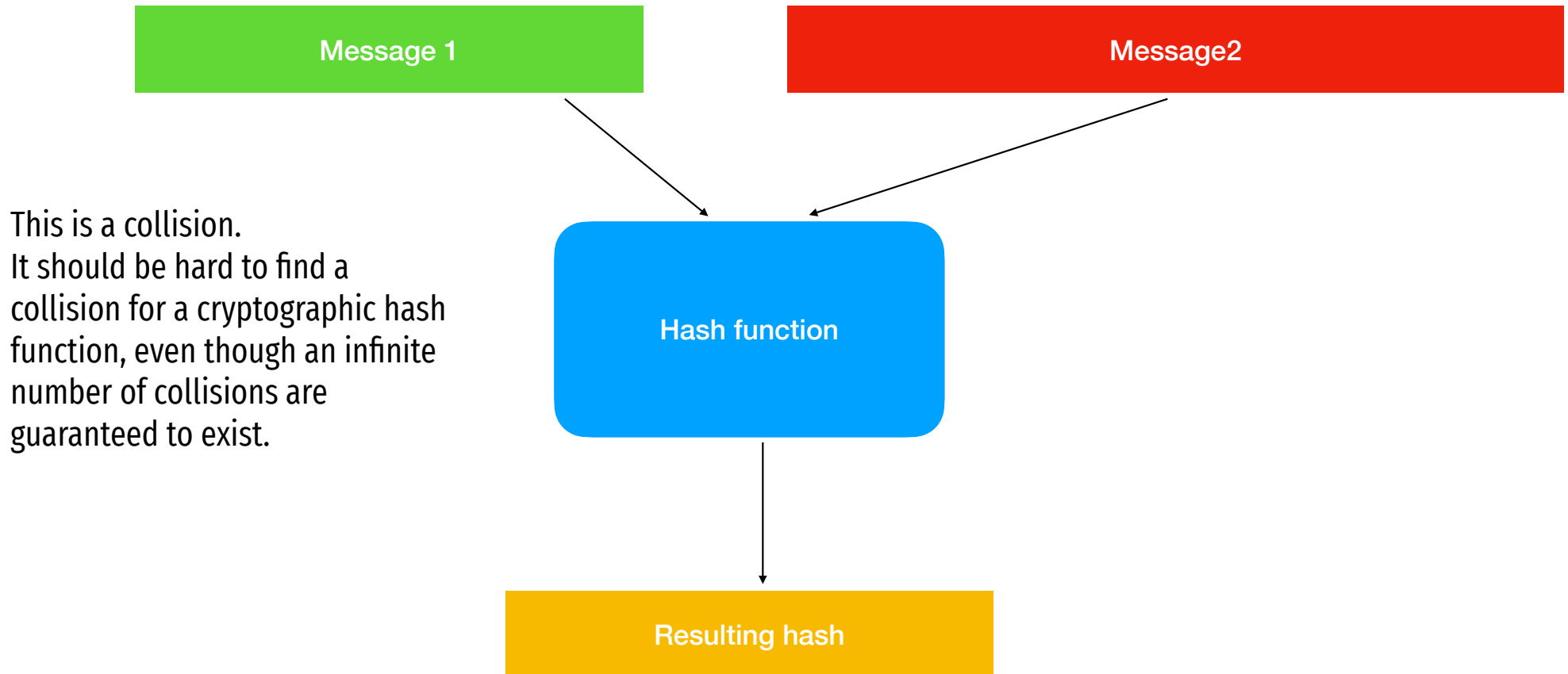
Hashed Passwords

- Key idea: store “hashed” versions of passwords
 - Use one-way cryptographic hash functions
 - Examples: MD5, SHA1, SHA256, SHA512, bcrypt, PBKDF2, scrypt

Goal of a hash function



Goal of a hash function: Collision resistance



MD5 is a broken hash function

```
$ md5 -s security
```

```
MD5 ("security") = e91e6348157868de9dd8b25c81aebfb9
```

```
$ md5 -s Security
```

```
MD5 ("Security") = 2fae32629d4ef4fc6341f1751b405e45
```

```
$ md5 -s Security1
```

```
MD5 ("Security1") = 8d01bda744a7a6392d3393e0ece561e8
```

```
$ echo -n "security" | shasum  
8eec7bc461808e0b8a28783d0bec1a3a22eb0821 -
```

```
$ echo -n "security" | shasum -a 256  
5d2d3ceb7abe552344276d47d36a8175b7aeb250a9bf0bf00e850cd23ecf2e43 -
```

