AUTHENTICATION

VITALY SHMATIKOV

Image: Lorrie Cranor's password quilt

What Threats Should This Service Worry About?

Hosts

Guests

airbnb

Database (e.g., SQL)

Threats from Malicious Users

Account abuse

- Uses posting malicious comments, reviews
- Scammers setting up fraudulent listings
- What else?

CS 5432

Account security

- Protect information from improper access
- Protect accounts from compromise

Need **permission model**
Need **user authentication**

Permission Model

Different kinds of **users**:

- Guests
- Hosts
- Admins (e.g., moderators)

Subjects

Different kinds of **resources**:

- Profile pages
- Credit card data

Objects

could be implicit, eg,
access control list (ACL)

Access Control Matrix

Butler Lampson, 1971

Objects

Subjects

	resource 1	resource 2	...	resource n
user 1	read, write	read, write, own		read
user 2				
...				
user m	append	read, execute		read,write, own

This is an authorization policy: what permissions does user have on object?

Unix-style file system permissions (rwx) is an implementation of this

Authentication vs. Authorization & Access Control

Authentication: is the user (or program) who they claim they are?

Authorization: should user (or program) have access to a given resource?

- Authorization decisions rely on correct authentication

Access control: policy and enforcement mechanism

The Core Problem of Authentication

How do you prove to someone that you are who you claim to be?

- Any system with access control must solve this problem

- **What you know**: password, PIN, answers to questions only you know
- **What you are**: biometrics
- **What you have**: phone number, mobile device, secure token
- **Where you are**: IP address, geolocation
- **Someone/something knows you:** single sign-on (Cornell NetID), PKI


CIRCLE · LINE
THE TONIGHT SHOW
JIMMY FALLON

Password-Based Authentication

User has a secret password.

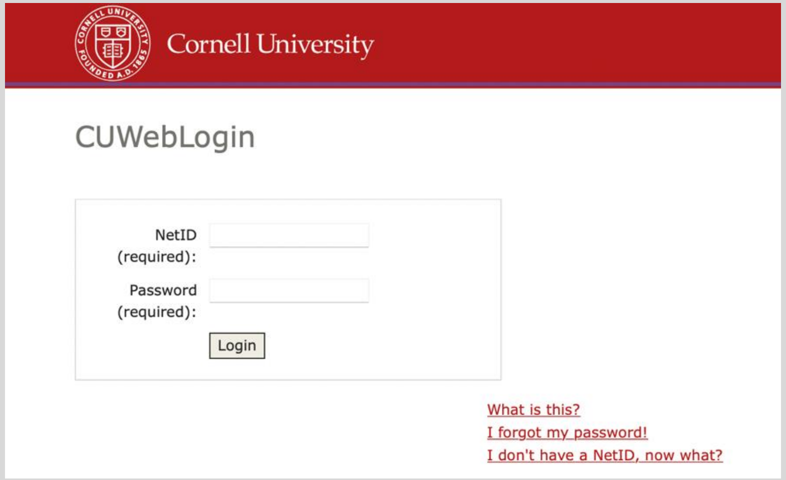
System checks it to authenticate the user.

- How is the password communicated?
- How is the password stored?
- How does the system check the password?
- How easy is it to guess the password?

Easy to deploy

Easy to use (nothing to carry, etc.)

No simple alternative



Attacks on Passwords

Online

- Try to guess passwords by logging to a live system

Offline

- Try to guess passwords in the (typically stolen) password database

Phishing

- Trick user into disclosing their password
- Spear-phishing: phishing a specific user with personalized attacks

Malware

- Compromise user's computer or phone, sniff passwords as they type them

Passwords Are The Bane of Computer Security

Phishing and use of stolen credentials are the top two hacking techniques

- Source: Verizon Data Breach Investigations Report

First step after any successful intrusion: install sniffer or keylogger to steal more passwords

Then run cracking tools on password files

- Modern systems usually do not store passwords in the clear (how are they stored?)

Back in 2016

Roger Stone
@RogerJStoneJr

Follow

Trust me, it will soon the Podesta's time in the barrel. #CrookedHillary

10:24 AM - 21 Aug 2016

389 481

In March 2016, the personal Gmail account of John Podesta, a former White House chief of staff and chair of Hillary Clinton's 2016 U.S. presidential campaign, was compromised in a data breach accomplished via a spear-phishing attack, and some of his emails, many of which were work-related, were hacked. Cybersecurity researchers as well as the United States

“Change Your Password Immediately”

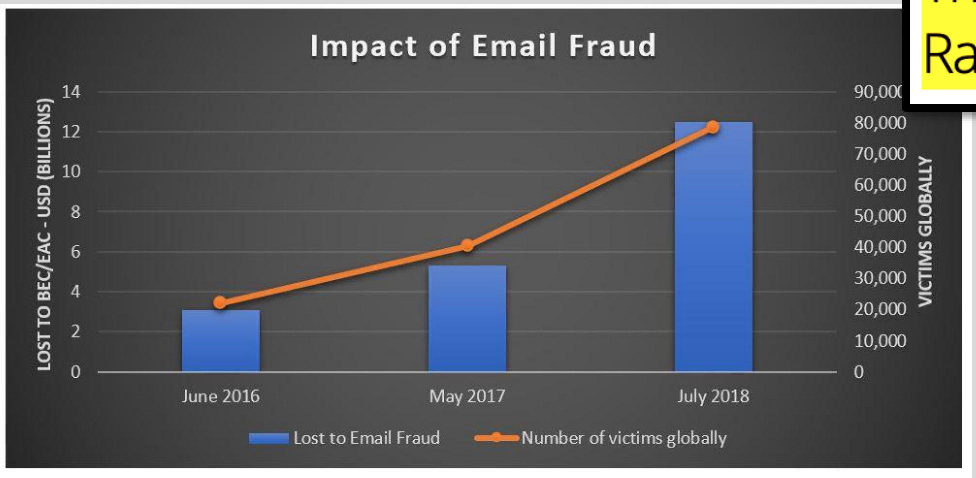
> *From:* Google <no-reply@accounts.googlemail.com>
> *Date:* March 19, 2016 at 4:34:30 AM EDT
> *To:* [redacted]ta@gmail.com
> *Subject:* *Someone has your password*
>
> Someone has your password
> Hi John
>
> Someone just used your password to try to sign in to your Google Account
> [redacted]@gmail.com.
>
> Details:
> Saturday, 19 March, 8:34:30 UTC
> IP Address: 134.249.139.239
> Location: Ukraine
>
> Google stopped this sign-in attempt. You should change your password
> immediately.
>
> CHANGE PASSWORD <https://bit.ly/1PibSU0>
>
> Best,
> The Gmail Team
> You received this mandatory email service announcement to update you about
> important changes to your Google product or account.

The link brought Podesta to a fake log-in page where he entered his Gmail credentials.

The email was initially sent to the IT department as it was suspected of being a fake but was described as "legitimate" in an e-mail sent by a department employee, who later said he meant to write "illegitimate".

Phishing and Email Fraud Statistics 2019

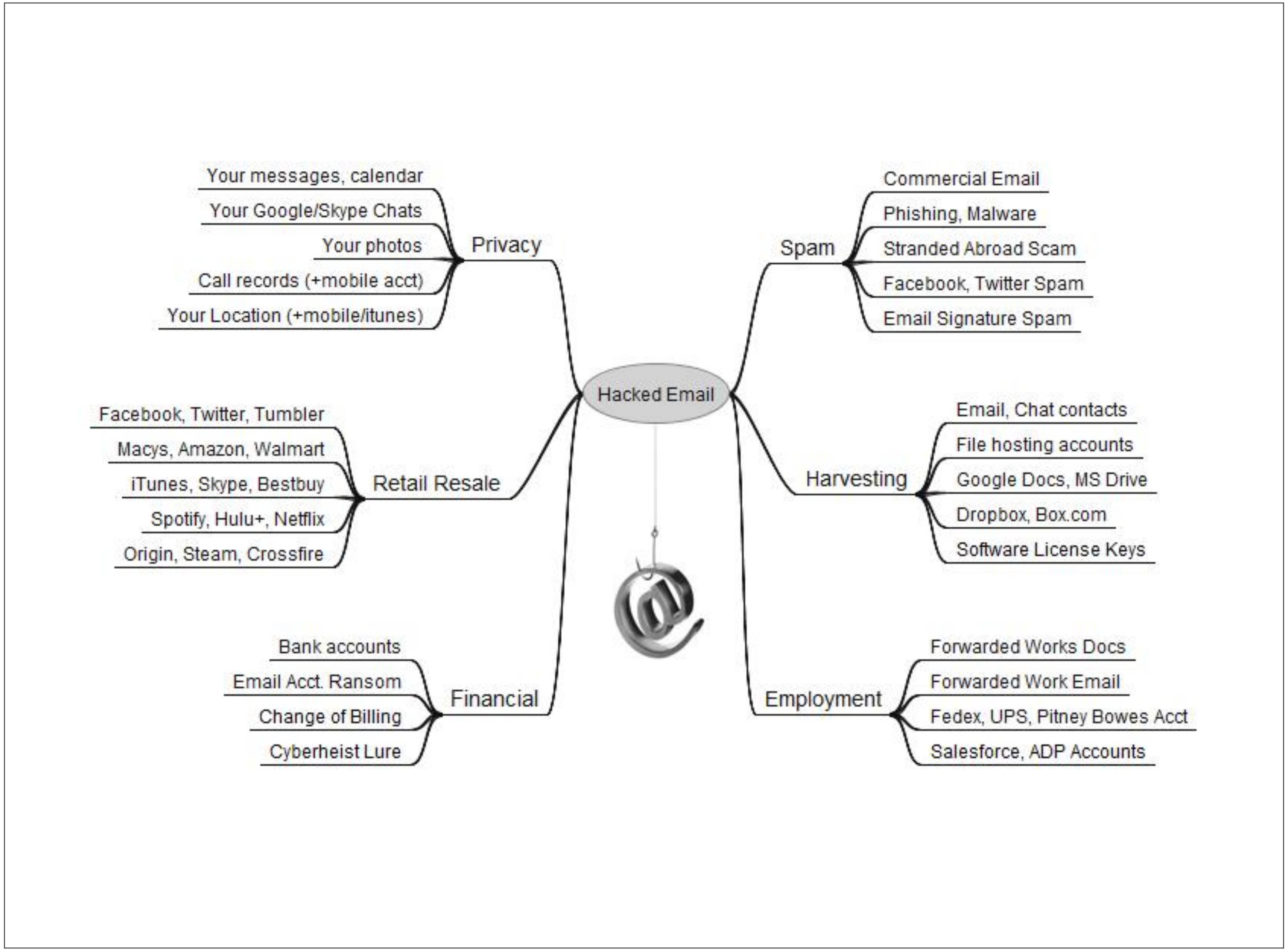
- The average financial cost of a data breach is $3.86m (IBM)
- Phishing accounts for 90% of data breaches
- 15% of people successfully phished will be targeted at least one more time within the year
- BEC scams accounted for over $12 billion in losses (FBI)



This Year, Phishing Causes Losses of $17,700 per minute And Ransomware Attacks Will Cost $22,184 Per Minute

Sources: https://retruster.com/blog/2019-phishing-and-email-fraud-statistics.html
https://www.proofpoint.com/us/corporate-blog/post/fbi-reports-125-billion-global-financial-losses-due-business-email-compromise
https://blog.knowbe4.com/this-year-phishing-causes-losses-of-17700-per-minute-and-ransomware-attacks-will-cost-22184-per-minute

From Here to Eternity



https://krebsonsecurity.com/2019/01/773m-password-megabreach-is-years-old

Default Passwords

Examples from Mitnick's "Art of Intrusion"

- U.S. District Courthouse server: "public" / "public"
- NY Times employee database: pwd = last 4 SSN digits
- "Dixie bank": break into router (pwd="administrator"), then into bank server (pwd="administrator"), install keylogger to snarf other passwords
  - "99% of people there used password123 as their password"

Mirai botnet (2016)

- Used default passwords in IoT devices (Internet cameras, home routers, etc.) to stage a massive distributed denial-of-service flooding attack

From Mirai’s Source Code

Username	Password
666666	666666
888888	888888
admin	*(none)*
admin	1111
admin	1111111
admin	1234
admin	12345
admin	123456
admin	54321
admin	7ujMko0admin
admin	admin
admin	admin1234
admin	meinsm
admin	pass
admin	password
admin	smcadmin
admin1	password
administrator	1234
Administrator	admin
guest	12345
guest	guest
mother	fucker
root	*(none)*
root	00000000
root	1111
root	1234
root	12345
root	123456
root	54321
root	666666
root	7ujMko0admin
root	7ujMko0vizxv
root	888888
root	admin
root	anko
root	default
root	dreambox
root	hi3518
root	ikwb
root	juantech
root	jvbzd

rockyou™ Hack (2009)

"Social gaming" company

Database with 32 million user passwords from partner social networks

Passwords stored in the clear

December 2009: entire database hacked using a SQL injection attack and posted on the Internet

