

**“If I could do this, I feel anyone could:”**

The Design and Evaluation of a  
Secondary Authentication Manager

Garrett Smith\*, Tarun Yadav\*, Jonathan Dutson,  
Scott Ruoti, and Kent Seamons

Brigham Young University and the University of Tennessee Knoxville

---

\*Denotes Equal Contribution

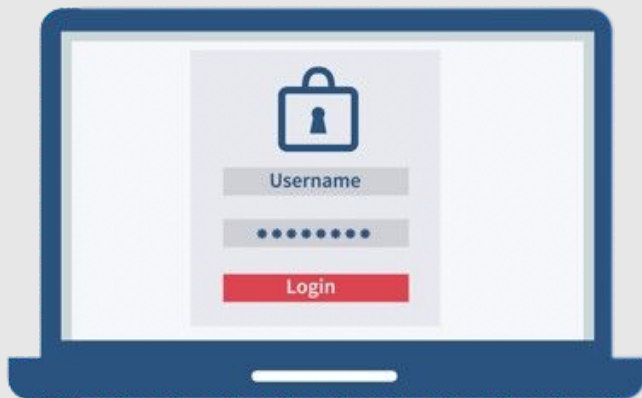
USENIX 2023

# Password Based Authentication

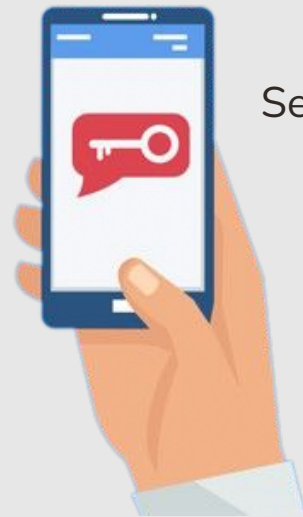


# Two-Factor Authentication

Primary Authentication  
Factor



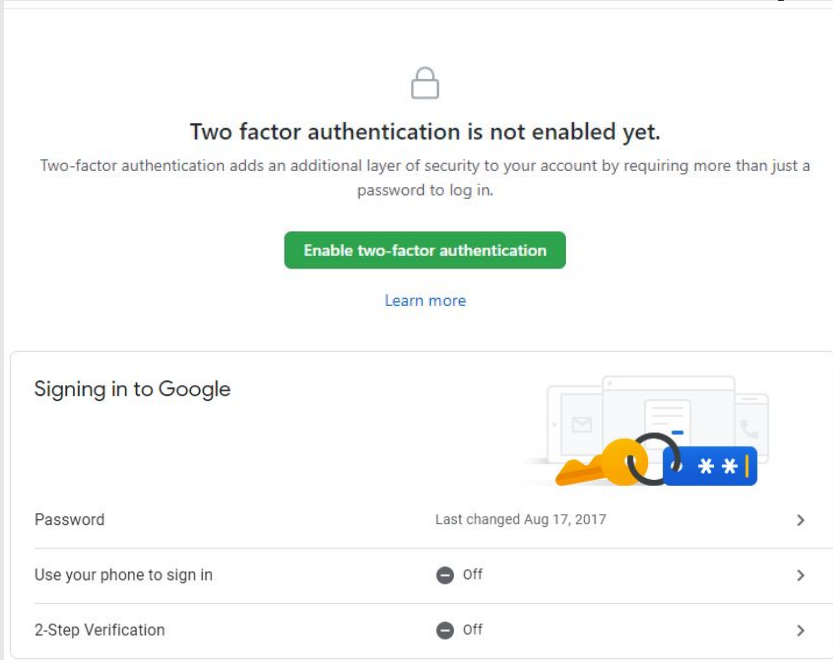
Secondary Authentication  
Factor (SAF)



# 2FA Implementations

2FA Implementations vary across websites

- Inconsistent terminology
- Different requirements and recommendations
- Varying workflows



The screenshot shows a web interface for enabling two-factor authentication. At the top, there is a lock icon and the text "Two factor authentication is not enabled yet." Below this, a sub-header explains that two-factor authentication adds an additional layer of security by requiring more than just a password. A prominent green button labeled "Enable two-factor authentication" is centered, with a "Learn more" link below it. The lower section, titled "Signing in to Google", contains a list of settings: "Password" (last changed Aug 17, 2017), "Use your phone to sign in" (set to Off), and "2-Step Verification" (set to Off). Each setting has a right-pointing chevron for further options. An illustration of a smartphone and a laptop with a key icon is positioned to the right of the settings list.