Hashed Passwords

- Key idea: store “hashed” versions of passwords
 - Use one-way cryptographic hash functions
 - Examples: MD5, SHA1, SHA256, SHA512, bcrypt, PBKDF2, scrypt
- Cryptographic hash function transform input data into scrambled output data
 - Deterministic: $\text{hash}(A) = \text{hash}(A)$
 - Collision resistant
 - Locating A' such that $\text{hash}(A) = \text{hash}(A')$ takes a long time (hopefully)
 - Example: 2^{21} tries for md5

Note:MD5 is broken

Hashed Password Example



User: Charlie



MD5('p4ssw0rd') =
2a9d119df47ff993b662a8ef36f9ea20



MD5('2a9d119df47ff993b662a8ef36f9ea20')
= b35596ed3f0d5134739292faa04f7ca3



hashed_password.txt	
charlie	2a9d119df47ff993b662a8ef36f9ea20
greta	23eb06699da16a3ee5003e5f4636e79f
alice	98bd0ebb3c3ec3fbe21269a8d840127c
bob	e91e6348157868de9dd8b25c81aebfb9

Attacking Password Hashes

- Recall: cryptographic hashes are collision resistant
 - Locating A' such that $\text{hash}(A) = \text{hash}(A')$ takes a long time (hopefully)
- Are hashed password secure from cracking?

Failure of

Failure of Operation

Failure of Abstraction

Failure of Operation

Humans pick easy-to-guess passwords.

Failure of Abstraction

Humans are not capable of remembering hard-to-guess passwords.

Attacking Password Hashes

- Recall: cryptographic hashes are collision resistant
 - Locating A' such that $\text{hash}(A) = \text{hash}(A')$ takes a long time (hopefully)
- Are hashed password secure from cracking?
 - **No!**
- Problem: users choose poor passwords
 - Most common passwords: 123456, password
 - Username: cbw, Password: cbw
- Weak passwords enable **dictionary attacks**

The authors have conducted experiments to try to determine typical users' habits in the choice of passwords when no constraint is put on their choice. The results were disappointing, except to the bad guy. In a collection of 3,289 passwords gathered from many users over a long period of time,

- 15 were a single ASCII character;
- 72 were strings of two ASCII characters;
- 464 were strings of three ASCII characters;
- 477 were strings of four alphanumerics;
- 706 were five letters, all upper-case or all lower-case;
- 605 were six letters, all lower-case.

An additional 492 passwords appeared in various available dictionaries, name lists, and the like. A total of 2,831 or 86 percent of this sample of passwords fell into one of these classes.