More about SQL injection later

Passwords in the RockYou Database

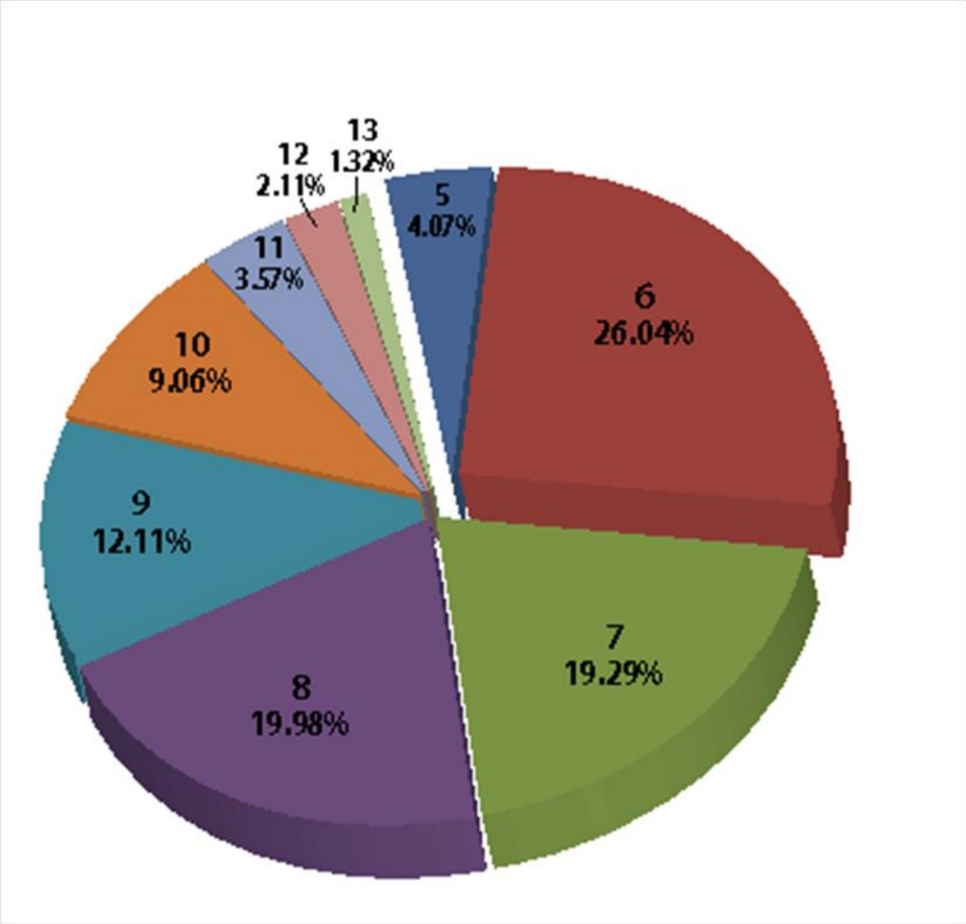
Password Popularity – Top 20

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

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

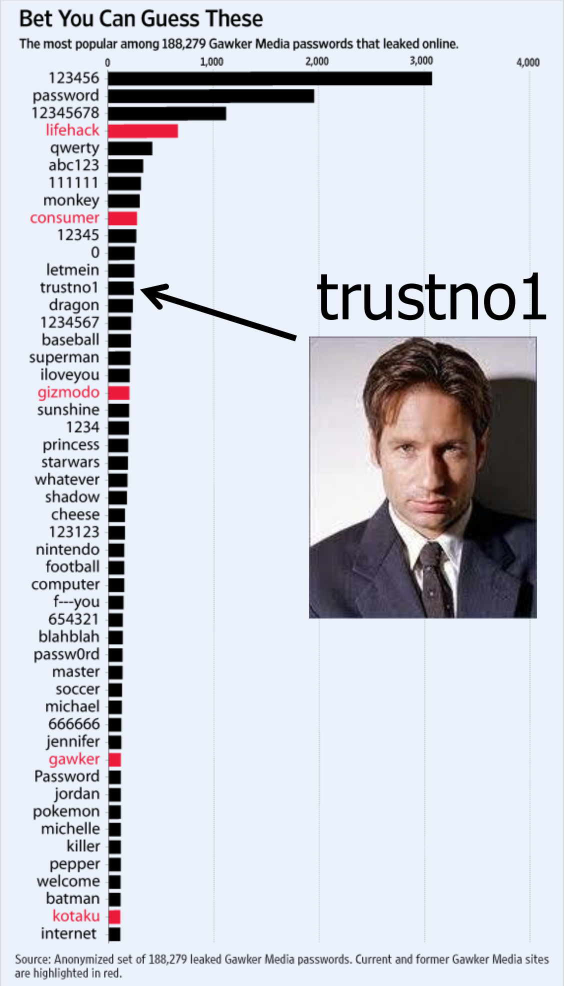
Source: Imperva

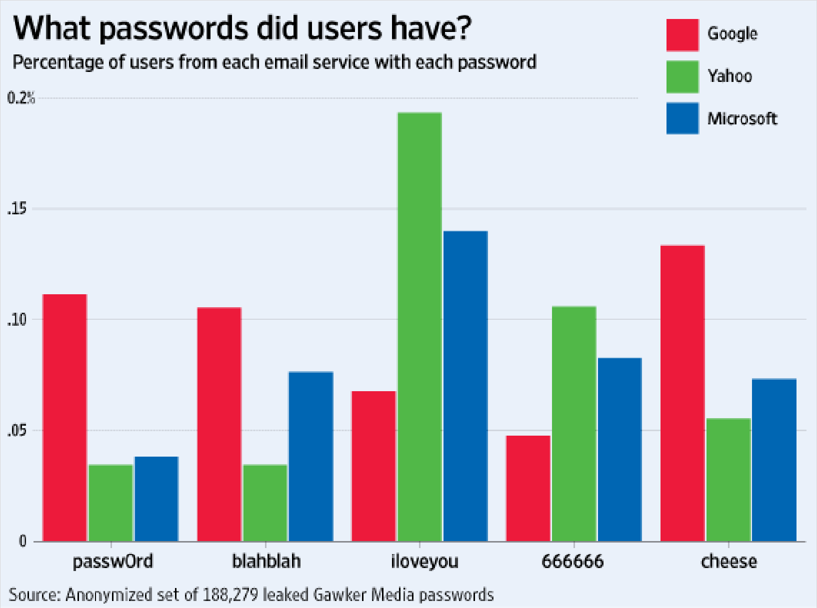
Password Length Distribution



Source: Imperva

Gawker Passwords (2010)





Source: WSJ

2020: major attack on US government and several companies via a compromised update to SolarWinds network management software

The company used the password solarwinds123 for a GitHub server

Company denied this was the source of the breach

"I believe that was a password that an intern used on one of his Github servers back in 2017"

SolarWinds CEO

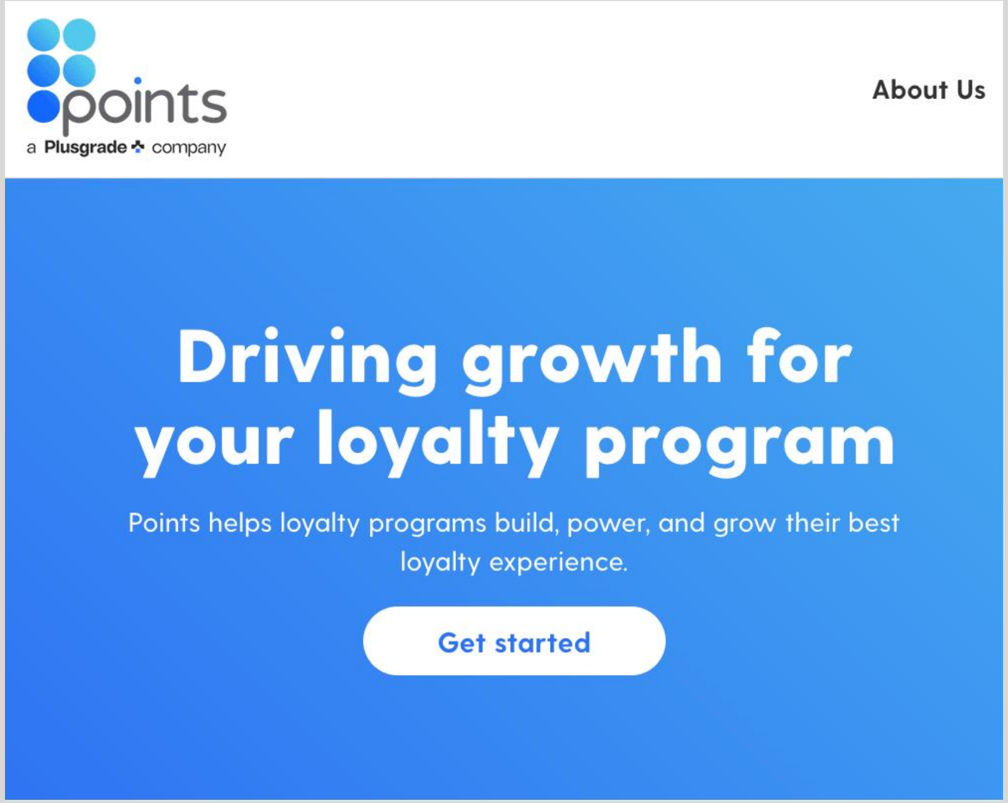
Image: Insider

IHG hack: 'Vindictive' couple deleted hotel chain data for fun

17 September 2022

"They accessed the FTSE 100 firm's databases thanks to an easily found and weak password, Qwerty1234"

https://www.bbc.com/news/technology-62937678



points.com, a platform for managing loyalty points and travel rewards

- Encrypted cookie assigned to each user of the points.com global administration website
- Encrypted with the word "secret"
- Any user could decrypt their cookie, assign themselves global administrator privileges, reencrypt the cookie and gain global administrator privileges for any reward system (grant unlimited miles, etc.)

https://arstechnica.com/security/2023/08/unlimited-miles-and-nights-vulnerability-in-travel-rewards-programs-found/

Cracking Techniques

Wordlists

- 20-500 million words and leaked passwords in publicly available lists

Mangling rules to generate variants

- Dozens of thousands of rules (Korelogic, Megatron, Generated2)

Cracking tools

- Example: John the Ripper, Hashcat

Password Mangling and Generation

Dictionary with words spelled backwards	First and last names, streets, cities	Same with upper-case initials
All valid license plate numbers in your state	Room numbers, telephone numbers, etc.	Letter substitutions and other tricks

If you can think of it, attacker will, too!

Social Engineering

Univ. of Sydney study (1996)

- 336 CS students emailed asking for their passwords
  - Pretext: “validate” password database after suspected break-in
- 138 returned their passwords; 30 returned invalid passwords; 200 reset passwords (not disjoint)

Treasury Dept. report (2005)

- Auditors pose as IT personnel attempting to correct a “network problem”
- 35 of 100 IRS managers and employees provide their usernames and change passwords to a known value

Bezos, Musk, Gates, Obama and others target of cryptocurrency hack on Twitter

Jefferson Graham, Emre Kelly and Mike Snider USA TODAY

Published 5:42 p.m. ET Jul. 15, 2020

The Twitter accounts of prominent figures from the worlds of tech and money, celebrities, a presidential candidate and a former president were all hacked Wednesday in what was the largest breach in the company's history.

Bogus messages soliciting bitcoin appeared on the Twitter accounts for Tesla CEO Elon Musk, Microsoft co-founder Bill Gates, Amazon CEO and founder Jeff Bezos, Berkshire Hathaway CEO and president Warren Buffett, former President Barack Obama, presumptive Democratic candidate Joe Biden, former New York mayor Michael Bloomberg, Israeli Prime Minister Benjamin Netanyahu and the corporate accounts for Apple and Uber.

Celebrities were also targeted in the bitcoin scam including rapper Kanye West and his wife Kim Kardashian and rapper Wiz Khalifa.

Twitter said late Wednesday that it detected what it believes was a "coordinated social engineering attack by people who successfully targeted some of our employees with access to internal systems and tools."

July 2020 Twitter Hack

The social engineering that occurred on July 15, 2020, targeted a small number of employees through a phone spear phishing attack. A successful attack required the attackers to obtain access to both our internal network as well as specific employee credentials that granted them access to our internal support tools. Not all of the employees that were initially targeted had permissions to use account management tools, but the attackers used their credentials to access our internal systems and gain information about our processes. This knowledge then enabled them to target additional employees who did have access to our account support tools. Using the credentials of employees with access to these tools, the attackers targeted 130 Twitter accounts, ultimately Tweeting from 45, accessing the DM inbox of 36, and downloading the Twitter Data of 7.

https://blog.twitter.com/en_us/topics/company/2020/an-update-on-our-security-incident.html

How People Use Passwords

Write them down

Use a single password at multiple sites

- Do you use the same password for Amazon and your bank account? NetID? Do you remember them all?

Forget them… many services use “security questions” to reset passwords

- “What is your favorite pet’s name?”
- Paris Hilton’s T-Mobile cellphone hack

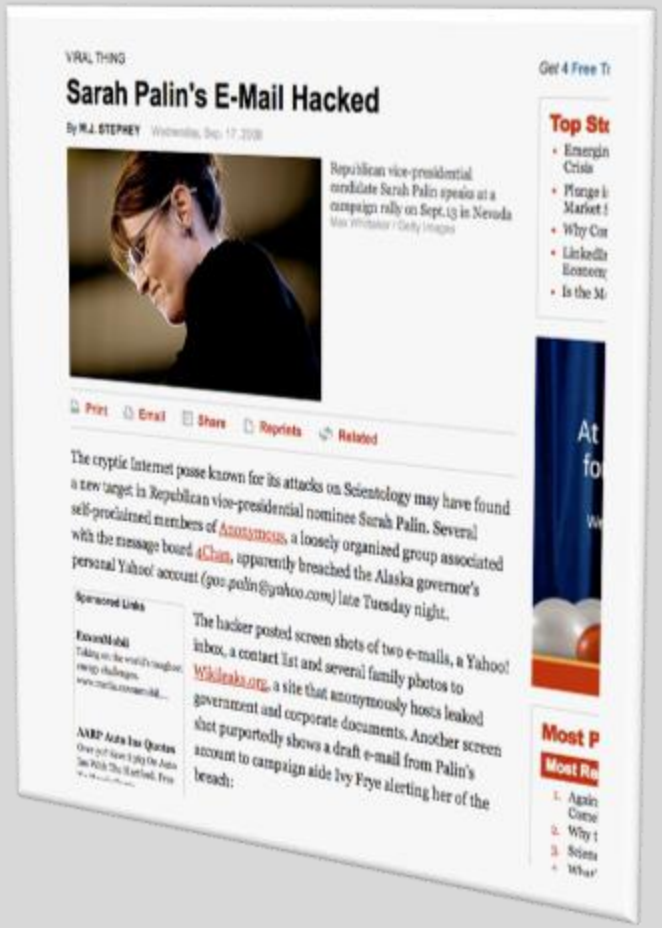
Sara Palin's Email Hack

Reset password for gov.palin@yahoo.com

- No secondary email needed
- Date of birth? Wikipedia
- ZIP code? Wasilla has 2
- Where did you meet your spouse? Wikipedia, Google, …

Changed pwd to "popcorn"

Hacker sentenced to 1 year in prison +
3 yrs of supervised release


VIRAL THING

Sarah Palin's E-Mail Hacked

By M.J. STEPHEY

Republican vice-presidential candidate Sarah Palin speaks at a campaign rally on Sept.13 in Nevada

Print Email Share Reprints Related

The cryptic Internet posse known for its attacks on Scientology may have found a new target in Republican vice-presidential nominee Sarah Palin. Several self-proclaimed members of Anonymous, a loosely organized group associated with the message board 4Chan, apparently breached the Alaska governor's personal Yahoo! account (gov.palin@yahoo.com) late Tuesday night.

The hacker posted screen shots of two e-mails, a Yahoo! inbox, a contact list and several family photos to Wikileaks.org, a site that anonymously hosts leaked government and corporate documents. Another screen shot purportedly shows a draft e-mail from Palin's account to campaign aide Ivy Frye alerting her of the breach:

slide: Gustav Rydstedt

Rabkin, "Security questions in the era of Facebook"

Problems with Security Questions

Inapplicable

- What high school did your spouse attend?

Not memorable

- Name of kindergarten teacher? Price of your first car?

Ambiguous

- Name of college you applied to but did not attend?

Easily guessable

- Age when you married? Year you met your spouse? Favorite president? Favorite color?

Automatically attackable (using public records!)

Answers Are Easy to Find Out… Or Easy to Forget

Make of your first car?
- Until 1998, Ford had >25% of market

First name of your best friend?
- 10% of males: James/Jim, John, Robert/Bob/Rob

Name of your first / favorite pet?
- Max, Jake, Buddy, Bear…
- Top 500 (covers 65% of names) available online

Information available from Facebook, etc.
- Where you went to school, college athletic rivals, favorite book/movie/pastime, high school mascot

Name of the street, etc.
- More than one

Name of your best friend?
- Friends change

City where you were born?
- NYC? New York? Manhattan? New York City? Big Apple?

People lie to increase security… then forget the answers

HealthCare.gov

<u>Federal:</u>

- What is a relative's telephone number that is not your own?
- Type a significant date in your life?
- What is the name of the manager at your first job?

<u>Individual states:</u>

- What is your youngest child's birth weight?
- What color was your first bicycle?
- If you needed a new first name, what would it be?
- What band poster did you have on your wall in high school?
- How many bones have you broken?

In August 2021, a 21-year-old hacker scanned T-Mobile's known Internet addresses

Discovered an unprotected router, used it to gain access to a data center near East Wenatchee, WA

Image: WSJ

Login credentials stored in the data center provided access to 100 more servers

T-Mobile Says Hack Exposed Personal Data of 40 Million People

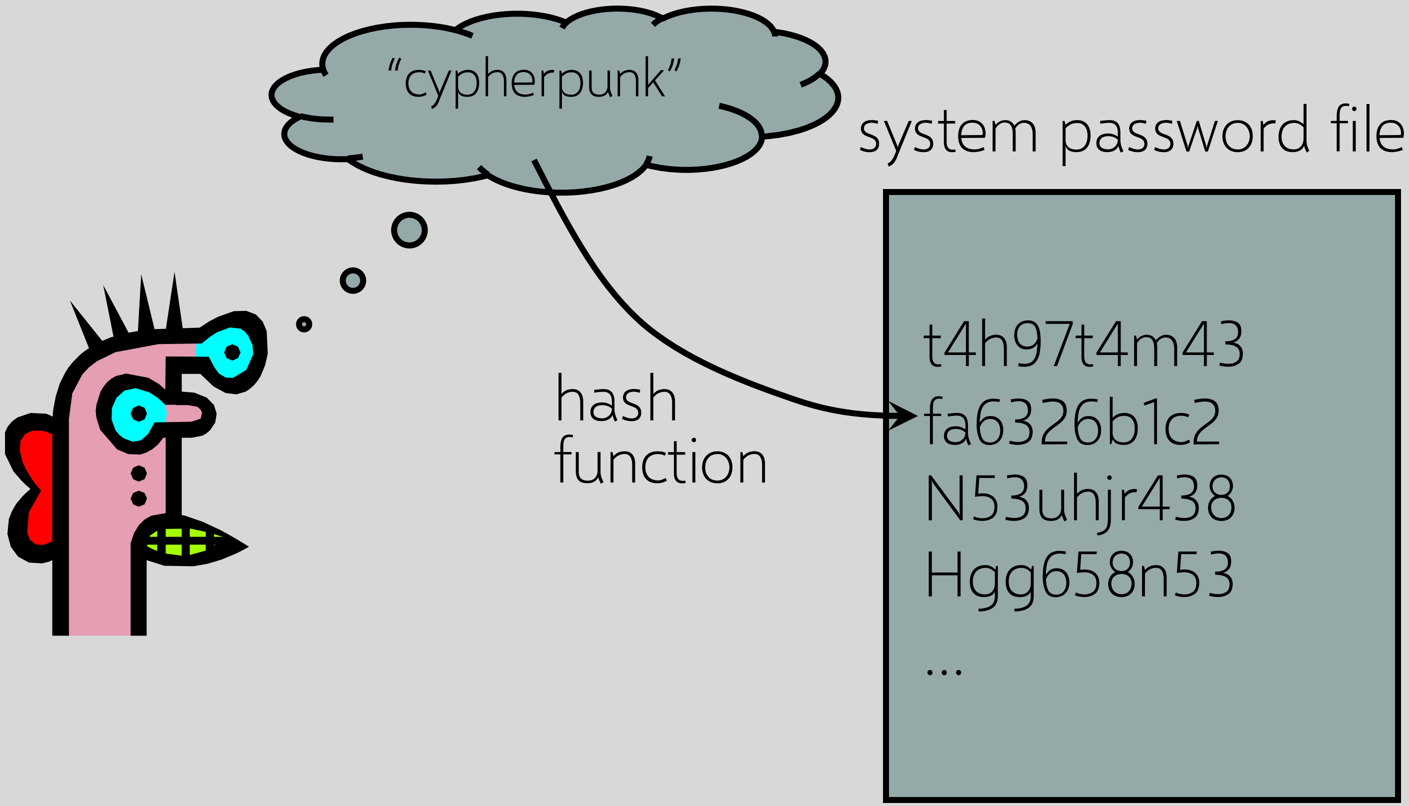
The company said that stolen files included the personal information of 7.8 million current customers and 40 million people who had applied for credit.

