Authentication @ Google

CS 155: Computer and Network Security

Diana Smetters
Google
smetters@google.com
Who am I?

Uber-Tech Lead for Sign-in, part of Google's Identity team.

Responsible for all the policies, systems and UIs that decide who gets into your Google Account, and who doesn't.

This means balancing security, access, and reliability.

My job is to make sure you can get into your Google Account, and bad people can’t.
To be more concrete....
Overview

- Review: What is authentication?
- Why is it hard, particularly at Google?
- Threats and defenses
- How do we work (what's my day job/team like)
- Questions
Authentication (authn)
Whether users are who they claim to be

Authorization (authz)
What users are and aren’t allowed to access
Why should I care?

With the shift to the cloud, security is increasingly about authentication.
How Does Authentication Work?

Stanford University

Stanford Login

Important Security Information: Logging in lets you access other protected Stanford websites with this browser, not just the website you requested.

- LOGIN HELP
- FORGOT YOUR PASSWORD?

Use of this system is subject to Stanford University's rules and regulations. See the Stanford Administrative Guide for more information.
How Does Authentication Work?

Stanford University

Stanford Login

Important Security Information: Logging in lets you access other protected Stanford websites with this browser, not just the website you requested.

FORGOT YOUR PASSWORD?

Login

Use of this system is subject to Stanford University's rules and regulations. See the Stanford Administrative Guide for more information.
How Does Authentication Work?

Verify Identity

Enter your personal information below.

**Last name**

**University ID** [what?]

**Last four digits of Social Security Number** [why?]

(or Individual Taxpayer ID Number)

**Birthdate** (MM/DD/YYYY)

**Password Reset Question:**

City, town, or village of birth?

**Password Reset Answer**

If you have forgotten your password and are not able to provide the requested information, please submit a help ticket or call 650-725-4357.
How Does Authentication Work?

Identifier + Challenges
Quiz #1

- How many online accounts do you have?
- How many that really matter?
- Do you ever use the same password for multiple accounts?
- Do you ever use account recovery?
- To sign in?
- Have you turned on 2-factor authentication for any of your accounts?
- When you didn't have to?
Threats

- Credential breach
- Malware (keyloggers)
- (Offline) Phishing
‘We’ve Been Breached’: Inside the Equifax Hack

The crisis has sent shock waves through the industry, spooked consumers and sparked investigations.

Equifax’s headquarters in Atlanta. Chief Executive Richard Smith has called the cyberattack the ‘most humbling moment in our 118-year history.’ PHOTO: RHONA WISE/EPA/SHUTTERSTOCK

By AnnaMaria Andriotis, Michael Rapoport and
CONTROL, WE HAVE FLOWN TO THE USA AND BREACHED THE TARGET'S HOUSE.

THEM WROTE ALL THEIR PASSWORDS IN A BOOK LABELED "PASSWORDS"!

THE FOOL!

HEY LOOK, SOMEONE LEAKED THE EMAILS AND PASSWORDS FROM THE SMASH MOUTH MESSAGE BOARDS.

COOL, LET'S TRY THEM ALL ON VENMO.

HOW PEOPLE THINK HACKING WORKS

HOW IT ACTUALLY WORKS

Credit: https://xkcd.com/2176/
Credential Breach

3.5B+ credentials leaked in dumps

17% minimum password reuse rate

67M accounts proactively re-secured

Source:
Data breaches, phishing, or malware? Understanding the risks of stolen credentials (Thomas et al., 2017) https://research.google/pubs/pub46437/
Important deal information. Urgent review to close on it.

Some more text that make it look like it's coming from a Trusted Source so I click without reservations.

And, of course, some more text saying not to reply to this email because that would not be secure. Instead, securely log into the website by clicking on this link that closely resembles your domain but instead of the "e" in the name of the domain, it's actually "cyrillic e" and renders very similarly to "latin e".

https://trustedomain/binary
https://bitly.com/abc
https://drive.google.com/abhasdk

trusteddomain hosted on GSuite
Likelihood of Compromise

- Involved in password breach: >10x
- Victim of keylogger: >40x
- Phished: >500x

Source:
Anatomy of Account Takeover (Milka, 2019)
https://www.usenix.org/conference/enigma2018/presentation/milka
Mitigation

- Multi-factor authentication
- Risk-based authentication challenges
- Implicit signals
Multi-factor

Identifier + Challenges + Challenges
Multi-factor in the modern world

Dynamic Risk & Integrity Signals
Controllable factors in Authentication

● When do we challenge you?
● What do we challenge you with?
● What "escape hatches" do we allow?
● What do we put under user control?