**Two factor authentication is not enabled yet.**

Two-factor authentication adds an additional layer of security to your account by requiring more than just a password to log in.

[Enable two-factor authentication](#)

[Learn more](#)

Signing in to Google

Password	Last changed Aug 17, 2017	>
Use your phone to sign in	Off	>
2-Step Verification	Off	>

# Updating Many Accounts

- First adopting 2FA
- Replacing an existing SAF (getting a new phone)
- Removing a lost SAF
- Adding an SAF  
(backup, spouse/child access)



# Authentication Manager



**Password  
Manager**

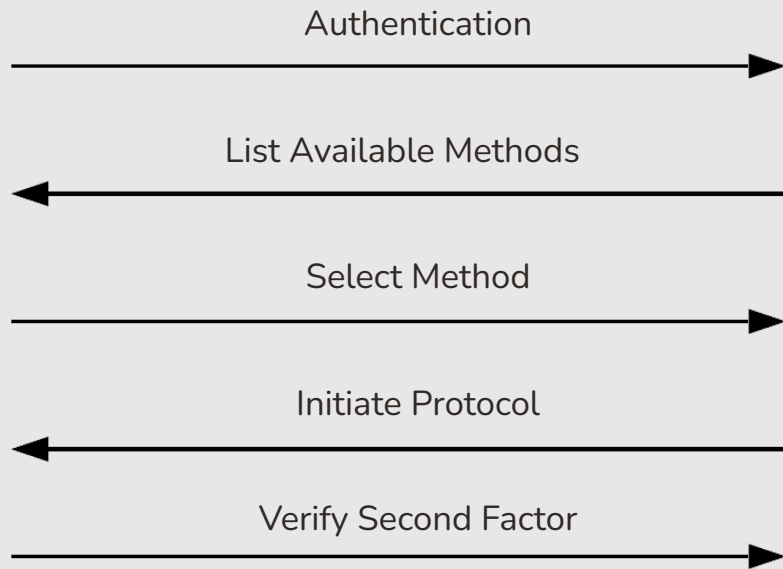


**SAF Manager**

# SAF Setup Abstraction



SAF Manager



Website

# Prototype

## Protect all of your accounts with 2-Factor Authentication



Each time you sign in to your accounts you'll need your password and a verification code.



Even if someone gets your password, they won't be able to gain access to your account.