NYT, August 18, 2021

Password Management

Countermeasure	Purpose
Password hashing	Database leak doesn't immediately reveal user passwords; slows **offline guessing attacks**
Strength meters	Nudge / force users to pick stronger passwords to mitigate guessing attacks
Lockout after N failed attempts	Prevent remote guessing attacks (X typically 10, 100, 1000); slows down / prevents **online guessing attacks**
Compromised credential checks	Check if password is in known breaches

Storing Passwords



Password Hashing

- Instead of user's password, store Hash(password)
- When user enters a password, compute its hash and compare with the entry in the password file
  - System does not store actual passwords
  - Cannot go from hash to password (except by guessing the password)
- Hash function H must have some properties

Cryptographic Hash Functions

Cryptographic hash function H maps any message to a short digest (e.g., 256-bit string)

- One-way:

  Given y = H(M), hard to compute M

- Collision-resistant:

  Can't find M, M' s.t. H(M) = H(M')

Good hash functions: SHA256, SHA512, SHA-3, bcrypt, scrypt, PBKDF2 ...

- ~~Deprecated hash functions:~~ MD5, SHA-1

specifically for passwords

Dictionary Attacks

Passwords are not random

- With 52 upper- and lower-case letters, 10 digits and 32 punctuation symbols, there are $94^8 \approx 6$ quadrillion possible 8-character passwords
- Humans like to use dictionary words, human and pet names ≈ 1 million common passwords

Attacker can pre-compute H(word) for every word in the dictionary – do this once <u>offline</u>

- Once password file is obtained, cracking is instantaneous
- Sophisticated password guessing tools are available (take into account frequency of letters, password patterns, etc.)

Brute-Force Password Cracking

```
DaleGribble% openssl speed sha256
Doing sha256 for 3s on 16 size blocks: 16553803 sha256's in 3.00s
Doing sha256 for 3s on 64 size blocks: 9314565 sha256's in 3.00s
Doing sha256 for 3s on 256 size blocks: 4382195 sha256's in 3.00s
Doing sha256 for 3s on 1024 size blocks: 1382599 sha256's in 3.00s
Doing sha256 for 3s on 8192 size blocks: 187044 sha256's in 3.00s
Doing sha256 for 3s on 16384 size blocks: 94277 sha256's in 3.00s
```

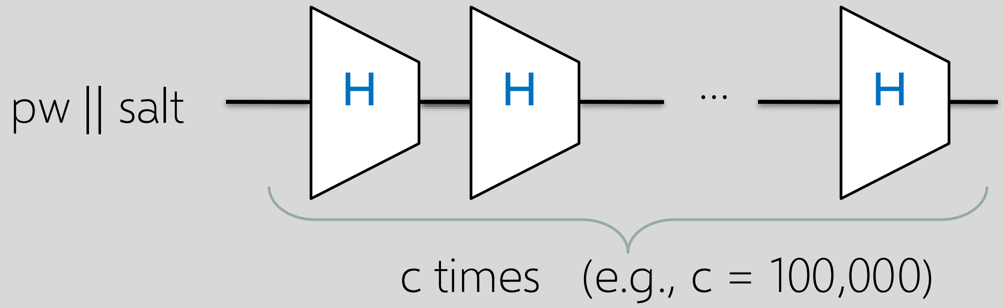
~450,000 hashes per second

How many guesses / hashes needed to crack a password?

Also rainbow tables:
precompute huge number of hashes to make a quick-lookup table

Making Cracking Harder

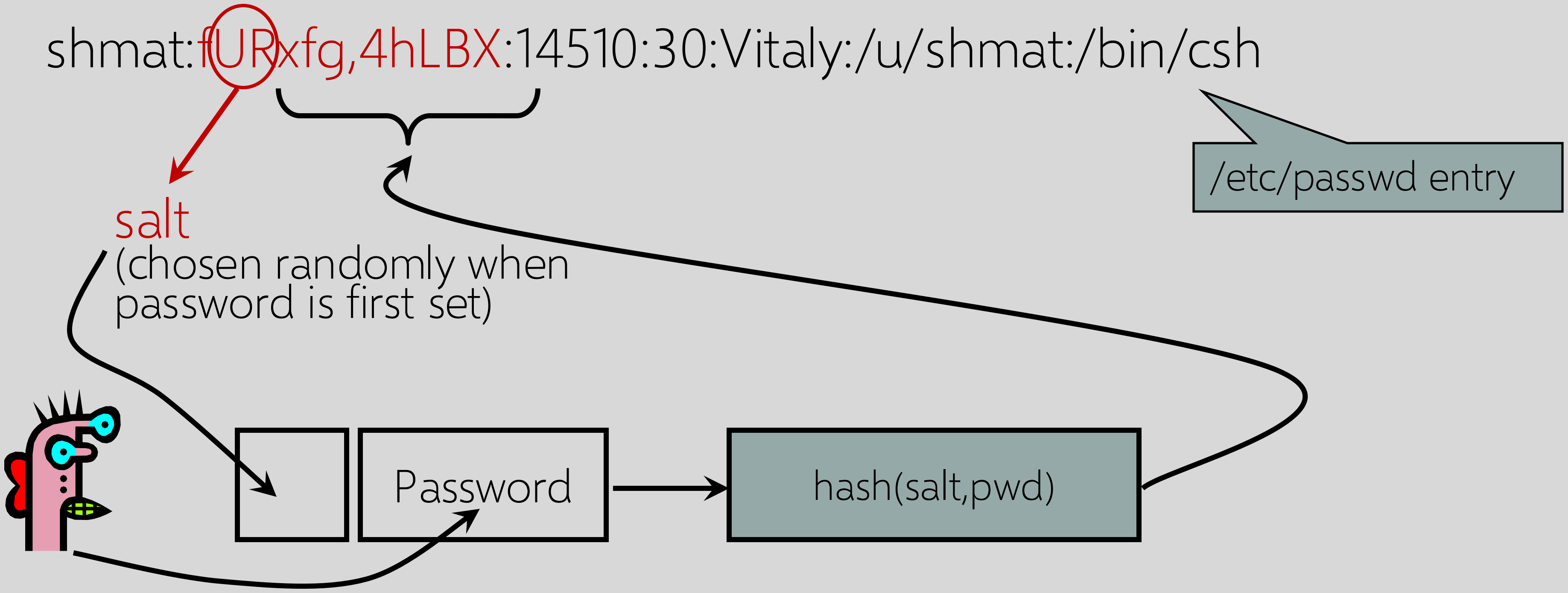
- Make hashing slower to slow down cracking attacks
- Use random per-user salts to prevent use of rainbow tables
- PKCS#5 approach:



$h = H^c(pw \,||\, salt)$

- Memory-hard hashing: Scrypt and argon2 require lots of memory to compute as well as time

Salt



- Users with the same password have <u>different</u> entries in the password file
- Offline dictionary attack becomes much harder

Advantages of Salting

Without salt, attacker can pre-compute hashes of all common passwords once

- Same hash function on all UNIX machines; identical passwords hash to identical values
- One table of hash values works for all password files

With salt, attacker must compute hashes of all common passwords for each possible salt value

- With 12-bit random salt, the same password can hash to 4096 different hash values

Modern Hash Cracking

Hash type	Hashes / second	Passwords / month for 10M set[3]	Brute force equivalent[4]
MD5 unsalted	~50G	~130,000,000G	~8-9 characters
MD5 salted[5]	~50G	~13G	~5 characters
MD5crypt (= salted, 1,000 x MD5)	~22M	~5.6M	~3-4 characters
Bcrypt (= salted, work factor 8)	~3500	~900	~1-2 characters

… with custom GPU and FPGA hardware

IBM X-Force "Cracken"
(circa 2017)

https://medium.com/@ScatteredSecrets/how-to-crack-billions-of-passwords-6773af298172

Measuring Password Strength

Hashing slows down but does not prevent guessing attacks

Deprecated approaches for measuring password strength

- NIST entropy estimate
- Shannon entropy

Today: strength meters based on guess ranks

Shannon Entropy

- Let $\mathcal{X}$ be password distribution
- Passwords are drawn iid from $\mathcal{X}$
- N is size of support of $\mathcal{X}$
- p_1 , p_2 , ..., p_N are probabilities of passwords in decreasing order

Shannon entropy:

$$H_1(\mathcal{X}) = \sum_{i=1}^{N} -p_i \log p_i$$

Poor Measure of Guessability

$N = 1{,}000{,}000$

$p_1 = 1 / 100$

$p_2 = (1 - 1/100)/999{,}999 \approx 1 / 2^{20}$

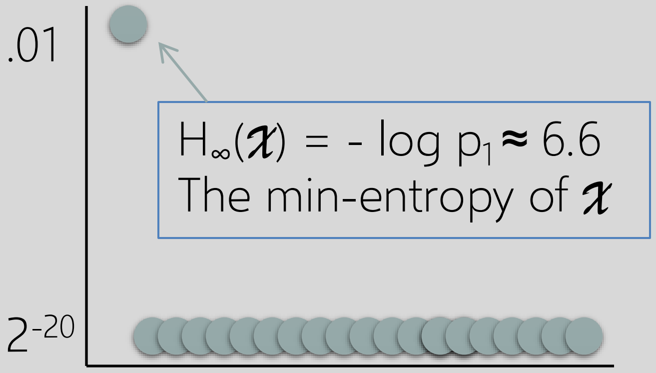
…

$p_N = (1 - 1/100)/999{,}999 \approx 1 / 2^{20}$

$H_1(\mathcal{X}) \approx 19$

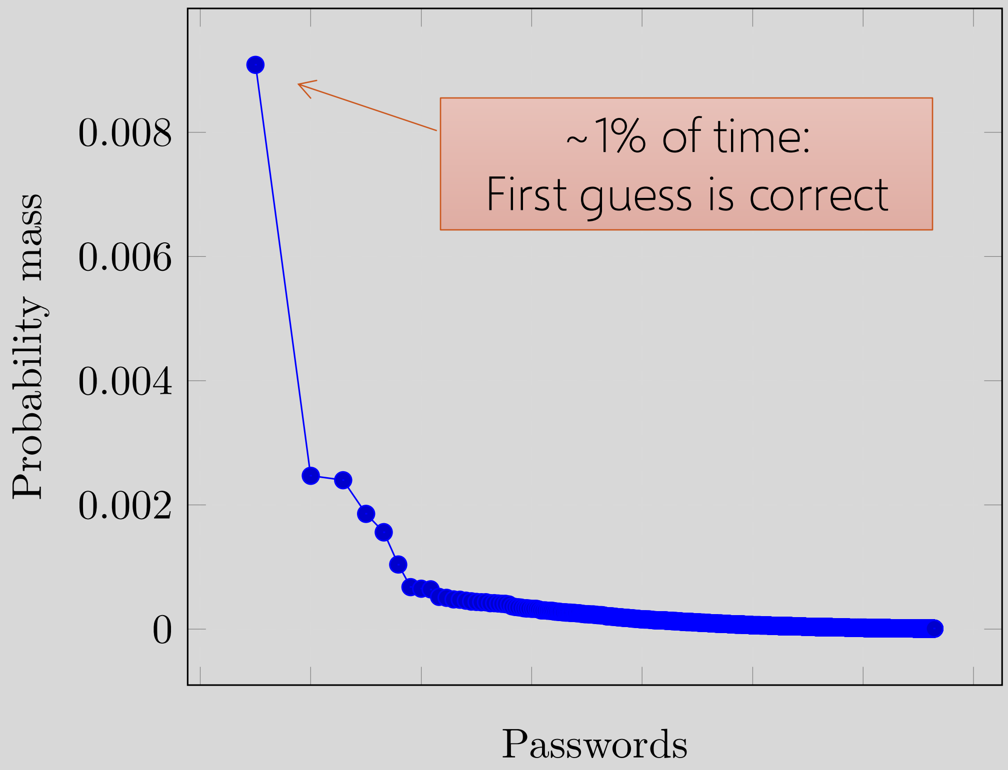
19 bits of "unpredictability". Probability of success about $1/2^{19}$?

What is probability of success if attacker makes one guess?



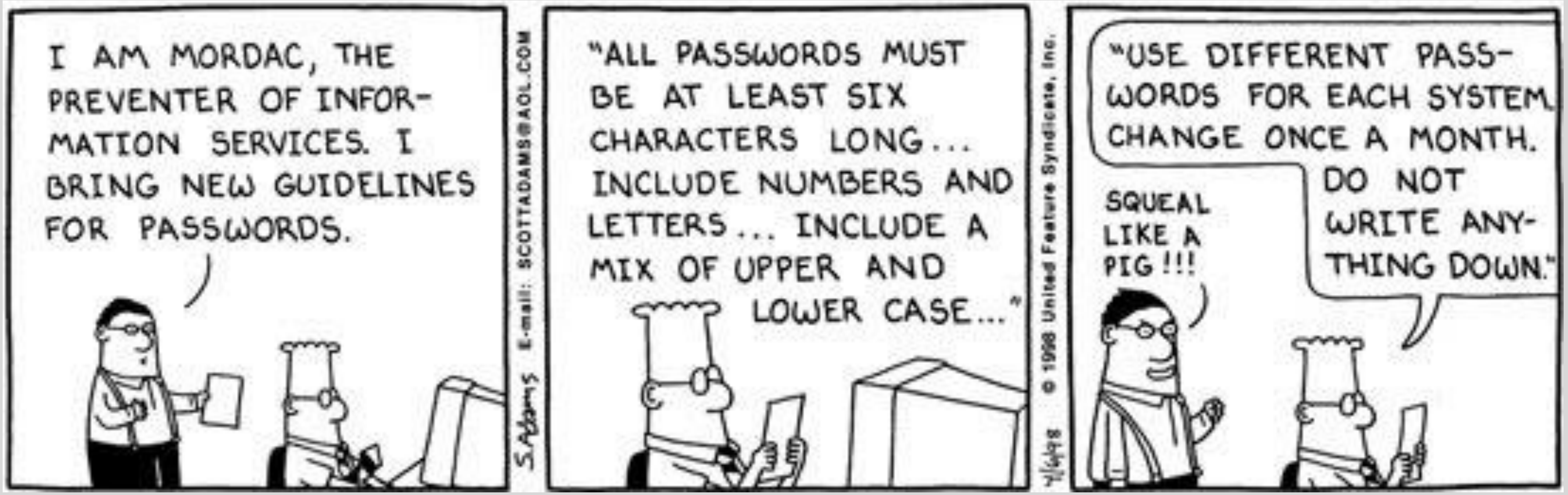
Shannon entropy is almost never a useful measure for security

RockYou Empirical Probability

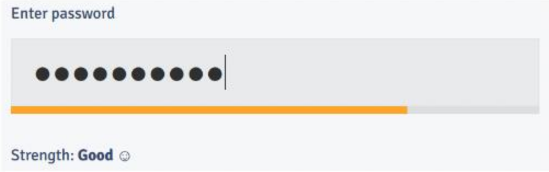


(Only first 5,000 points shown)

Password Policies



Password policies of the 120 most popular English-language websites

Interventions	Best practices from prior research	Our key findings
Blocklists 	• Do check users' passwords against lists of leaked and easily-guessed passwords [1, 2, 3, 4]. • Do reject the password if it appears on a blocklist, prompt the user to select a different password [1, 4].	• More than half (71 / 120) of websites do not check passwords at all, allowing all 40 of the most common passwords we tested (e.g., "12345678", "rockyou"). • 19 more websites block less than half of the most common passwords we tested.
Strength meters and minimum-strength requirements 	• Do provide real-time password strength estimates [5, 6, 7]. • Do set minimum-strength requirements by estimating guessability (the number of guesses it would take for an adversary to crack the password) [3, 8, 9, 10, 11].	• Only 23 / 120 websites used password strength meters. • Of those 23, 10 websites misuse meters as nudges toward specific types of characters and do not incorporate any notion of guessability.
Composition policies 	• Do not require specific character classes; let users freely construct passwords [2, 3, 7, 12]. • NIST: Do set a minimum-length of at least 8 characters.	• 54 / 120 sites still require specific character classes such as digits or special characters. • We devised a new method to measure the security and usability of composition policies. Based on our method, we found that all 120 policies performed poorly: none provided ≥ 60% security and usability simultaneously.