● What implicit signals do we get that help distinguish users from attackers?
When do we challenge you?

Deterministic (mostly)

Verify it's you

This device isn't recognized. For your security, Google wants to make sure it's really you. Learn more

Try another way to sign in

- Tap Yes on your phone or tablet
- Get a verification code at (•••) 1234-5678
  Standard rates apply
- Call your phone on file (•••) 1234-5678
- Use your phone or tablet to get a security code (even if it's offline)
- Get help

Risk-based
What do we challenge you with?

Account takeover prevention rates, by challenge type

<table>
<thead>
<tr>
<th>Challenge Type</th>
<th>Automated Bot</th>
<th>Bulk Phishing Attack</th>
<th>Targeted Attack</th>
<th>95% Confidence Interval</th>
</tr>
</thead>
<tbody>
<tr>
<td>On-device prompt</td>
<td>100%</td>
<td>99%</td>
<td>90%</td>
<td></td>
</tr>
<tr>
<td>SMS code</td>
<td>100%</td>
<td>96%</td>
<td>76%</td>
<td></td>
</tr>
<tr>
<td>Security key</td>
<td>100%</td>
<td>100%</td>
<td>100%</td>
<td></td>
</tr>
<tr>
<td>Secondary email address</td>
<td>73%</td>
<td>68%</td>
<td>79%</td>
<td></td>
</tr>
<tr>
<td>Phone number</td>
<td>26%</td>
<td>50%</td>
<td>100%</td>
<td></td>
</tr>
<tr>
<td>Last sign-in location</td>
<td>100%</td>
<td>100%</td>
<td>100%</td>
<td></td>
</tr>
</tbody>
</table>

Source:
Evaluating Login Challenges as a Defense Against Account Takeover (Doerfler et al.) https://ai.google/research/pubs/pub48119
Password Brute-Forcing: Defeatable with Per-User Quotas

Username | Password
---|---
john_doe | qwerty (crossed out)
john_doe | password (crossed out)
jdoe | 111111
jane.doe | 12345678
janed | abc123 (green check mark)

25
Password Spraying

<table>
<thead>
<tr>
<th>Username</th>
<th>Password</th>
</tr>
</thead>
<tbody>
<tr>
<td>john_doe</td>
<td>password</td>
</tr>
<tr>
<td>jdoe</td>
<td>111111</td>
</tr>
<tr>
<td>jane.doe</td>
<td>12345678</td>
</tr>
<tr>
<td>janed</td>
<td>abc123</td>
</tr>
<tr>
<td></td>
<td>password1</td>
</tr>
</tbody>
</table>
Why is this hard?

And maybe harder for Google than others?

- Moving target w/evolving attackers
- Defenses themselves pose (availability) risks
Can you get access to your stuff?
- Fast?
- Easily?
- Eventually?

Increased security means you have to say **no**, at least some of the time.
Different accounts pose different protection problems

**Subscription video-streaming:**
- **Large user base** (e.g. 100M)
- **Potential damage:**
  - Theft of service/content
  - Theft of personal data
  - Ratings fraud (abuse)
- **Lockout prevention:**
  - Customer support/payment info
- **User cost of account loss:** low

**Educational institution:**
- **Small user base** (< 100K)
- **Potential damage:**
  - Theft of personal data
  - Content manipulation/DoS
- **Lockout prevention:**
  - Administrator fallback prevents account loss
- **User cost of account loss:** N/A
Different accounts pose different protection problems

**Google:**
- Large user base (**2B+ active**), many products
- **Potential damage:**
  - Theft/damage of personal data
  - Loss of income (e.g. for YouTube creators/App developers)
  - Leapfrog attacks against other accounts
    - Recovery email
    - "Sign in with Google"
  - Abuse against others
    - Spam, Ad click fraud, Review fraud
- **Lockout prevention:**
  - User-configured account recovery + devices
- **User cost of account loss:** ranges from zero to irreplaceable
Quiz #2

How many Google Accounts do you have?