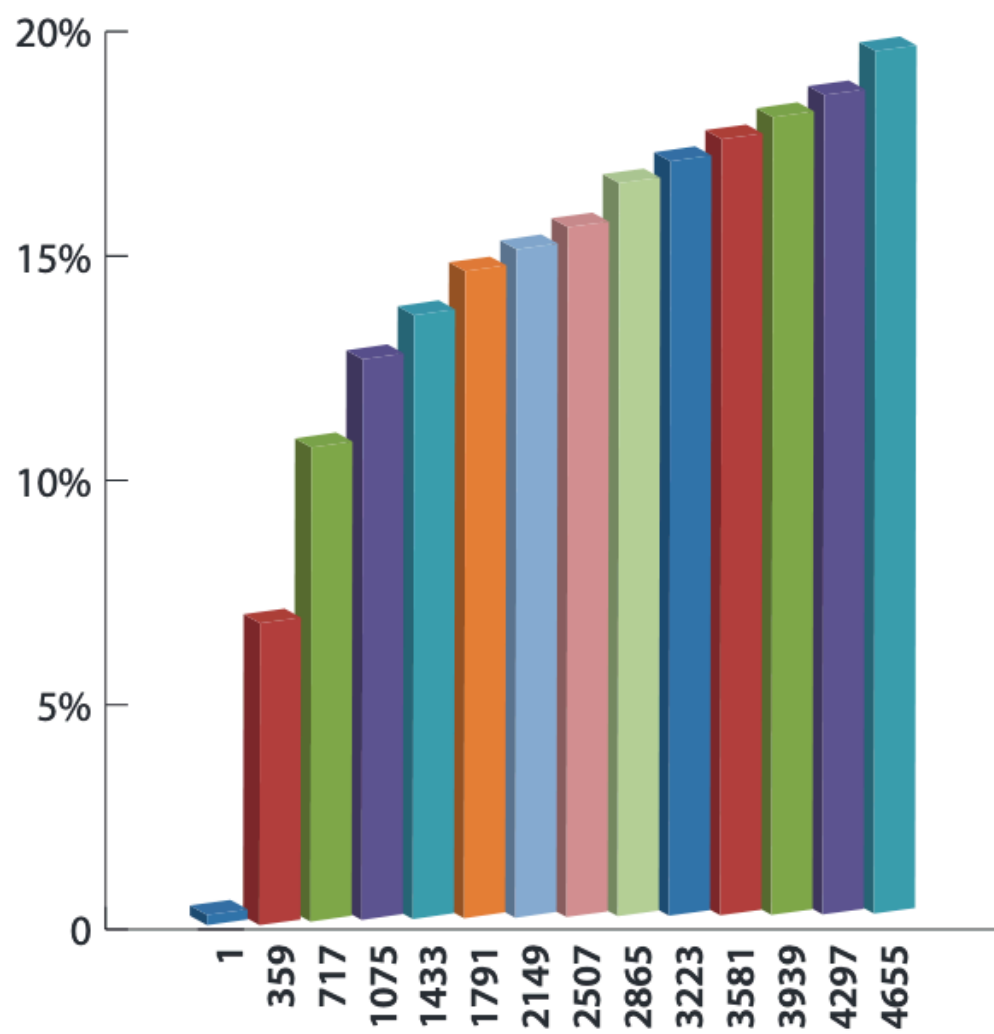
From Rockyou breach

Rank	Password	Number of Users with Password (Absolute)
1	123456	290731
2	12345	79078
3	123456789	76790
4	Password	61958
5	iloveyou	51622
6	princess	35231
7	rockyou	22588
8	1234567	21726
9	12345678	20553
10	abc123	17542

Password Popularity—Top 20

Rank	Password	Number of Users with Password (Absolute)
11	Nicole	17168
12	Daniel	16409
13	babygirl	16094
14	monkey	15294
15	Jessica	15162
16	Lovely	14950
17	michael	14898
18	Ashley	14329
19	654321	13984
20	Qwerty	13856

https://www.imperva.com/docs/gated/WP_Consumer_Password_Worst_Practices.pdf



Accumulated Percent of Dictionary Attack Success

Most Common Passwords

Rank	2013	2014
1	123456	123456
2	password	password
3	12345678	12345
4	qwerty	12345678
5	abc123	qwerty
6	123456789	123456789
7	111111	1234
8	1234567	baseball
9	iloveyou	dragon
10	adobe123	football

2012: 6.5 million hashes leaked onto Internet 90% cracked in 2 weeks

2016: 177.5 million more hashes leaked 98% cracked in 1 week

2012 LinkedIn Breach had 117 Million Emails and Passwords Stolen, Not 6.5M

May 18, 2016



Long time users of LinkedIn users may very well need to change their passwords once more



Related Posts

Web Skimming
Attack on Blue
❖ Bear Affects
School Admin

One month ago today, we wrote about Adobe's [giant data breach](#).

As far as anyone knew, including Adobe, it affected about 3,000,000 customer records, which made it sound pretty bad right from the start.

But worse was to come, as recent updates to the story bumped the number of affected customers to a [whopping 38,000,000](#).

We took Adobe to task for a lack of clarity in its breach notification.

OUR COMPLAINT

One of our complaints was that Adobe said that it had lost *encrypted* passwords, when we thought the company ought to have said that it had lost



```
4464 1 User ID yahoo.com|-g2B6PhWEH36 5 Password hint try: qwerty123 --
4465 |--|xxxxx@jcom.home.ne.jp|-Eh5tLomK+N*8zcs0vWU9bw==|-|-----|
4466 |--|xx@hotmail.com|-ahw2b2BELzgRTWYvQGn+kw==|-quiero a...|--
4467 |--|xxx@yahoo.com|-leMTcMPEPcjioxG6CatHBw==|-|--
4468 |username 2 Username e.com|-2GtbVrmsERzioXG6CatHBw==|-|--
4469 |--|xxxxx@yahoo.com|-4LSLo772tH4= 4 Password data (base64)
4470 |--|xxx@hotmail.com|-xxxxx4xxxxxG6CatHBw==|-|--
4471 |--|xxx@yahoo.com 3 Email address xG6CatHBw==|-myspace|--
4471 |--|xxx@hotmail.com|-kby1918wDrrioxG6CatHBw==|-regular|--
```