Lee et al. "Password policies of most top websites fail to follow best practices" (2022)

Restrictive Password Policies Don't Help

Overly restrictive password policies…

- 7 or 8 characters, at least 3 out of {digits, upper-case, lower-case, non-alphanumeric}, no dictionary words, change every 4 months, password may not be similar to previous 12 passwords…

… result in frustrated users and less security

- Burdens of devising, learning, forgetting passwords
- Users construct passwords insecurely, write them down
  - Can't use their favorite password construction techniques (small changes to old passwords, etc.)
  - "An item on my desk, then add a number to it"
- Heavy password re-use across systems

Inglesant and Sasse, "The True Cost of Unusable Password Policies"

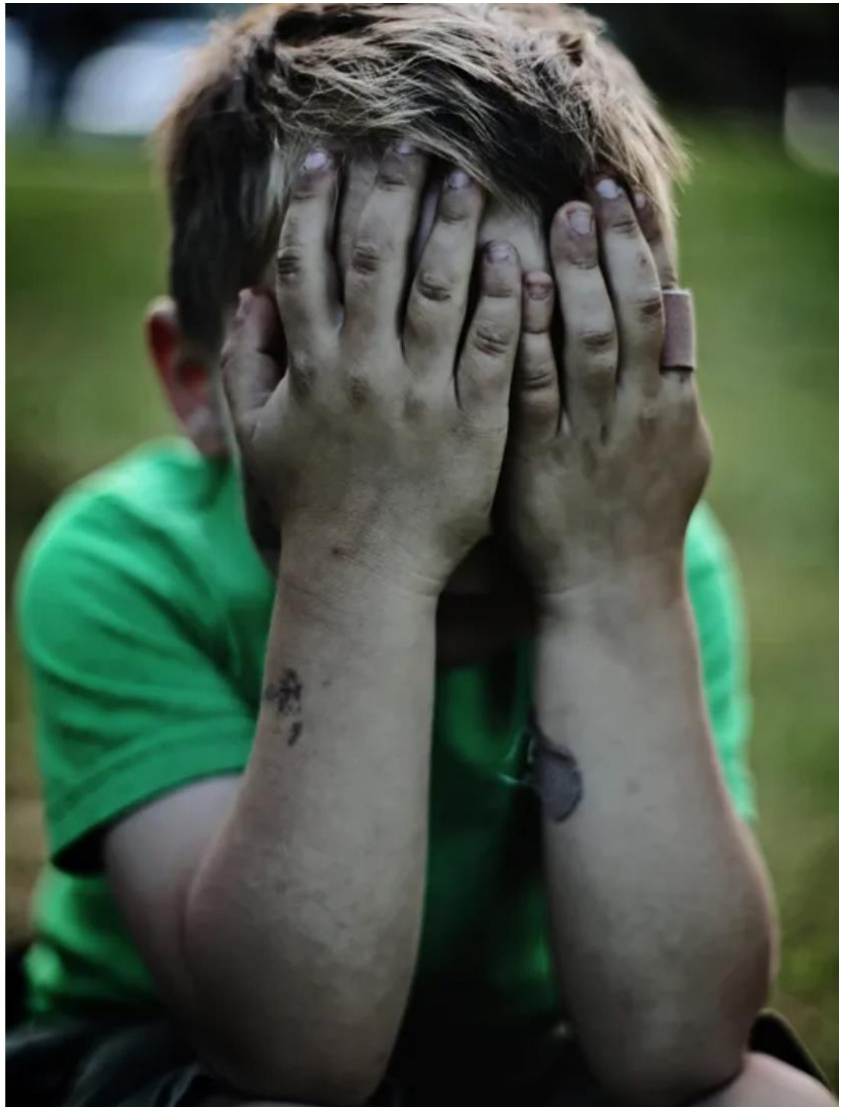
DPR

Know a site with dumb password rules? Contribute →

Dumb Password Rules

A compilation of 289 sites with dumb password rules.

View sites Contribute →



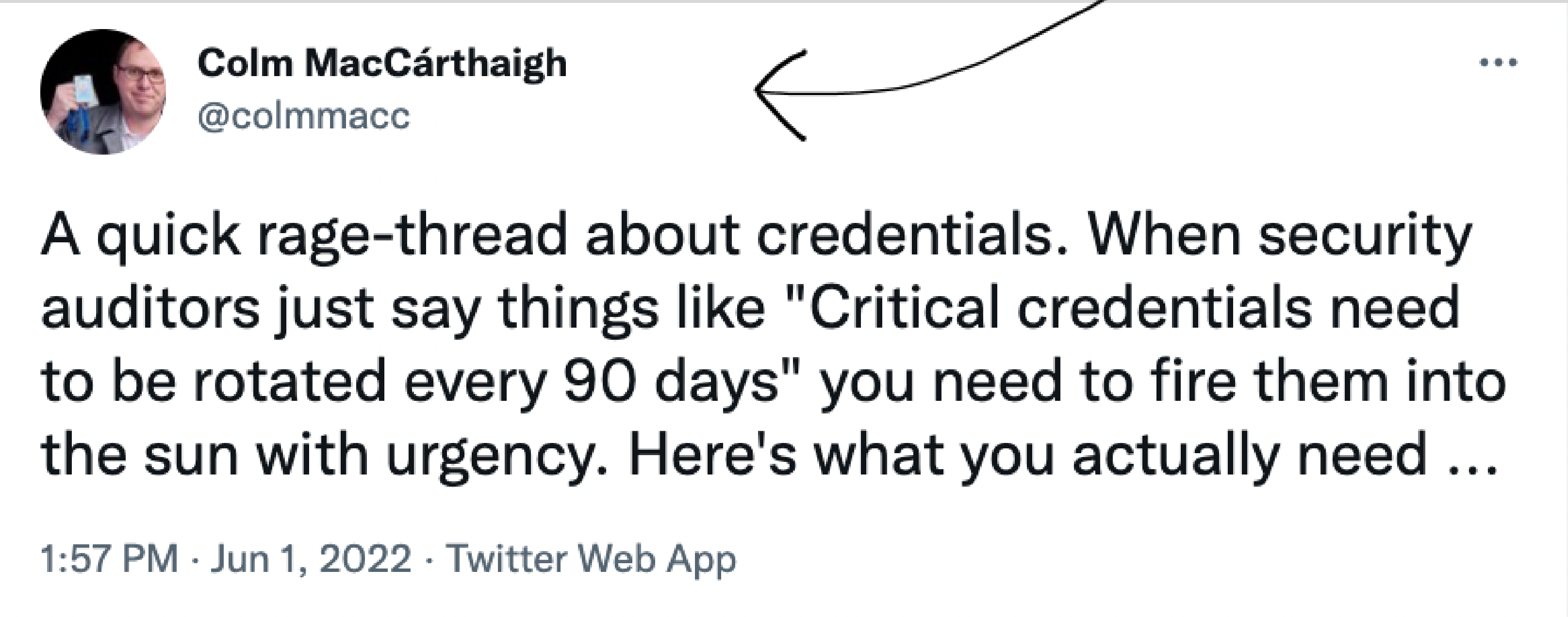
dumbpasswordrules.com

Password Management

5 minutes to brainstorm ideas for how to improve password-based authentication

Managing Credentials

VP and Distinguished Engineer at AWS
Works on identity and cryptography services


Colm MacCárthaigh
@colmmacc

A quick rage-thread about credentials. When security auditors just say things like "Critical credentials need to be rotated every 90 days" you need to fire them into the sun with urgency. Here's what you actually need ...

1:57 PM · Jun 1, 2022 · Twitter Web App

https://twitter.com/colmmacc/status/1532058883908198401

1. Rotation does nothing. It's revocation that matters. You always need a well-tested mechanism to make sure that you can remove or invalidate a credential that has been compromised.
2. Have closed loops. Deactivated credentials are a common source of outages. When introducing a new credential you see it everywhere it needs to be before using it. When you remove one, you need to see it gone from use before deactivating.
3. Logging and detective controls are key. You need to be able to see when and where a credential is being used. This is important for operational safety and security. How would you even detect a stolen credential without this?
4. Be INCREDIBLY wary of time-based expiry. Use only when there is no other option (e.g. public SSL certificates). There's really no way to win with time-based expiry. If your expiry time is something like a year, you don't get much security. Are you ok with an attacker using that cred for a year? So you still need revocation. If your expiry time is very short, like hours, are you *always* going to beat that renewal deadline? got good clocks?
5. Store credentials only where they are needed. This seems obvious but is rarely done. In particular it's common to see "treasure trove" secret-distribution control-planes that know all of the credentials.

https://twitter.com/colmmacc/status/1532058883908198401

6. If there is no reason to suspect credential disclosure or misuse, leave it alone. Replacing credentials usually exposes them to more systems, at least temporarily.
7. Asymmetric cryptography when you can, if not then choose between either memory-hard compute-hard hashing or derived-key symmetric auth depending on what fits your use-case. Avoid storing valuable secrets server side..
8. Keep credentials inside one-way enclaves like TPMs, TEEs, HSMs, when you can. Best line of defense is to keep credentials inaccessible.
9. If you can't write down a common password comparison side-channel from memory, do not implement your own authentication.
10. Check for all-zeroes creds, and repeated values. You can do this with hashing, you don't need to record the secrets. Coding errors, failures of entropy systems, and erasure mistakes are common enough to make this check worth doing.

All attacks on authentication we'll see in this course violate one or more of these rules

https://twitter.com/colmmacc/status/1532058883908198401

Hacker Group Says It Accessed Tesla's, Others' Internal Video-Surveillance Feeds

Exposed password to administrative account of security-camera vendor Verkada opened door to networks, hackers said

Tillie Kottmann, one of the hackers, said the group found a username and password for a Verkada administrative account on the internet, permitting them to obtain the footage. That included footage from 222 cameras placed inside various Tesla factories and warehouses, Kottmann said in a message.
In all, the group could have accessed material from 150,000 Verkada cameras

https://www.wsj.com/articles/hacker-group-says-it-accessed-teslas-others-internal-video-surveillance-feeds-11615396594

23andMe® BLOG SHOP LEARN ABOUT SIGN IN REGISTER KIT HELP

Information on 6.9 million users compromised: names, relationships, percentage of shared DNA…

+ Traits News Research Stories

Credential Stuffing Incident: What happened?

As our investigation comes to a close, we wanted to share the details of what took place and our findings.

In early October, we learned that a threat actor accessed a select number of individual 23andMe.com accounts through a process called credential stuffing. That is, usernames and passwords that were used on 23andMe.com were the same as those used on other websites that have been previously compromised or otherwise available. We do not have any indication that there was a data security incident within our systems, or that 23andMe was the source of the account credentials used in these attacks.

STRONTIUM Attacks

aka Fancy Bear, aka APT28, aka Sofacy
(GRU, Russian military intelligence)

Microsoft has tied STRONTIUM to a newly uncovered pattern of Office365 credential harvesting activity aimed at US and UK organizations directly involved in political elections

target: elections

…

spear-phishing to harvest credentials

password spraying

STRONTIUM relied heavily upon spear phishing in its credential harvesting efforts leading up to the 2016 US presidential election. In 2016, spear-phishing was the most common tactic for stealing credentials from targeted accounts. This time around, STRONTIUM appears to be taking a different approach, namely, brute-force/password-spray tooling. This shift in tactics, also made by several other nation-state actors, allows them to execute large-scale credential harvesting operations in a more anonymized manner. The tooling STRONTIUM is using routes its authentication attempts through a pool of approximately 1,100 IPs, the majority associated with the Tor anonymizing service.

cover tracks using Tor

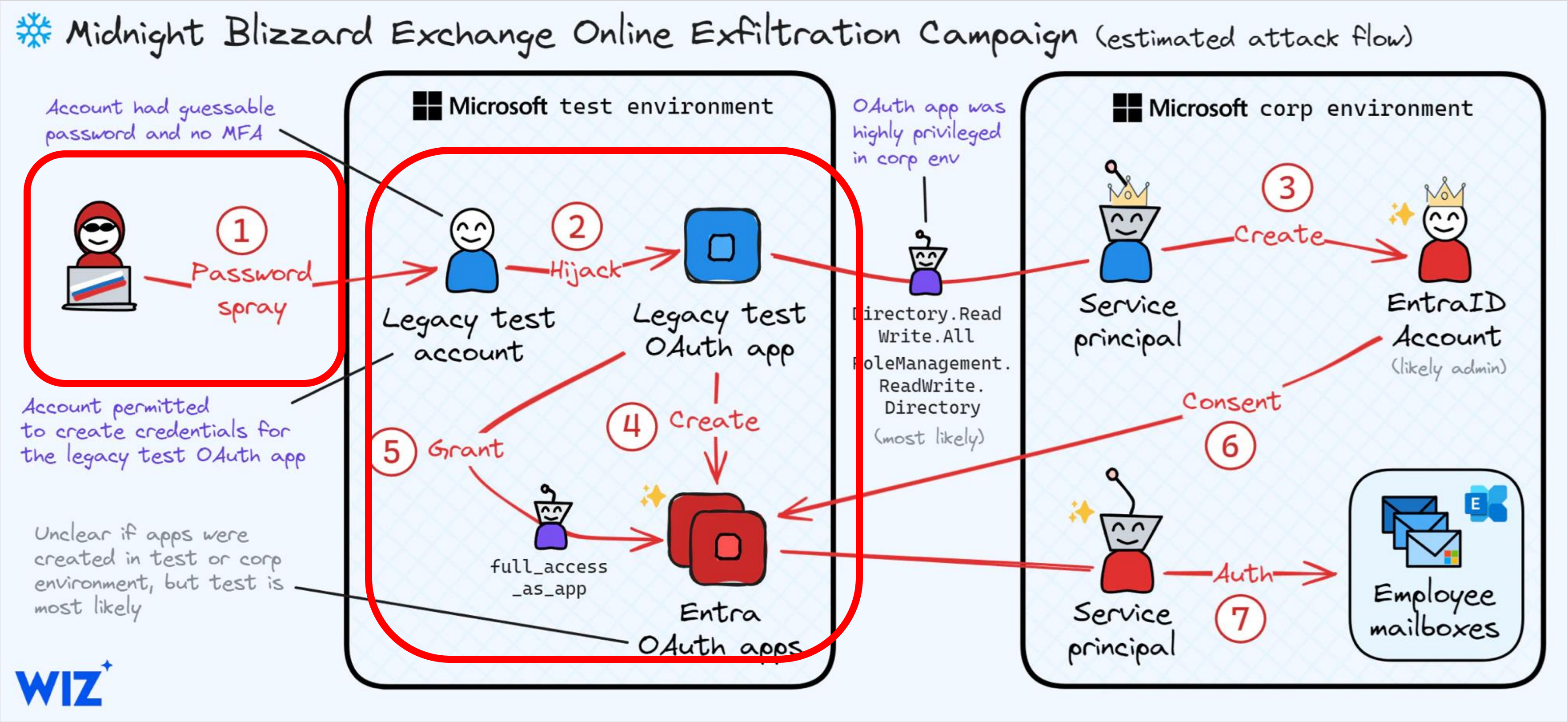
https://www.microsoft.com/security/blog/2020/09/10/strontium-detecting-new-patters-credential-harvesting/