Add 2FA Option

Remove 2FA Option



Select the accounts you would like to protect with 2FA



Google



Facebook



Dropbox



LinkedIn



Twitter



Github



Amazon



Yahoo

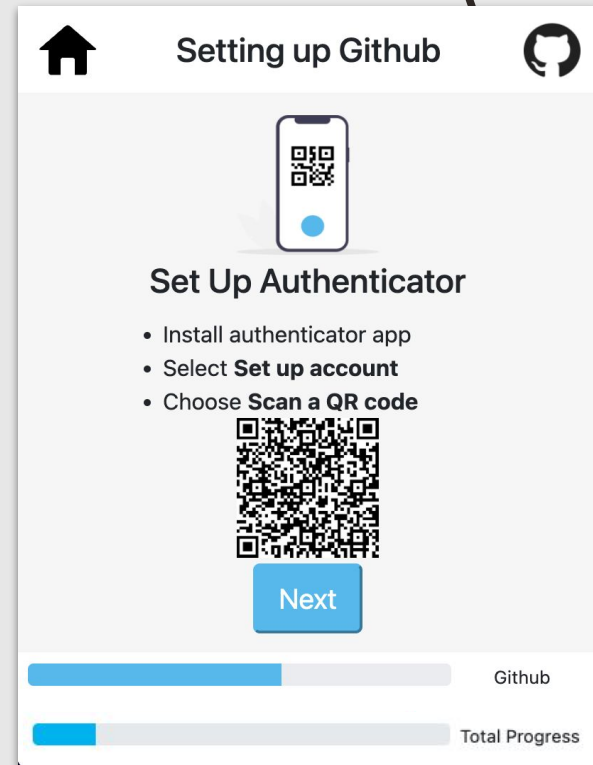
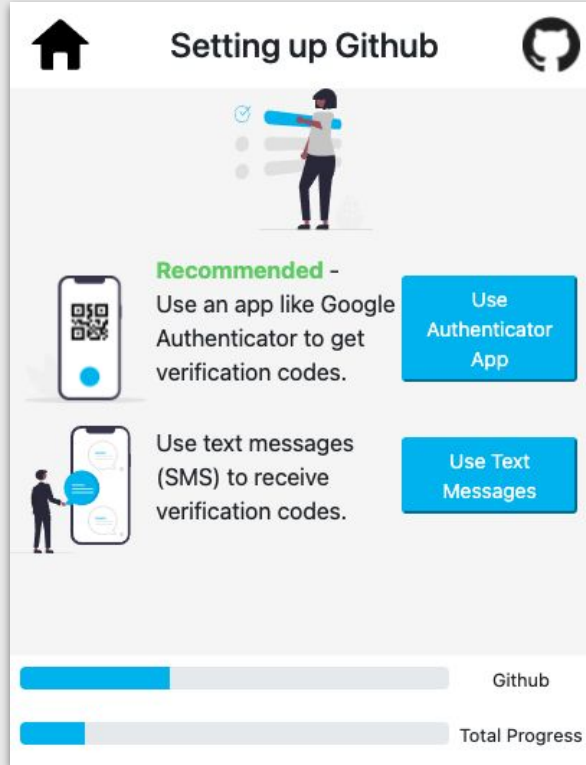
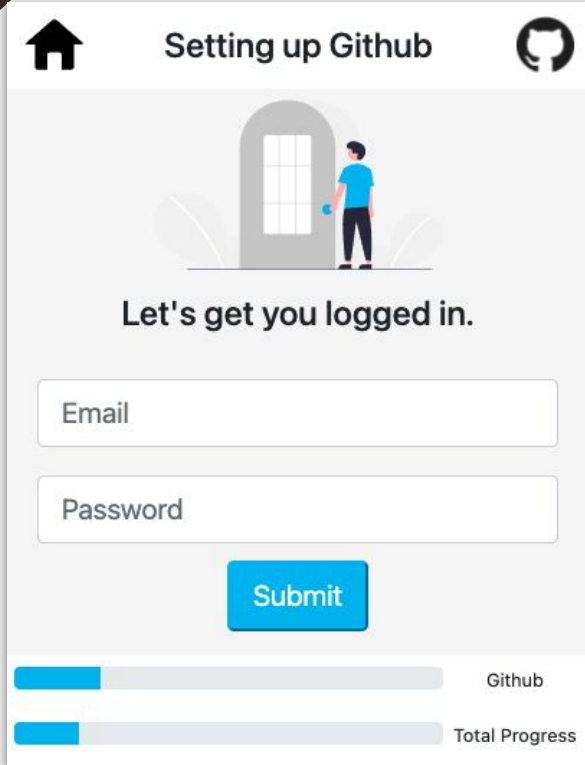


Reddit



Get Started




# Prototype



# Prototype

Setting up Github





### Set Up Authenticator


Enter the 6-digit code you see in the app.