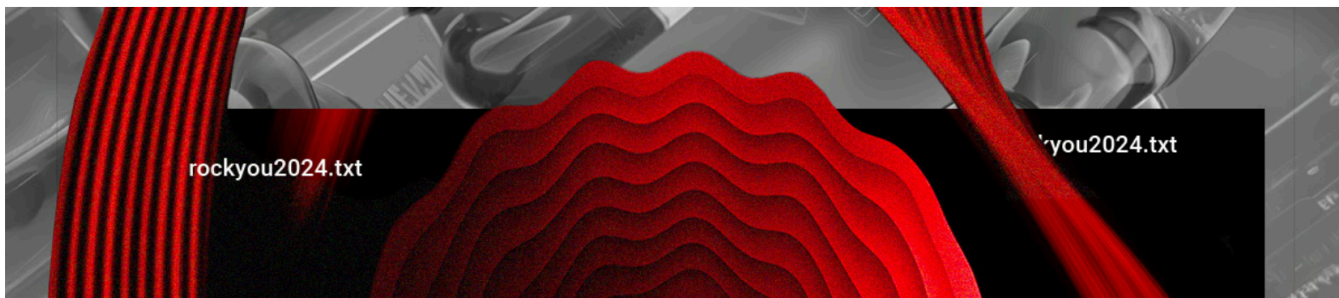
Adobe password data		Password hint	
110edf2294fb8bf4	->	numbers 123456	1 123456
110edf2294fb8bf4	->	==123456	
110edf2294fb8bf4	->	c'est "123456"	
8fda7e1f0b56593f e2a311ba09ab4707	->	numbers	2 12345678
8fda7e1f0b56593f e2a311ba09ab4707	->	1-8	
8fda7e1f0b56593f e2a311ba09ab4707	->	8digit	
2fca9b003de39778 e2a311ba09ab4707	->	the password is password	3 password
2fca9b003de39778 e2a311ba09ab4707	->	password	
2fca9b003de39778 e2a311ba09ab4707	->	rhymes with assword	
e5d8efed9088db0b	->	q w e r t y	4 qwerty
e5d8efed9088db0b	->	ytrewq tagurpidi	
e5d8efed9088db0b	->	6 long qwert	
ecba98cca55eabc2	->	sixxone	6 111111
ecba98cca55eabc2	->	1*6	
ecba98cca55eabc2	->	sixxones	