Midnight Blizzard Attacks (2024)

Only a few requests to each account -- evades detection based on many failures

Only a slow rate of request from each residential IP -- evades detection based on volume

Legacy test account with OAuth privileges



Lateral move to take over OAuth

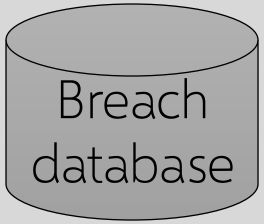
https://www.wiz.io/blog/midnight-blizzard-microsoft-breach-analysis-and-best-practices

Preventing Credential Stuffing and Spraying

Attacker tries multiple credentials from known breaches

`POST /login.html?name=bob&pw=12345`

Is (Bob, 12345) in a public breach?
If yes, ask user to choose new password



Third-party services for making such queries:

- HaveIBeenPwned
- Google password checker

Have I Been Pwned

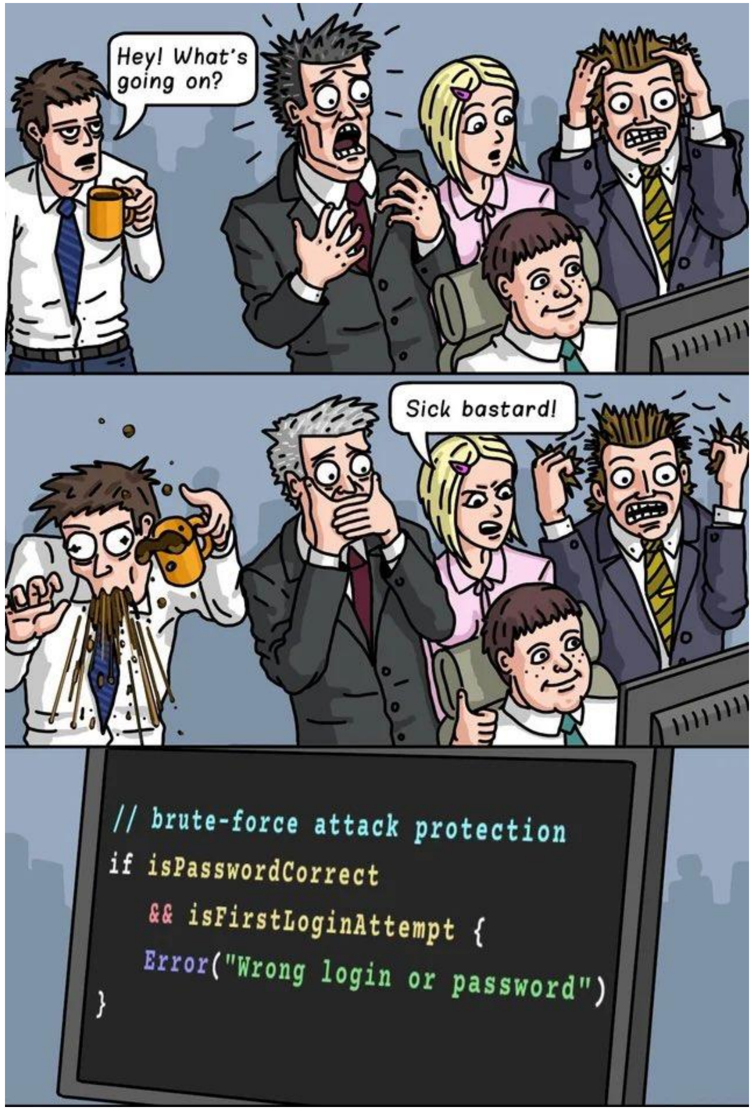
556	11,454,726,823	114,131	207,749,076
pwned websites	pwned accounts	pastes	paste accounts

Largest breaches

772,904,991	Collection #1 accounts
763,117,241	Verifications.io accounts
711,477,622	Onliner Spambot accounts
622,161,052	Data Enrichment Exposure From PDL Customer accounts
593,427,119	Exploit.In accounts
509,458,528	Facebook accounts
457,962,538	Anti Public Combo List accounts
393,430,309	River City Media Spam List accounts
359,420,698	MySpace accounts
268,765,495	Wattpad accounts

Recently added breaches

20,154,583	IndiaMART accounts
878,209	Imavex accounts
6,137,666	SubaGames accounts
2,789,609	Eatigo accounts
1,304,447	OrderSnapp accounts
2,660,295	MMG Fusion accounts
2,743,539	Audi accounts
112,031	Guntrader accounts
505,466	Short Édition accounts
30,433	Vastaamo accounts


Hey! What's going on?
Sick bastard!
// brute-force attack protection
if isPasswordCorrect
&& isFirstLoginAttempt {
Error("Wrong login or password")
}

Credential Tweaking Attacks

Suppose user changes password to 123456

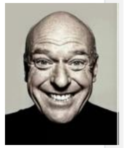
Credential stuffing no longer works, but guessing attacker could try variants of 12345

Deep learning techniques to learn conditional probability distribution

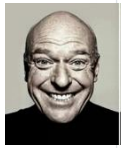
- p(pw' | pw) where pw is leaked password, pw' is variant
- Trained from leak data to capture typical password variants

Experiments showed that 1,316 Cornell accounts vulnerable (Pal et al. 2019)

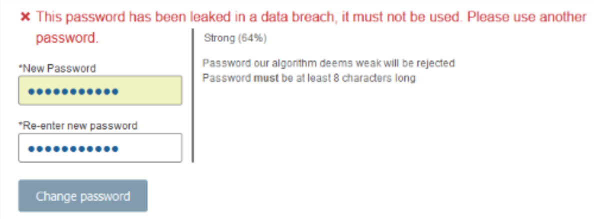
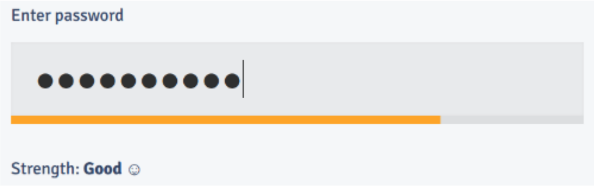
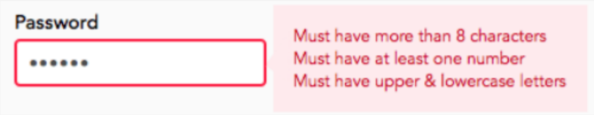
Check against leaked and easily-guessed passwords



Provide real-time strength estimates when users set their passwords



Do not require specific characters

Interventions	Best practices from prior research	Our key findings
Blocklists  	• Do check users' passwords against lists of leaked and easily-guessed passwords [1, 2, 3, 4]. • Do reject the password if it appears on a blocklist, prompt the user to select a different password [1, 4].	• More than half (71 / 120) of websites do not check passwords at all, allowing all 40 of the most common passwords we tested (e.g., "12345678", "rockyou"). • 19 more websites block less than half of the most common passwords we tested.
Strength meters and minimum-strength requirements  	• Do provide real-time password strength estimates [5, 6, 7]. • Do set minimum-strength requirements by estimating guessability (the number of guesses it would take for an adversary to crack the password) [3, 8, 9, 10, 11].	• Only 23 / 120 websites used password strength meters. • Of those 23, 10 websites misuse meters as nudges toward specific types of characters and do not incorporate any notion of guessability.
Composition policies  	• Do not require specific character classes; let users freely construct passwords [2, 3, 7, 12]. • NIST: Do set a minimum-length of at least 8 characters.	• 54 / 120 sites still require specific character classes such as digits or special characters. • We devised a new method to measure the security and usability of composition policies. Based on our method, we found that all 120 policies performed poorly: none provided ≥ 60% security and usability simultaneously.

https://passwordpolicies.cs.princeton.edu/

Hackers breached Colonial Pipeline with one compromised password

The password has since been discovered inside a batch of leaked passwords on the dark web.

Hackers gained entry into the networks of Colonial Pipeline Co. on April 29 through a virtual private network account, which allowed employees to remotely access the company's computer network

...

The account's password has since been discovered inside a batch of leaked passwords on the dark web. That means a Colonial employee may have used the same password on another account that was previously hacked

...

The VPN account, which has since been deactivated, didn't use multifactor authentication, a basic cybersecurity tool, allowing the hackers to breach Colonial's network using just a compromised username and password.

https://www.aljazeera.com/economy/2021/6/4/hackers-breached-colonial-pipeline-with-one-compromised-password

This Agency's Computers Hold Secrets. Hackers Got In With One Password.

Hackers used one worker's login information to penetrate the Law Department's network after officials failed to implement a simple security measure.

New York City's Law Department holds some of the city's most closely guarded secrets: evidence of police misconduct, the identities of young children charged with serious crimes, plaintiffs' medical records and personal data for thousands of city employees.

...

the hack was enabled by the Law Department's failure to implement a basic safeguard, known as multifactor authentication, more than two years after the city began requiring it

https://www.nytimes.com/2021/06/18/nyregion/nyc-law-department-hack.html

UNC5537 Targets Snowflake Customer Instances for Data Theft and Extortion

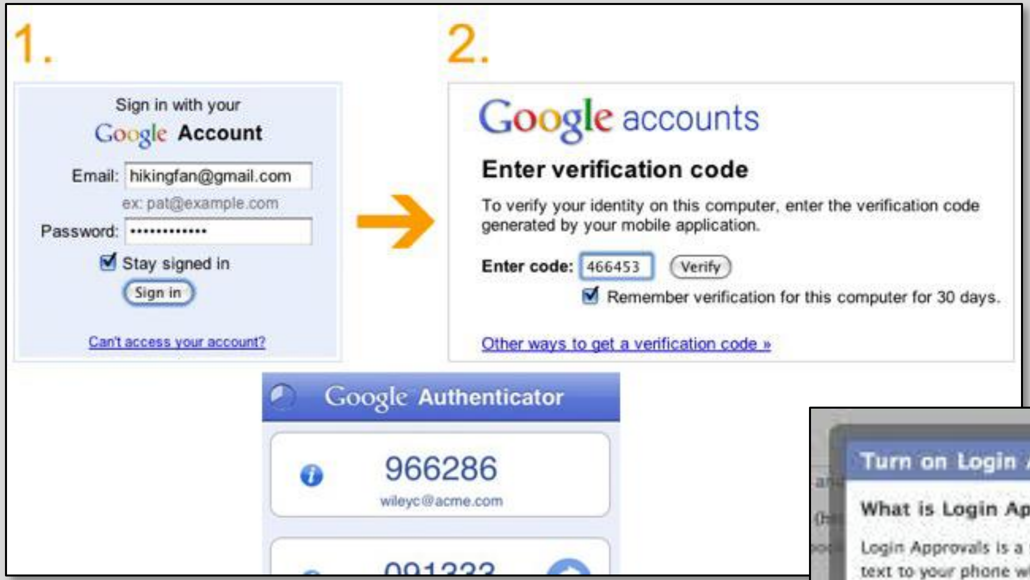
June 10, 2024

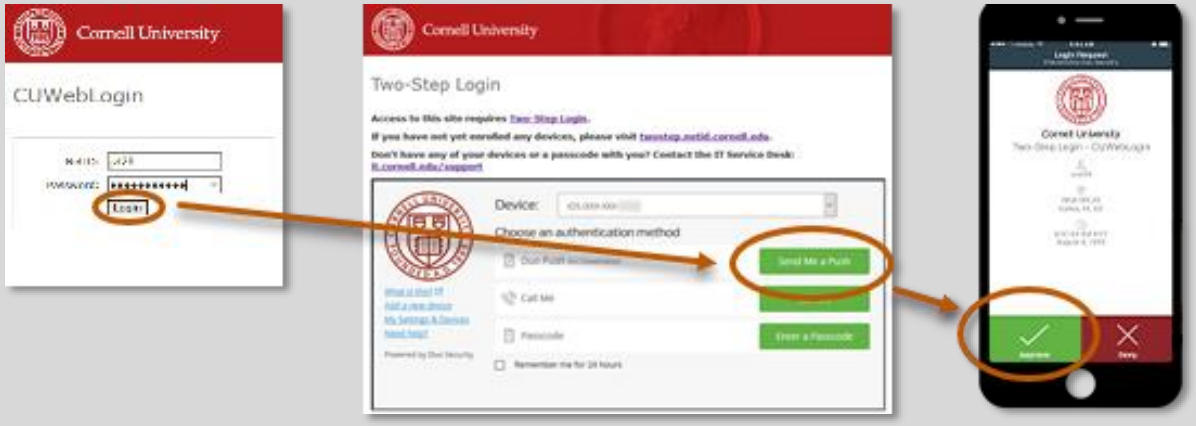
Major cloud storage and data analytics company

- 1.3 TB of Ticketmaster data (over 560 million names, addresses, credit card numbers)
- 30 million Santander bank accounts and 28 million credit card numbers

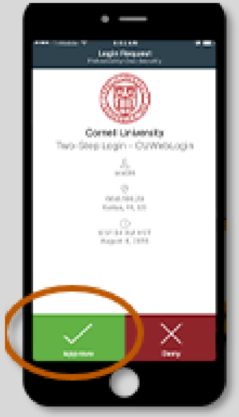
"The Snowflake platform allows customers to oversee their security environments, and didn't require its customers to set up multi-factor authentication (MFA)."

Multi-Factor Authentication





Authentication Factors



Combine passwords with another way to authenticate user

Second factor is usually proof of ownership of …

- Email address
- Telephone number (via SMS)
- Device (via authenticator app)
- Hardware token (one-time-password token, universal second factor U2F token)

Effectiveness of 2FA

Microsoft: 99.9% of compromised accounts did not use multi-factor authentication

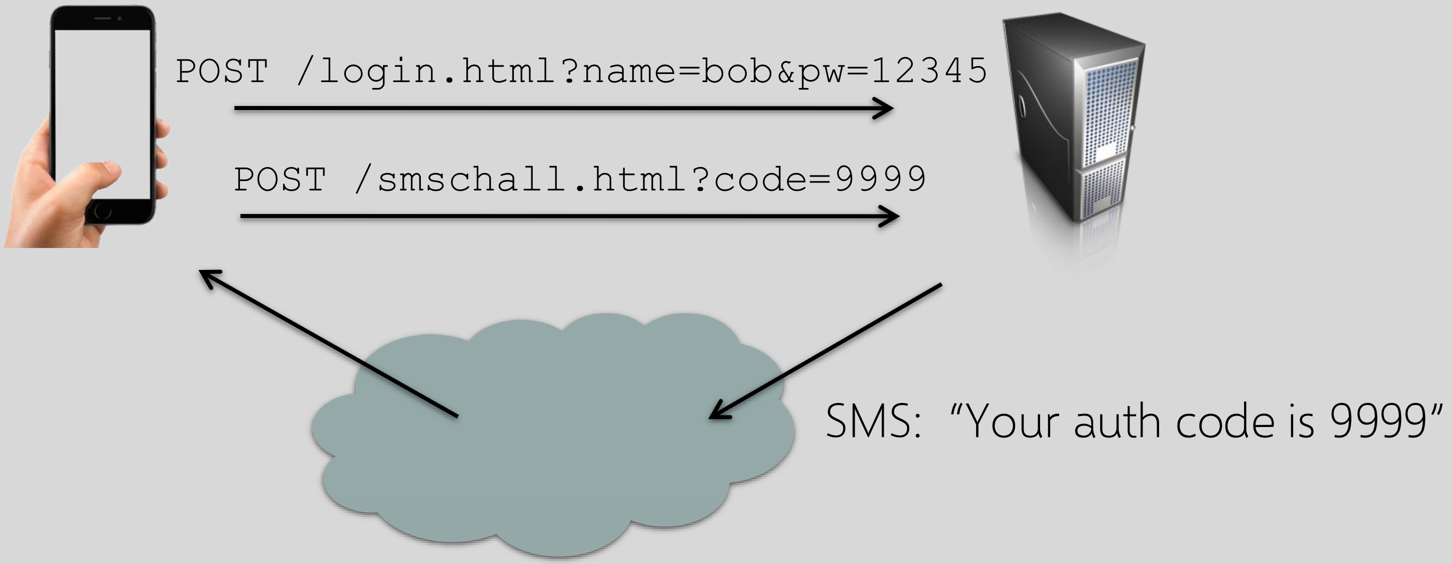
Only 11% of all enterprise accounts use a MFA solution overall.