[Need to scan QR code again?](#)

Github

Total Progress

Setting up Github

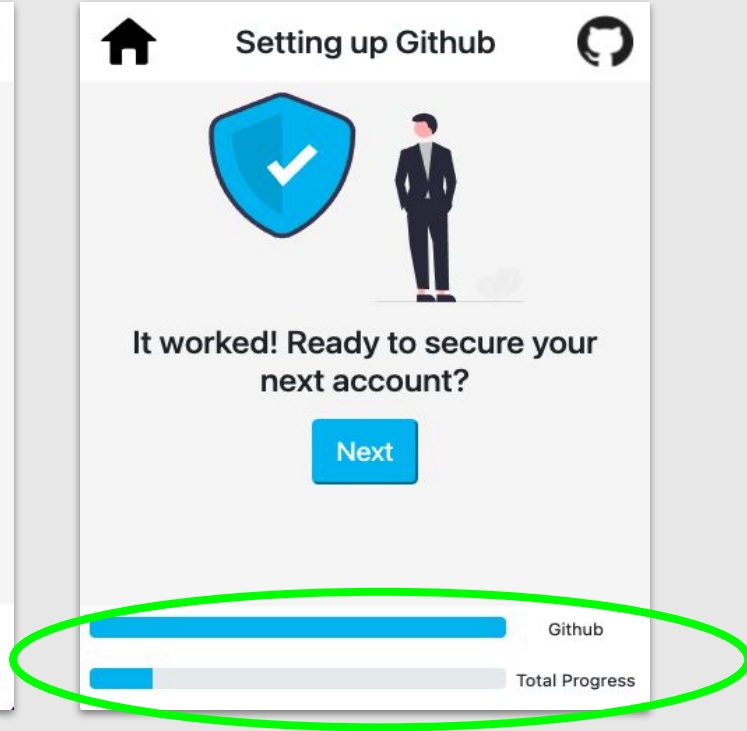
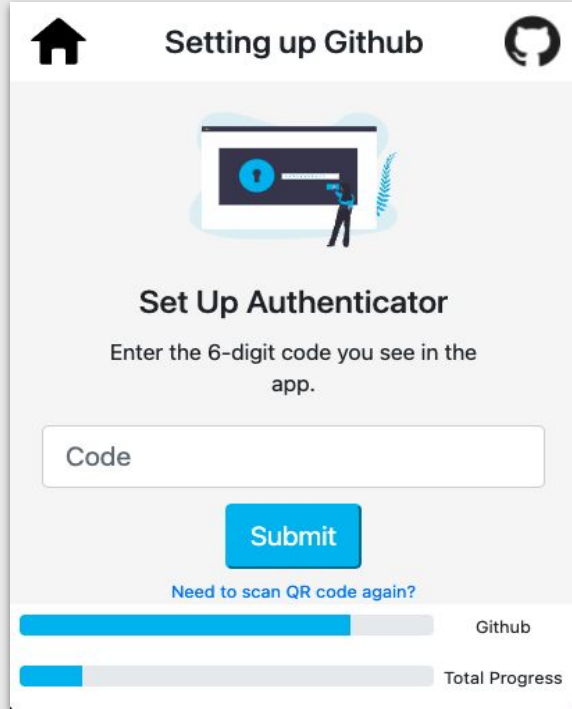


### It worked! Ready to secure your next account?

Github

Total Progress

# Prototype



# User Study Design

## Dependent Variables

- Success rate
- Completion Time
- Usability
  - System Usability Scale

## Independent Variables

- 2FA Setup Process
  - Manual
  - Automated
- 2FA Experience
  - Novice 2FA Users
  - Experienced Users

# Study Design

Independent Variables	Group A	Group B	Group C
2FA Experience	Novice User	Novice User	Advanced User
2FA Methods	Manual Method	SAF Manager	SAF Manager

# Study Design

- 60 Participants - Prolific Academic
- A|B, C Assigned by 2FA usage
- A|B Assigned randomly

Measure	Items	A	B	C	Total
Gender	Female	13	12	4	29
	Male	7	8	16	31
Age	18-24	4	1	1	6
	25-34	7	5	9	20
	35-44	5	4	2	11
	45-54	2	5	4	11
	55+	2	4	2	9