RockYou2024: 10 billion passwords leaked in the largest compilation of all time

Updated on: July 04, 2024 12:33 PM  4

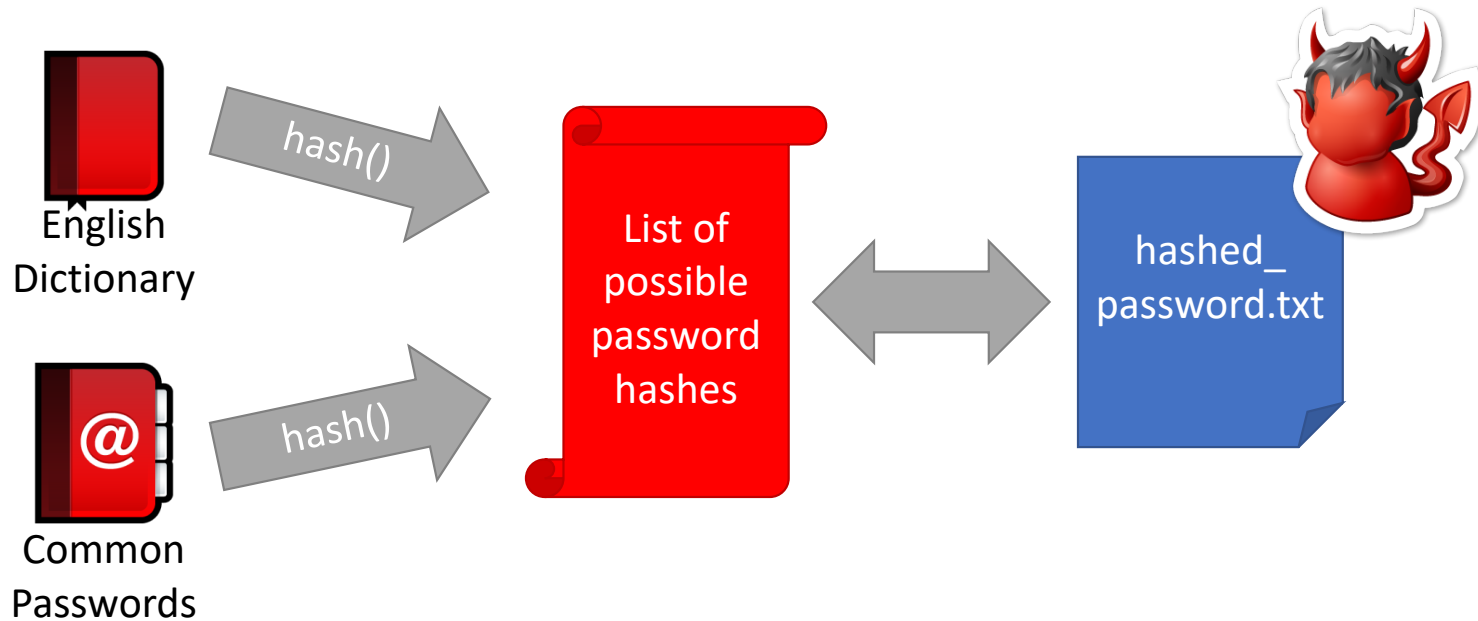


Vilius Petkauskas, Deputy Editor



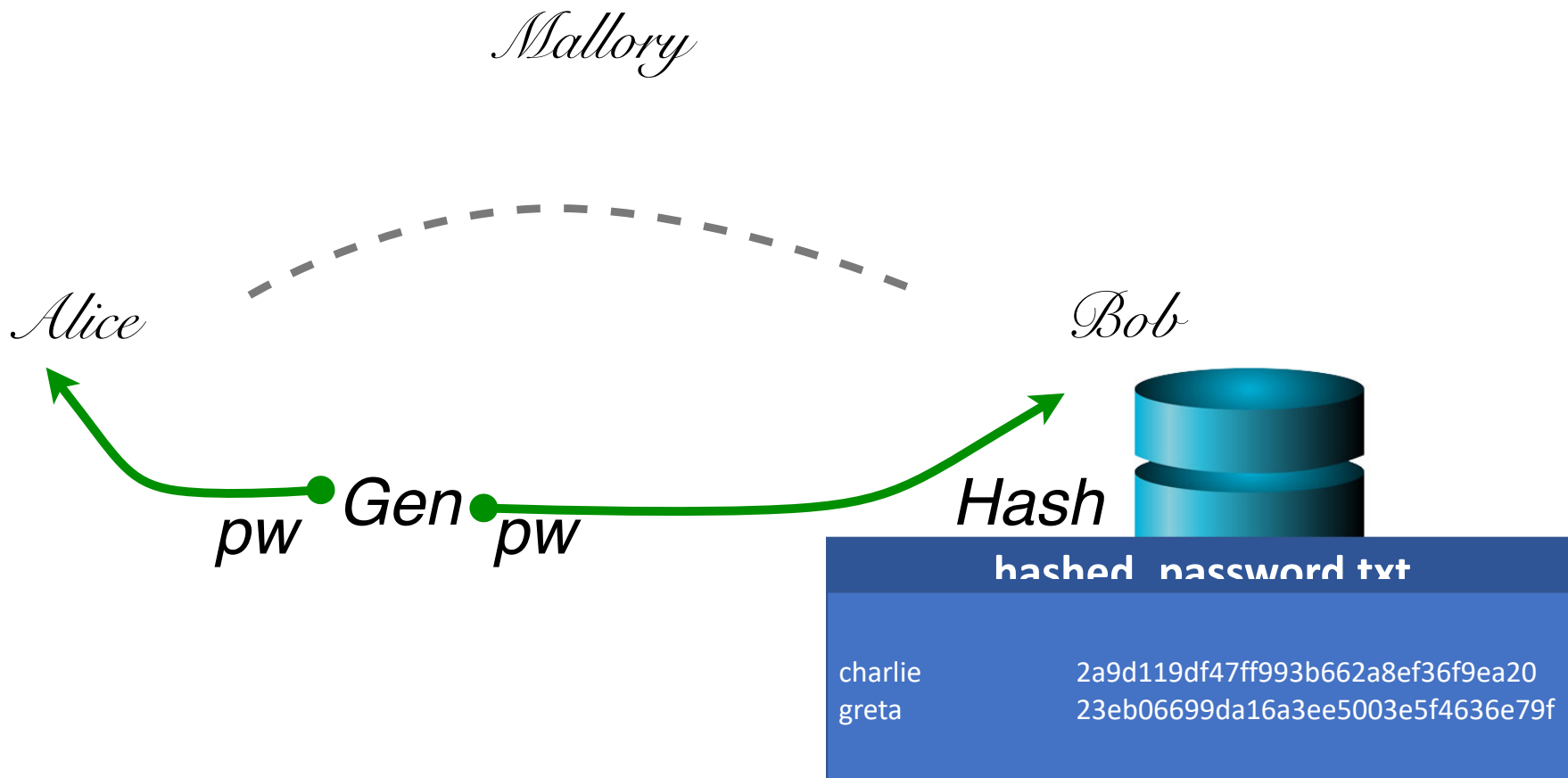
The king is dead. Long live the king. Cybernews researchers discovered what appears to be the largest password compilation with a staggering 9,948,575,739 unique plaintext passwords. The file with the data, titled **rockyou2024.txt**, was posted on July 4th by forum user ObamaCare.