Microsoft report, Mar 2020

successfully auto-enabled 2SV for over 150 million people, and we've also required it for over 2 million of our YouTube creators. As a result of this effort, we have seen a **50% decrease in accounts being compromised** among those users.

Google report, Feb 2022

SMS Authentication



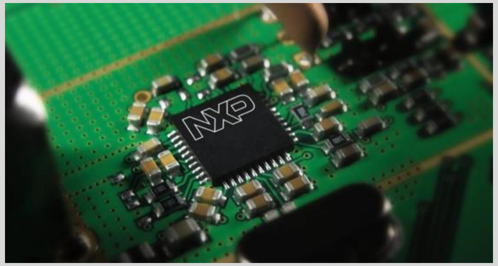
Suppose you know someone's password (e.g., due to breach) but their account is protected by SMS-based 2FA. What can you do as an attacker?

Circumventing SMS-Based 2FA

- Have physical access to device that receives SMS
- Phishing attacks: confuse or trick user into disclosing SMS to you
- SIM swap: trick phone company into registering victim's phone # to your device
- SMS hijacking: exploit vulnerabilities in cellular network
  - https://berlin.ccc.de/~tobias/31c3-ss7-locate-track-manipulate.pdf
  - [Doerfler et al. 2019]: SMS 2FA circumvented in ~4% of phishing attacks, ~26% of targeted attacks
- Better practice: authenticator app or hardware token

Hackers spent 2+ years looting secrets of chipmaker NXP before being detected

Chimera has extensive experience stealing data from a wide range of companies. The threat actor uses a variety of means to compromise its victims. In the campaign that hit NXP, hackers often leveraged account information revealed in previous data breaches of sites such as LinkedIn or Facebook. The data allowed Chimera to guess the passwords that employees used to access VPN accounts. Team members were able to bypass multi-factor authentication by changing telephone numbers associated with the accounts.



https://arstechnica.com/security/2023/11/hackers-spent-2-years-looting-secrets-of-chipmaker-nxp-before-being-detected/

SMS Rerouting

A Hacker Got All My Texts for $16

A gaping flaw in SMS lets hackers take over phone numbers in minutes by simply paying a company to reroute text messages.

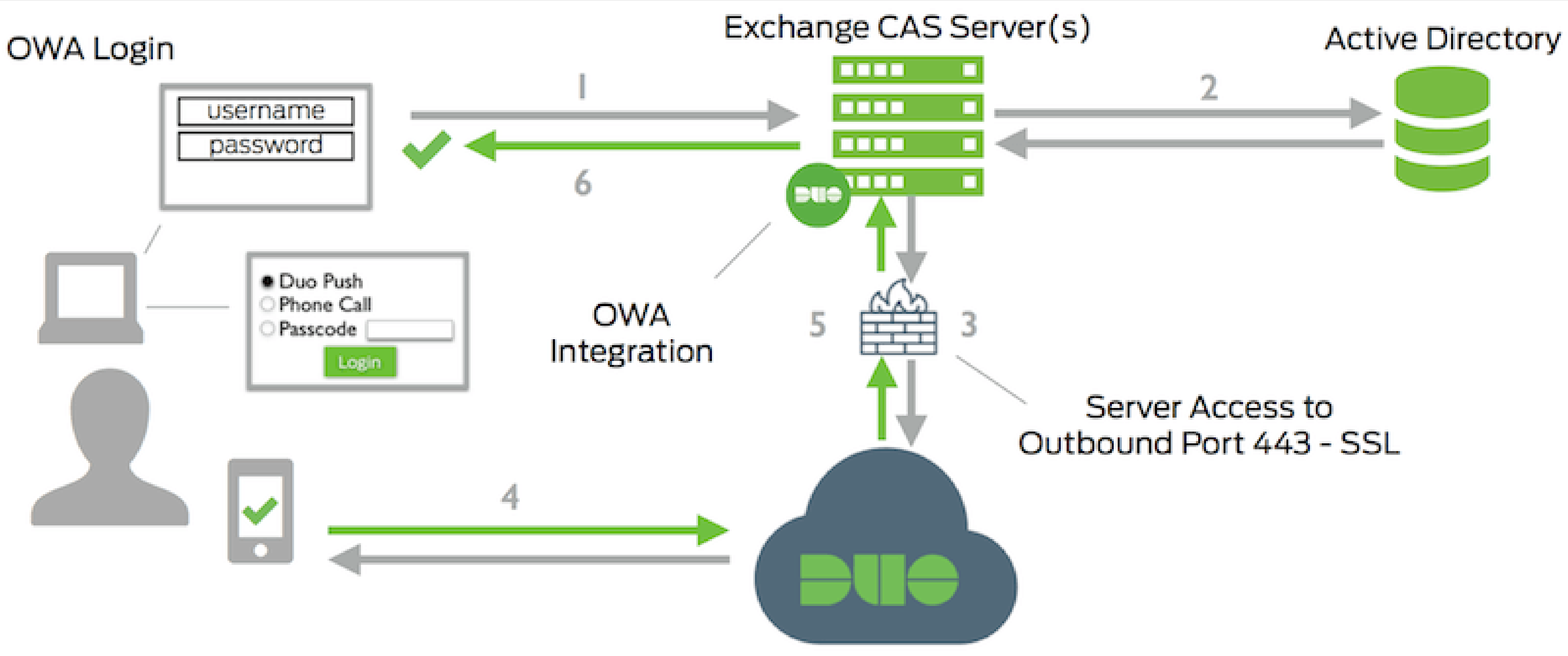
The OSR database is a core component of the message routing infrastructure in North America … It is known as an "override registry" as it enables an individual subscriber to receive messaging services from a different provider than voice services.

"I used a prepaid card to buy their $16 per month plan and then after that was done it let me steal numbers just by filling out LOA info with fake info," Lucky225 added, referring to a Letter of Authorization, a document saying that the signer has authority to switch telephone numbers.

Not SIM swapping or phone number hijacking
The victim doesn't notice (phone service not interrupted)

https://www.vice.com/en/article/y3g8wb/hacker-got-my-texts-16-dollars-sakari-netnumber

Duo 2FA Authentication



https://duo.com/docs/owa

Uber Hacked by Lapsus$ (September 2022)

External contractor
(more about vendor security later)

An Uber EXT contractor had their account compromised by an attacker. It is likely that the attacker purchased the contractor's Uber corporate password on the dark web, after the contractor's personal device had been infected with malware, exposing those credentials. The attacker then repeatedly tried to log in to the contractor's Uber account. Each time, the contractor received a two-factor login approval request, which initially blocked access. Eventually, however, the contractor accepted one, and the attacker successfully logged in.

From there, the attacker accessed several other employee accounts which ultimately gave the attacker elevated permissions to a number of tools, including G-Suite and Slack. The attacker then posted a message to a company-wide Slack channel, which many of you saw, and reconfigured Uber's OpenDNS to display a graphic image to employees on some internal sites.

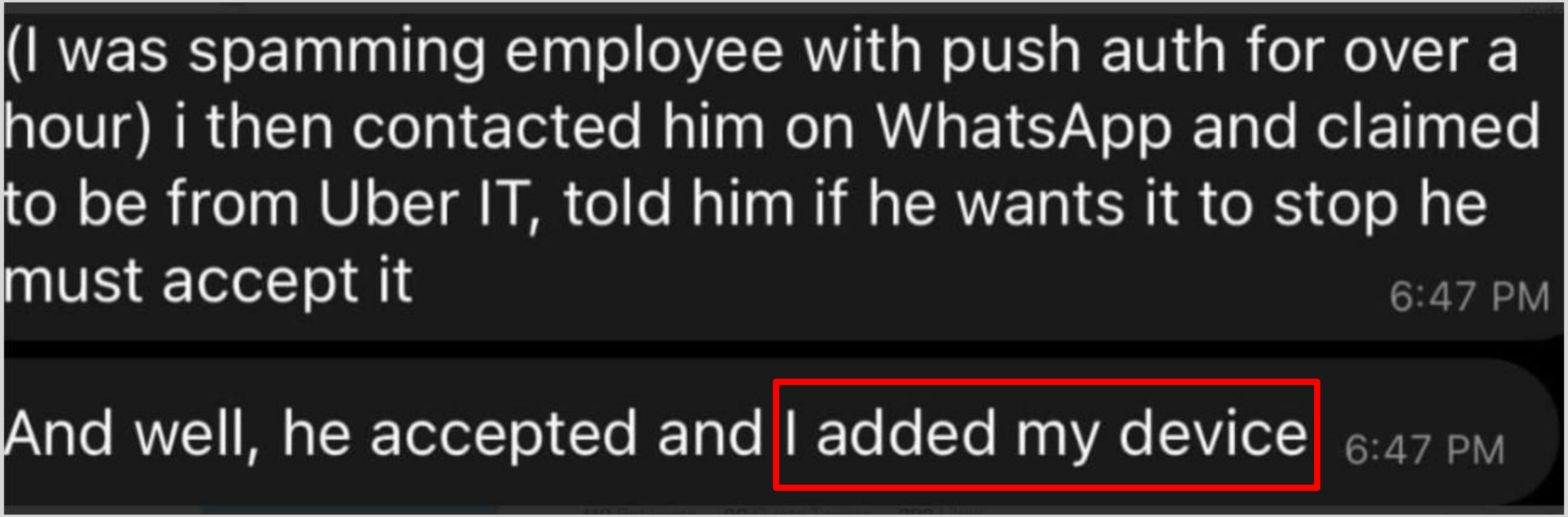
Stolen credentials
purchased on Dark Web

Flood of MFA requests,
one eventually accepted

Access other accounts,
ultimately gaining access
go G-Suite and Slack

https://www.uber.com/newsroom/security-update/

Bypassing MFA



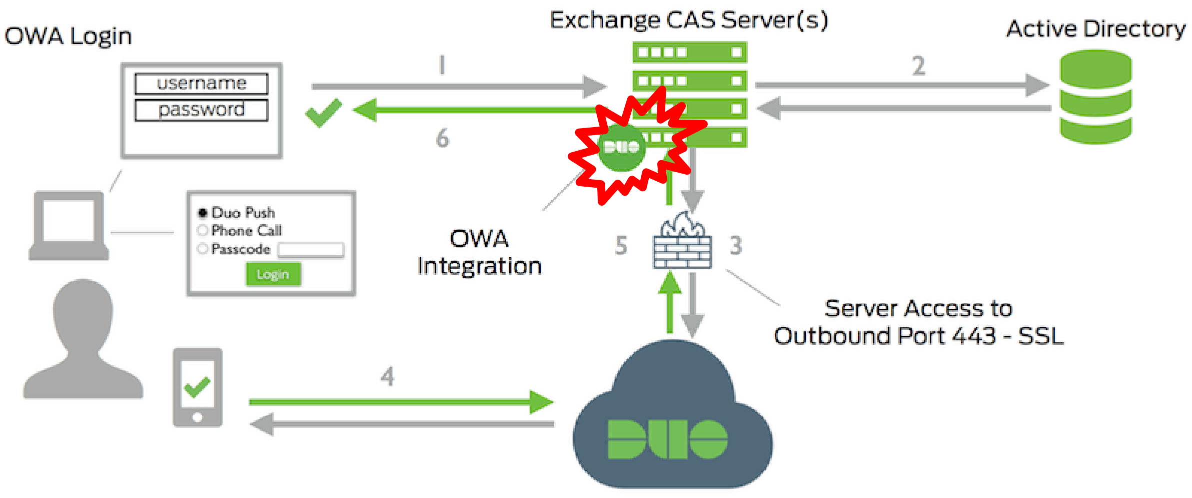
Attacker added their
own device for MFA

Source: https://mobile.twitter.com/BillDemirkapi/status/1570799440868552706/

2020 SolarWinds Hack

- Compromised computer networks across the US government
  - Pentagon, State, Treasury, Energy, Justice, Commerce, Labor, DHS, NIH …
- Many state and local governments
- Many corporations
  - Microsoft, Intel, Cisco, network security firms such as FireEye
- 18,000 customers in total

SolarWinds hackers have a clever way to bypass multifactor authentication

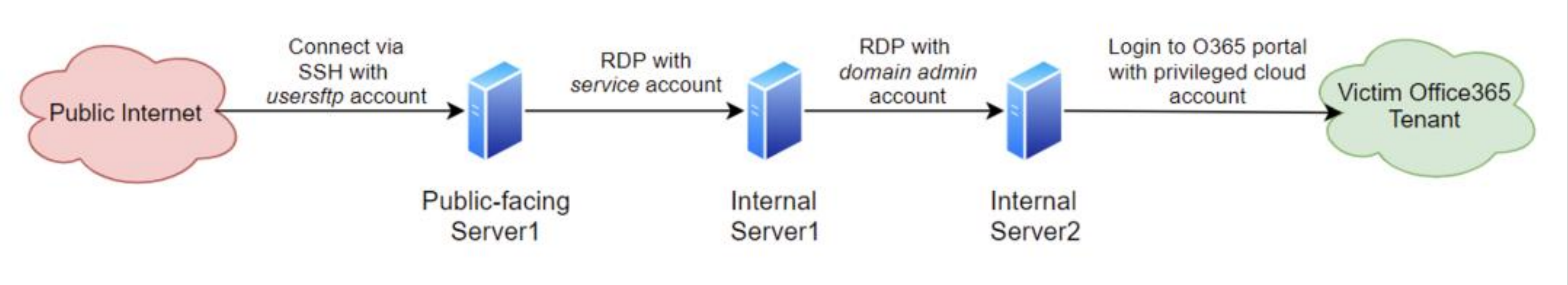


... the attacker had accessed the Duo integration secret key (akey) from the OWA server. This key then allowed the attacker to derive a pre-computed value to be set in the duo-sid cookie. After successful password authentication, the server evaluated the duo-sid cookie and determined it to be valid. This allowed the attacker with knowledge of a user account and password to then completely bypass the MFA set on the account.