How many do you care about/pay attention to?
Weaponized protection mechanisms

If you build something to let users protect themselves, hijacklers will turn it against them.
Threats

- Credential breach
- Malware (keyloggers)
- (Offline) Phishing
- Challenge compromise
SMS: Not so hot anymore

SIM swap scam: What it is and how to protect yourself

SIM Swapping Attacks: What They Are & How to Stop Them

Fraudsters with social engineering skills are hijacking cell phone SIM cards to access victims' bitcoin and social media accounts.

How to Protect Yourself Against a SIM Swap Attack

Your phone number is increasingly tied to your online identity. You need to do everything possible to protect it.
Mitigation

- Multi-factor authentication
- Risk-based authentication challenges
- Implicit signals
- Dynamic challenge policies
Dynamic challenge policies

- Automatically offer the strongest challenges available
- Suppress weaker challenges in risky situations where the user has better options

Strengthening 2-Step Verification by showing phone prompts to more users
Tuesday, June 16, 2020

What's changing
Starting on July 7, 2020, we will make phone verification prompts the primary 2-Step Verification (2SV) method for all eligible users, unless they are already using security keys as their 2SV method of choice. This means that if you sign in to your Google
Threats

- Credential breach
- Malware (keyloggers)
- (Offline) Phishing
- Challenge compromise
- Active Man-in-the-Middle (MITM)
1. Click link
2. Verify page
3. Enter credentials
4. Send SMS code
5. Enter code into site
1. Visit site
2. View and verify page
3. Enter credentials
Evilginx - Advanced Phishing with Two-factor Authentication Bypass

06 APRIL 2017 on hacking, research, phishing, mitm
YouTube ‘influencers’ get 2FA tokens phished

24 SEP 2019

2-factor Authentication, Google, Security threats, Social networks
Mitigation

- Multi-factor authentication
- Risk-based authentication challenges
- Implicit signals
- Dynamic challenge policies
- Detecting and blocking active MITM
- Relying on trusted devices
- Phishing-resistant challenges
Announcing some security treats to protect you from attackers’ tricks
October 31, 2018

Posted by Jonathan Skelker, Product Manager

Guidance to developers affected by our effort to block less secure browsers and applications
Friday, August 28, 2020

Posted by Lillian Marie Agerup, Product Manager

We are always working to improve security protections of Google accounts. Our security systems automatically detect, alert and help protect our users against a range of security threats. One form of phishing, known as “man-in-the-middle”, is hard to detect when an embedded browser framework (e.g., Chromium Embedded Framework - CEF) or another automation platform is being used for authentication. MITM presents a risk to your account and works by stealing your session cookies. We are blocking MITM for developers using one of these platforms. More information can be found in the blog post linked below.

Learn more about the Chrome Embedded Framework.
Trusted/Known Devices

Cardinal Key
Simplicity and Security

Get a Cardinal Key
“Unphishable” challenges
Even Better - Phones as (free) Security Keys

Google Smart Lock
Google LLC

Now, your Android phone is also a security key

- Enhanced account protection
  Strongest 2FA protection against phishing
- Easy to use
  Simple, one-time enrollment process, no app required
- Convenient for users
  Use the phone which is already in your pocket.

Google now treats iPhones as physical security keys

With an update to the Google Smart Lock app

By Jon Porter | @JonPorty | Jan 15, 2020, 5:02am EST
A simpler and safer future — without passwords

Google will soon automatically enroll users in 2FA

You’ll have the option to opt-out

Google to Opt People Into Two-Factor Authentication Automatically

Google will start with those who regularly engage with Google products on mobile and have recovery options saved to their accounts, but going forward, 2FA will be opt out rather than opt in.
Threats

- Credential breach
- Malware (keyloggers)
- Phishing
- Challenge compromise
- Active MITM
- Malware (session theft)
Cookie/Token Theft: When it's too hard to get in the front door...

You go in through the window
What's it like to do this job?

Team:
- Identity org of ~400
  - Sites in Sunnyvale, San Francisco, Munich, Zurich and Tel Aviv
- Sign-in team of ~55 engineers
  - Divided into 6 subteams with different specializations (not all security)
  - 25% female

What do we do?
- Write code
- Do & review design
- Do data analysis
- Work with xfn partners
  - Product managers
  - UX designers & writers
  - UX researchers
  - Data analysts
- Go to a lot of meetings (at least me)

We're hiring!
Questions?