Dictionary Attacks

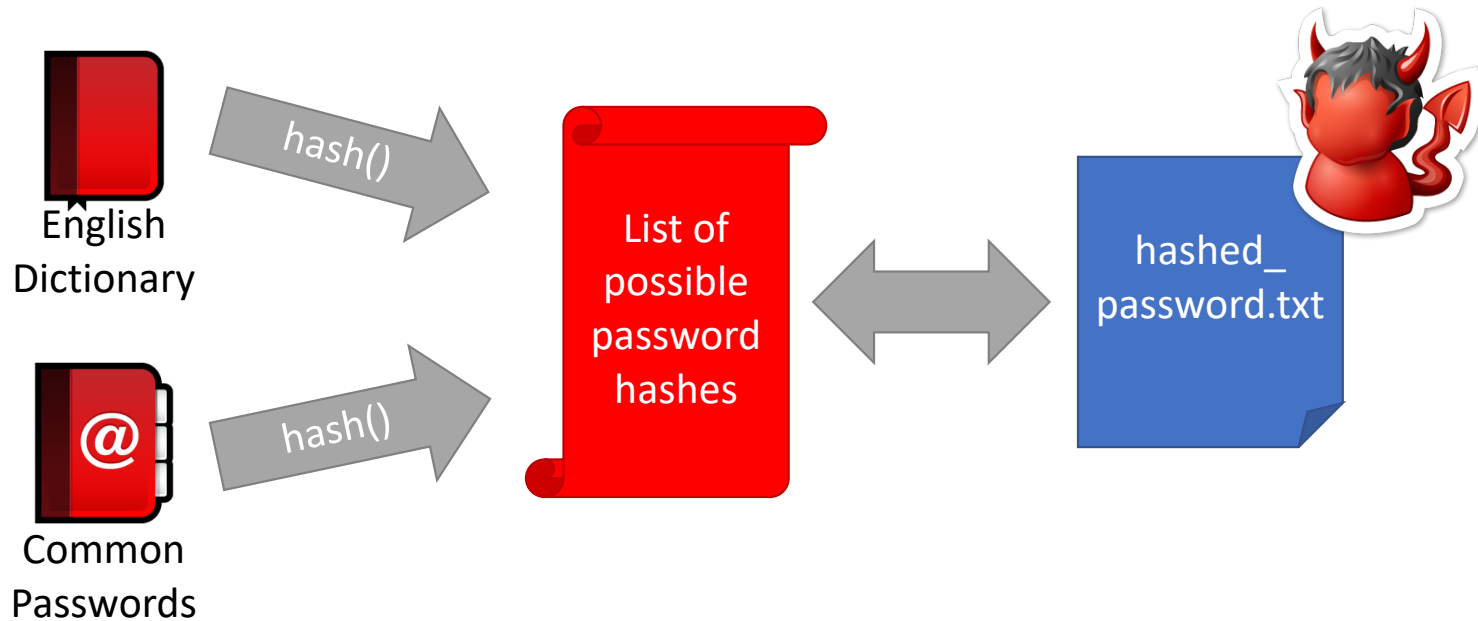


- Common for 60-70% of hashed passwords to be cracked in <24 hours

Attack 1



Dictionary Attacks



- Common for 60-70% of hashed passwords to be cracked in <24 hours

Brute force attack estimates

How big is the alphabet from which pwd are chosen?