More about Web authentication later

https://arstechnica.com/information-technology/2020/12/solarwinds-hackers-have-a-clever-way-to-bypass-multi-factor-authentication/

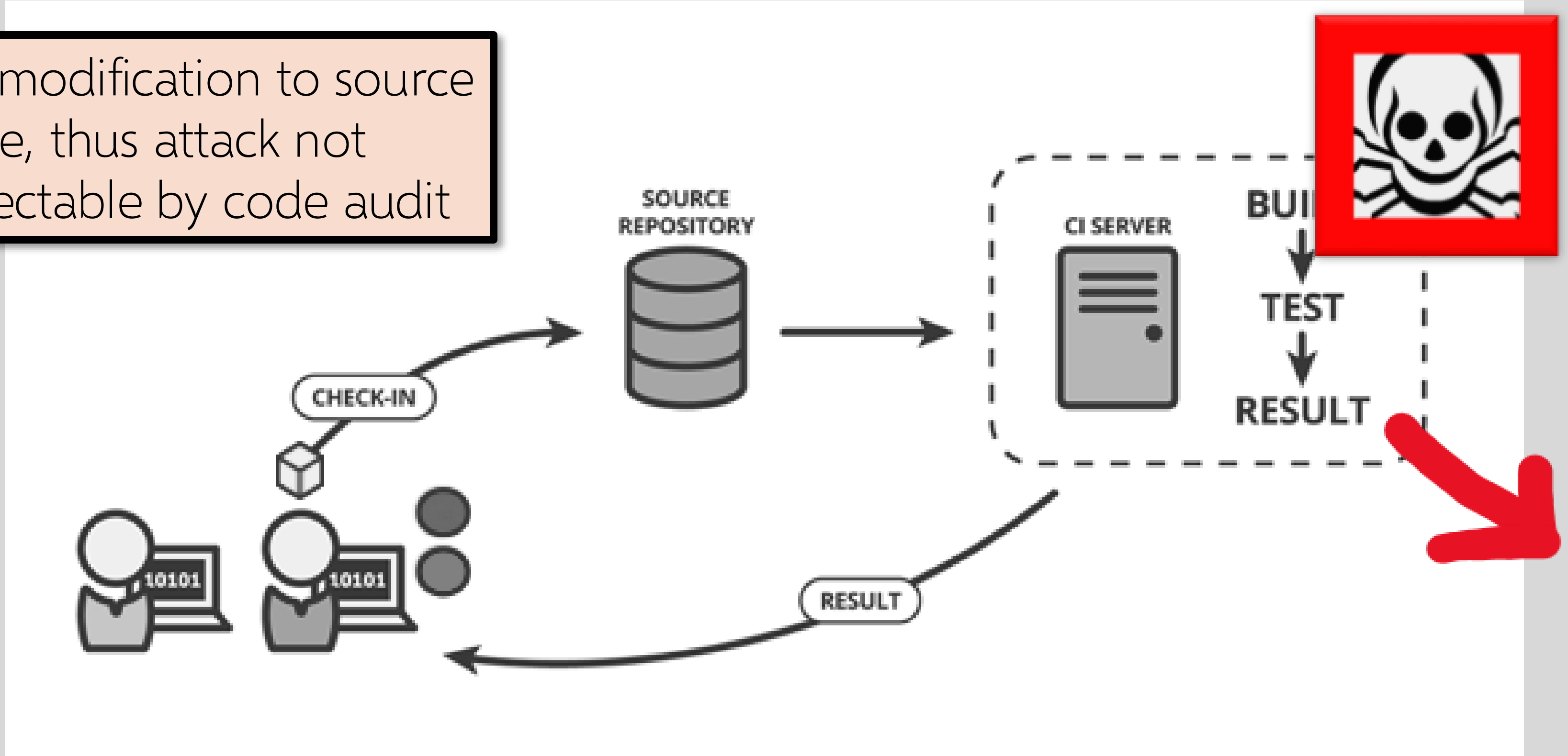
Credential Hopping (SolarWinds Hack)



https://www.crowdstrike.com/blog/observations-from-the-stellarparticle-campaign/

Software Development: Continuous Integration

No modification to source code, thus attack not detectable by code audit



Malicious functionality introduced into the executable code during the build process

Deployed to all customers of Orion network management product

Image: https://techbeacon.com/app-dev-testing/are-you-really-doing-continuous-integration-heres-how-tell

Over 90 percent of Gmail users still don't use two-factor authentication

The security tool adds another layer of security if your password has been stolen

By Thuy Ong | @ThuyOng | Jan 23, 2018, 8:30am EST

Usability remains a key issue preventing adoption

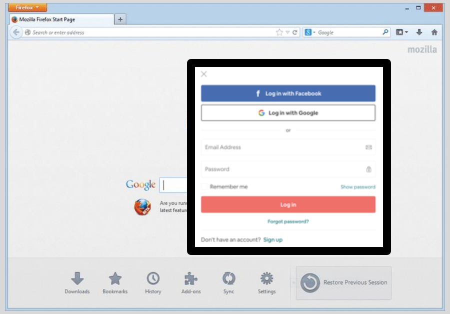
Other Authentication Signals

- Location-based authentication
  - IP-based geolocation
- Device identification
  - Cookies, device fingerprinting
- Behavioral cues
  - Typical actions on platform (even after authenticated)
- Biometrics
  - Fingerprints, etc

Single Sign-On (SSO)

Identity provider handles authentication

- Google, Facebook, proprietary services, etc.



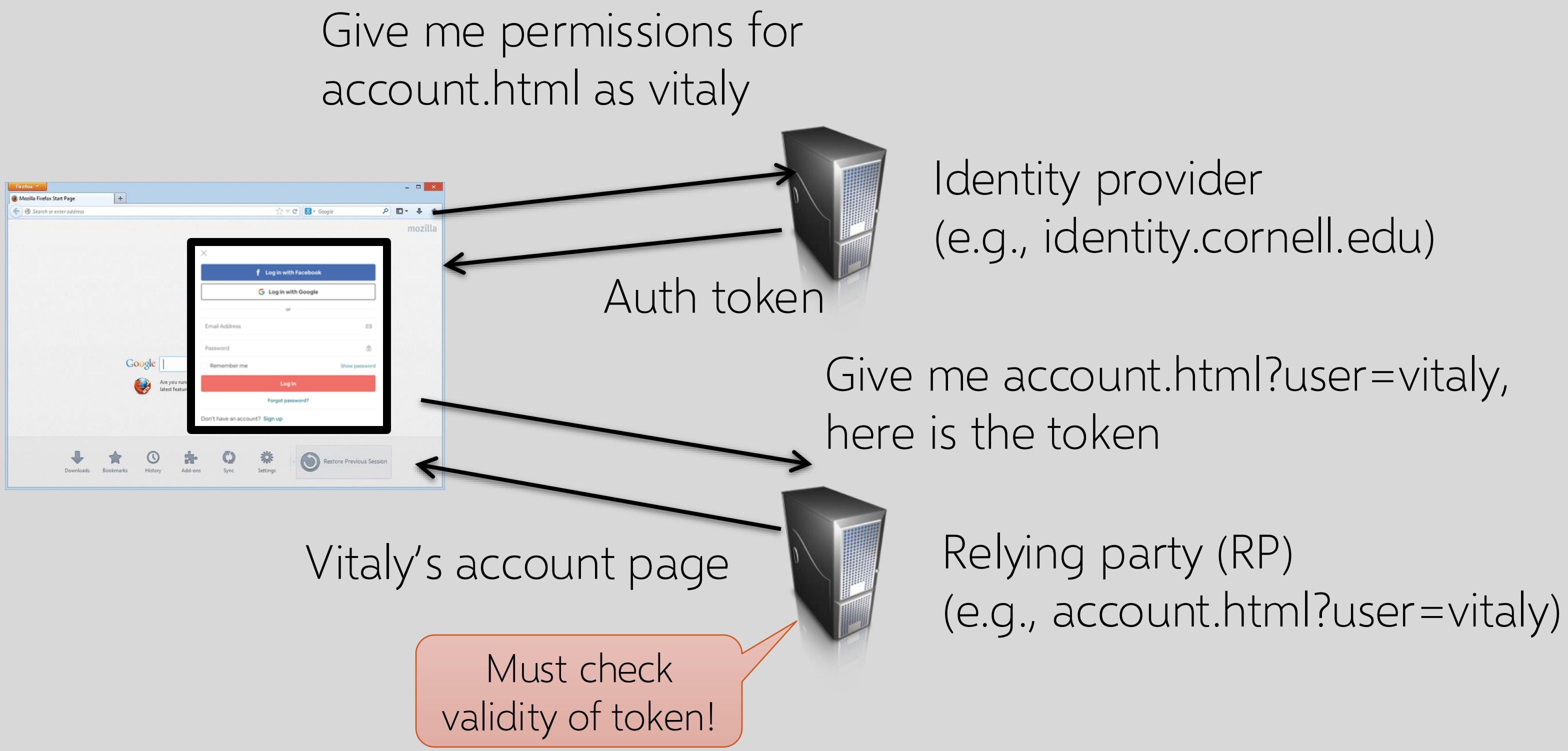
Identity provider
(e.g., identity.cornell.edu)

Relying party (RP)
(e.g., account.html?user=vitaly)

<u>In-class 5-minute exercise:</u>
How would you securely authorize browser to access www.cornell.edu/account.html?user=vitaly based on authentication to identity.cornell.edu?

Single Sign-On (SSO)

Many standards and systems: SAML, OpenID Connect + OAuth 2.0, …



OAuth 2.0

Widely used authorization protocol standard

Common in Web and mobile apps

Two types of “authorization grants”

- **Authorization code:** used by server-side apps to access resources
- **Implicit:** used by client-side apps (JavaScript, mobile apps, etc.)

https://www.digitalocean.com/community/tutorials/an-introduction-to-oauth-2

OAuth 2.0 Implicit Flows

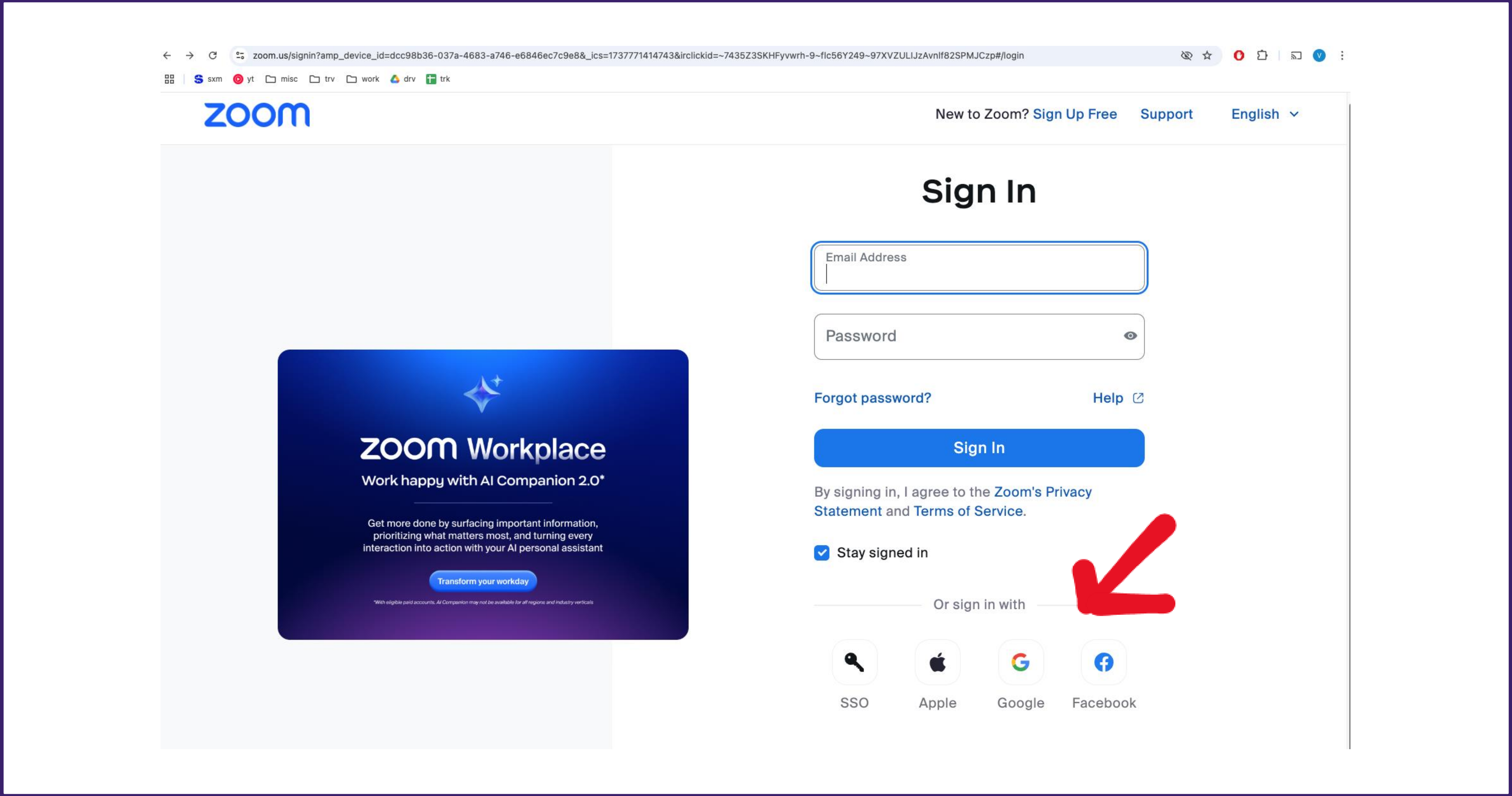
Request triggers redirect to authorization request

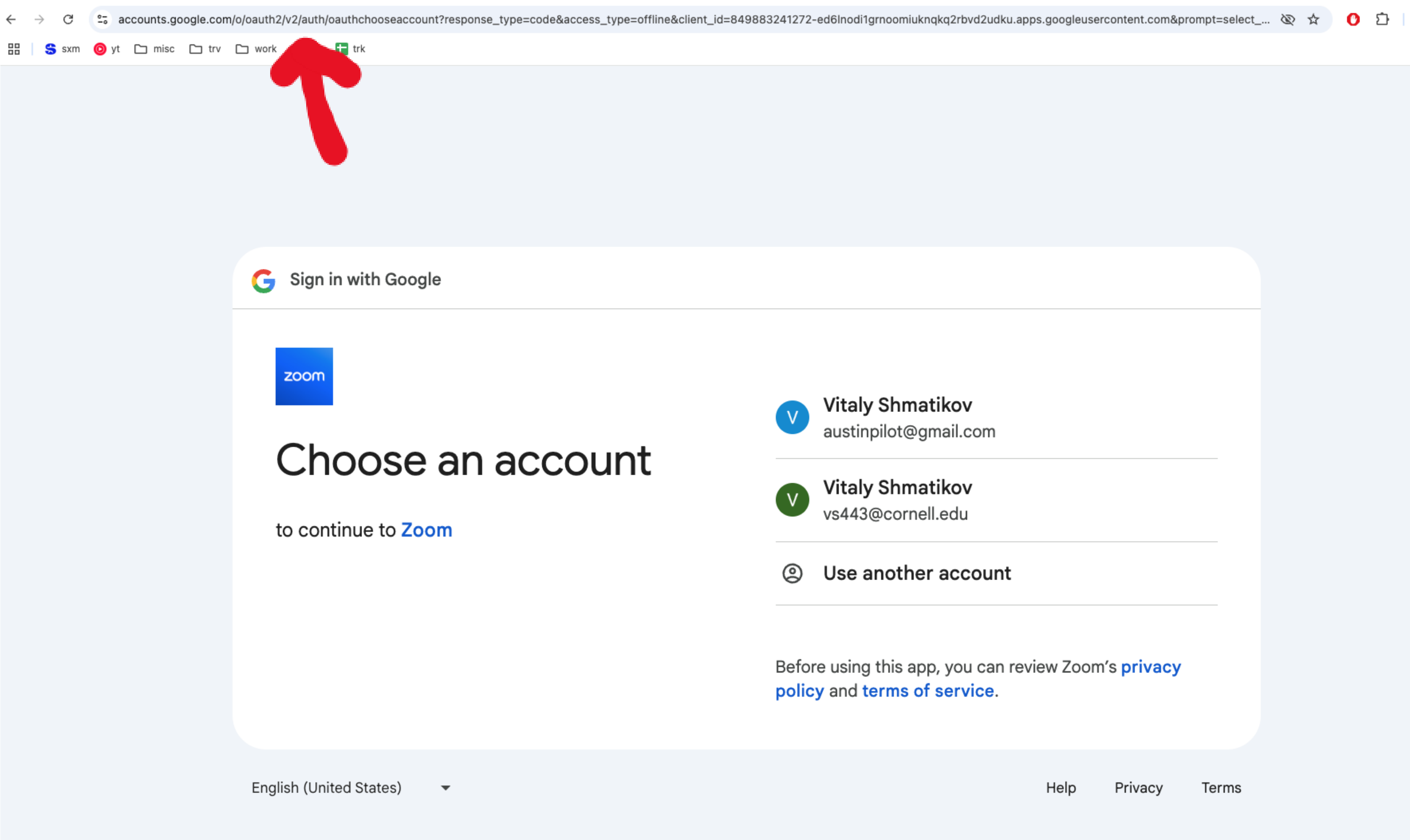
```
https://authserv.com/authorize?response_type=code &
                               client_id=CLIENT_ID &
                               redirect_uri=https://myapp.com/callback &
                               scope=read
```