# Results - Success Rate

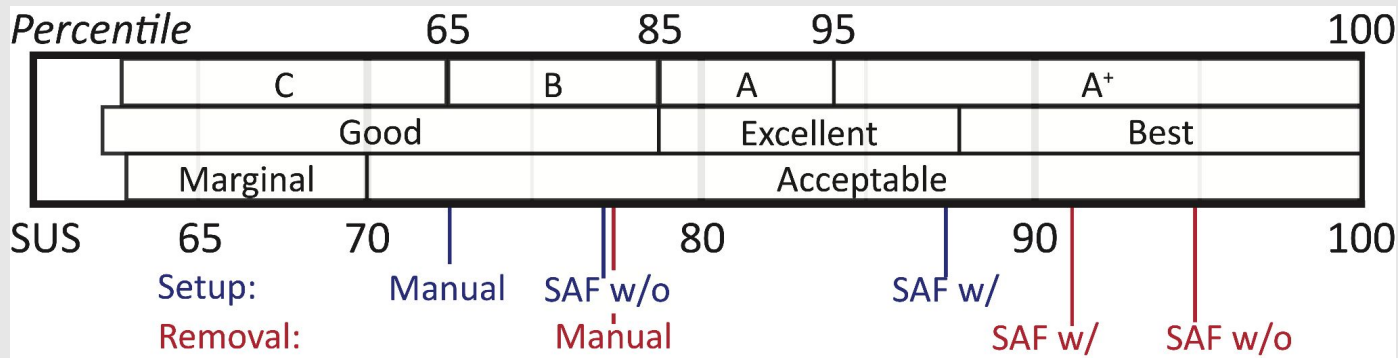
Group	Tool Used	Success Rate
A	Existing Websites	75% - (15)
B	SAF Manager	100% - (20)
C	SAF Manager	90% - (18)

# Results - Completion Time

Group	Tool Used	Completion Time
A	Existing Websites	7 minutes 52 seconds
B	SAF Manager	5 minutes 15 seconds
C	SAF Manager	4 minutes 22 seconds



# Results - System Usability Scale



	Study Group	Setup Method	2FA Experience
Manual	Group A	Manual	Novice
SAF W/o	Group B	SAF Manager	Novice
SAFE W/	Group C	SAF Manager	Experienced

# Common Issues

## Enable two-step verification ×

An authenticator app lets you generate security codes on your phone without needing to receive text messages. If you don't already have one, we support any of [these apps](#).

To configure your authenticator app:

- Add a new time-based token.
- Use your app to scan the barcode below, or enter your secret key manually.



Back

Next

## Enable two-step verification ×

Enter the security code generated by your mobile authenticator app to make sure it's configured correctly.

Back

Next

# Common Issues

## Enable two-step verification

### Backup phone number (optional)

If you lose access to your primary security code source, we can send them to your backup mobile number instead.

United States +1

(201) 555-0123

While this step is optional, we encourage you to set up a backup phone number in case you lose your mobile phone or are otherwise unable to receive your security code.

Back

Next

## Enable two-step verification

Your security codes will be generated by your authenticator app

You can use these one-time backup codes to access your account.

1. **lio7 6zqm**
2. **varx rhyj**
3. **ye6a pqj7**
4. **r31i 3dp9**
5. **f89u cesb**
6. **oszf zjk0**
7. **w6e7 5w50**
8. **vrtg zlrn**
9. **ud51 ilmi**
10. **v1z5 tjbs**

Write these down and keep them safe.

Back

Next

## Enable two-step verification

From now on, when you sign in to the Dropbox website or link a new device, you'll need to enter a security code from your phone.

Next

# **Design Limitations**

- Limited Scalability
  - Adoption
-

# How can we address scalability?

- Web API
- Crowdsourcing
- Web Standards

GET

**/supportedMethods** Lists all supported 2FA methods

GET

**/enabledMethods** Lists all 2FA methods currently enabled by the user

POST

**/requestSetup** Request enrollment for a 2FA method

POST

**/response** Return response to challenge

DELETE

**/remove** Unregisters a second factor

# Where do we go from here?

- Recovery
- Passwordless Authentication
- Improve Existing Workflows
- Standardize 2FA Experience
- Unified Authentication Manager

# Thanks!

Any Questions?



Read our paper or see our source code!