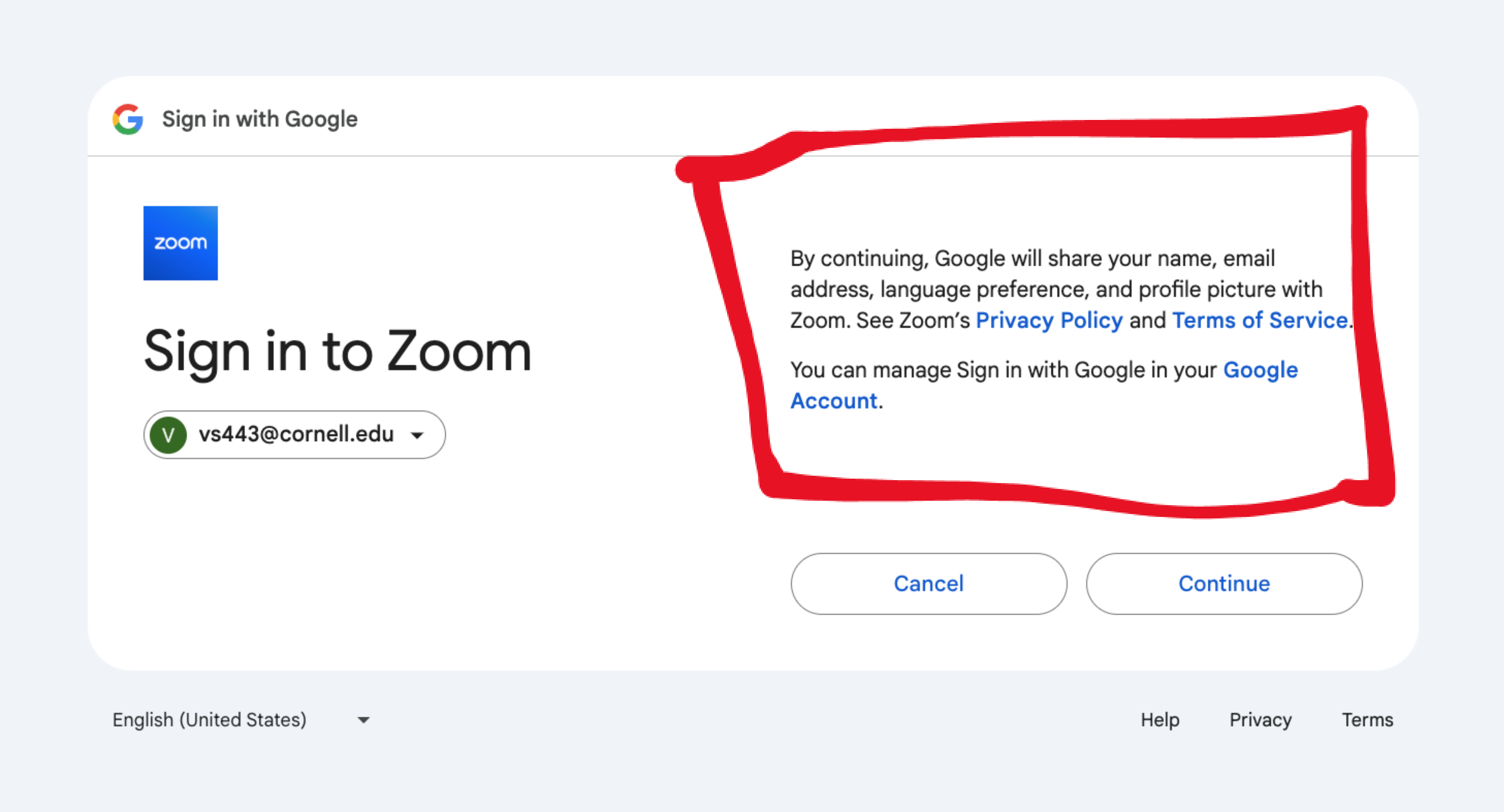
Redirects browser via redirect URI, with an auth token

```
https://myapp.com/callback?token=ACCESS_TOKEN
```

Now client-side can use this token to access resource


zoom.us/signin?amp_device_id=dcc98b36-037a-4683-a746-e6846ec7c9e8&_ics=1737771414743&irclickid=~7435Z3SKHFyvwrh-9~flc56Y249~97XVZULIJzAvnlf82SPMJCzp#/login
sxm
yt
misc
trv
work
drv
trk
zoom
New to Zoom? Sign Up Free
Support
English
zoom Workplace
Work happy with AI Companion 2.0*
Get more done by surfacing important information, prioritizing what matters most, and turning every interaction into action with your AI personal assistant
Transform your workday
Sign In
Email Address
Password
Forgot password?
Help
Sign In
By signing in, I agree to the Zoom's Privacy Statement and Terms of Service.
Stay signed in
Or sign in with
SSO
Apple
Google
Facebook


accounts.google.com/o/oauth2/v2/auth/oauthchooseaccount?response_type=code&access_type=offline&client_id=849883241272-ed6lnodi1grnoomiuknqkq2rbvd2udku.apps.googleusercontent.com&prompt=select_...
sxm
yt
misc
trv
work
trk
Sign in with Google
zoom
Choose an account
to continue to Zoom
Vitaly Shmatikov
austinpilot@gmail.com
Vitaly Shmatikov
vs443@cornell.edu
Use another account
Before using this app, you can review Zoom's privacy policy and terms of service.
English (United States)
Help
Privacy
Terms


Sign in with Google
zoom
Sign in to Zoom
V vs443@cornell.edu
By continuing, Google will share your name, email address, language preference, and profile picture with Zoom. See Zoom's Privacy Policy and Terms of Service.
You can manage Sign in with Google in your Google Account.
Cancel
Continue
English (United States)
Help
Privacy
Terms

Strengthening Passwords

Add biometrics

- For example, keystroke dynamics or voiceprint
- Revocation is often a problem with biometrics

Graphical passwords

- Goal: increase the size of memorable password space
- Dictionary attacks are believed to be difficult because images are very “random” - is this true?

PixelPin

Upload a picture,
use 3 or more points as the "password"

random?

Alternatives to Passwords

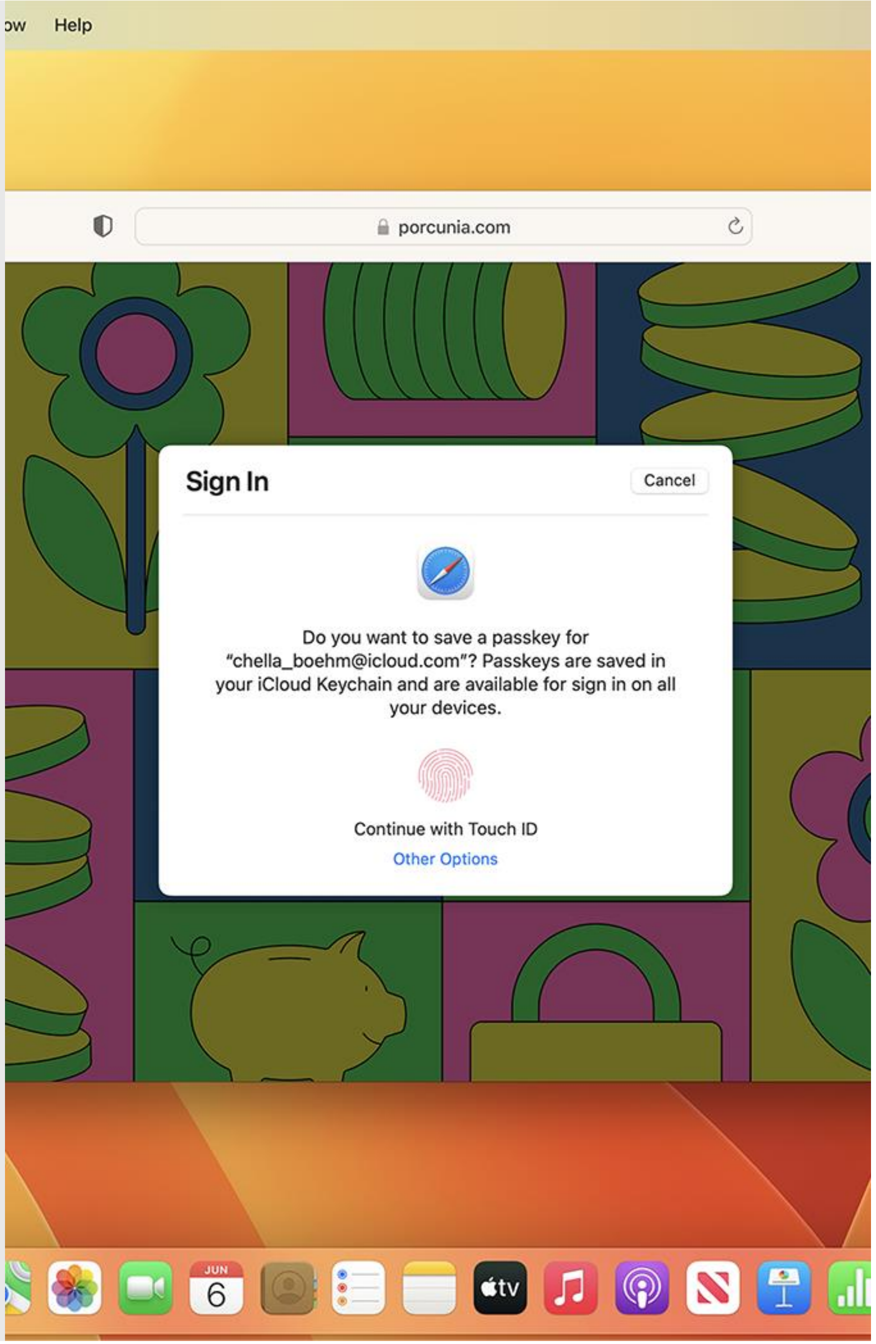
Mobile phones,
USB devices,
special tokens,
etc. etc.

LaunchKey

iOS 16 and MacOS Ventura (since Fall 2022)

Passkeys

- Unique value for each site
- Generated by the client-side OS using biometrics (Face ID, Touch ID)
- Stored in the iCloud keychain, synchronized across devices
- Not stored on the server
- Open standards via FIDO alliance

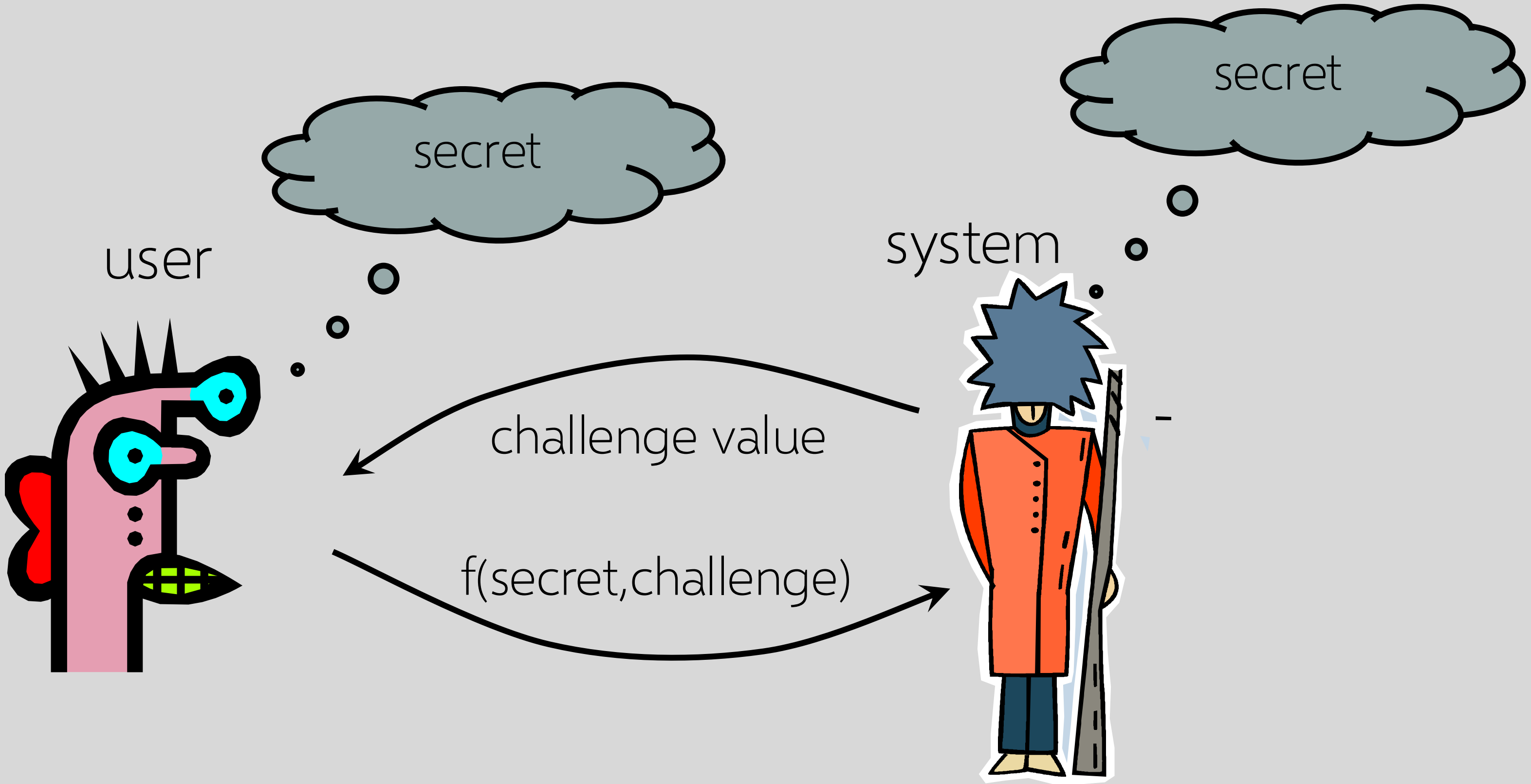


One-Time Passwords

Idea: use a shared secret to derive a one-time password

If the attacker eavesdrops on the network, he'll learn this password but it will be useless for future logins

Challenge-Response



Why is this better than a password over the network?

Challenge-Response Authentication

User and system share a secret (key or password)

Challenge: system presents user with some string

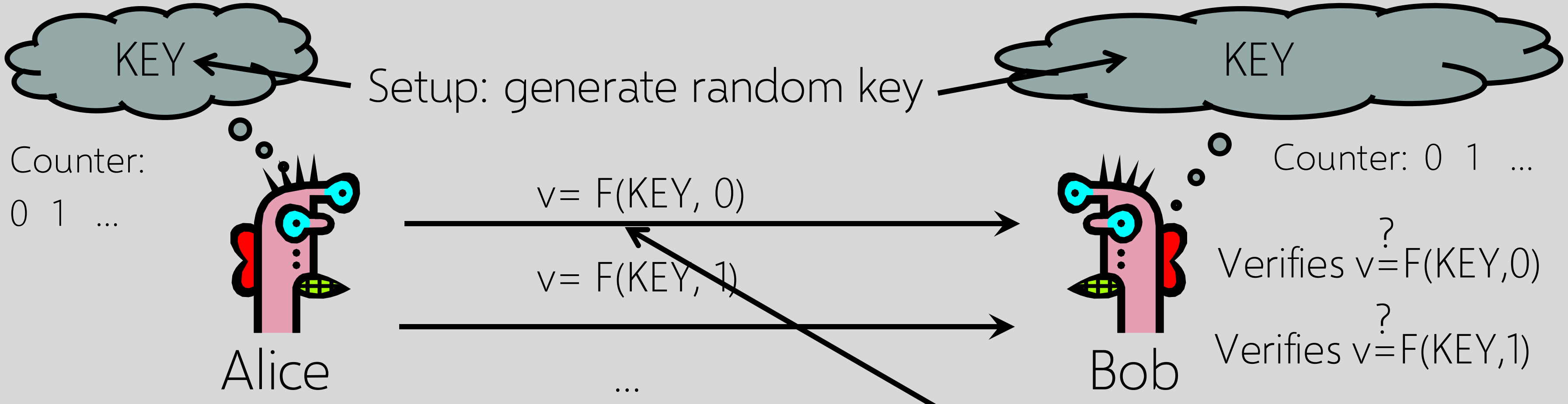
Response: user computes the response based on the secret and the challenge

- Secrecy: difficult to recover secret from response
  - Cryptographic hashing or symmetric encryption work well
- Freshness: if the challenge is fresh, attacker on the network cannot replay an old response
  - Fresh random number, counter, timestamp….

Good for systems with pre-installed secret keys

- Car keys; military friend-or-foe identification

SecurID



RSA uses a custom function
Input: 64-bit key, 24-bit counter
Output: 6-digit value

Advancing the counter

- Time-based (60 seconds) or every button press

Allow for skew in the counter value

- 5-minute clock skew by default

The Full Story of the Stunning RSA Hack Can Finally Be Told

In 2011, Chinese spies stole the crown jewels of cybersecurity—stripping protections from firms and government agencies worldwide. Here's how it happened.

- Phishing email to a staffer with subject line "2011 Recruitment plan" and Excel attachment
- Script in attachment exploited a zero-day vulnerability in Adobe Flash
- Malware scraped usernames and passwords from infected computer, used them to penetrate more machines and accounts (including admin accounts)
- A single server on RSA network was connected to storage with secret key seeds on the SecurID manufacturing side
  - Including seeds for already shipped fobs, as backup for customers' servers
- Stolen seeds later used to breach 2FA at Lockheed Martin and other military contractors

https://www.wired.com/story/the-full-story-of-the-stunning-rsa-hack-can-finally-be-told/