“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
Password Based Authentication

My Password 123456
Two-Factor Authentication

Primary Authentication Factor

Secondary Authentication Factor (SAF)
2FA Implementations vary across websites
- Inconsistent terminology
- Different requirements and recommendations
- Varying workflows
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

Authentication
List Available Methods
Select Method
Initiate Protocol
Verify Second Factor

SAF Manager
Website

USENIX 2023
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

Setting up Github

Let's get you logged in.

Email
Password
Submit

Setting up Github

Recommended - Use an app like Google Authenticator to get verification codes.

Use text messages (SMS) to receive verification codes.

Use Authenticator App
Use Text Messages

Setting up Github

Set Up Authenticator

- Install authenticator app
- Select Set up account
- Choose Scan a QR code

Next
Prototype

Set Up Authenticator
Enter the 6-digit code you see in the app.

Code

Submit

Need to scan QR code again?

GITHUB
Total Progress

GITHUB
Total Progress

It worked! Ready to secure your next account?
Prototype

Set Up Authenticator
Enter the 6-digit code you see in the app.

Submit

Need to scan QR code again?

It worked! Ready to secure your next account?

Next

Github

Total Progress
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

<table>
<thead>
<tr>
<th>Independent Variables</th>
<th>Group A</th>
<th>Group B</th>
<th>Group C</th>
</tr>
</thead>
<tbody>
<tr>
<td>2FA Experience</td>
<td>Novice User</td>
<td>Novice User</td>
<td>Advanced User</td>
</tr>
<tr>
<td>2FA Methods</td>
<td>Manual Method</td>
<td>SAF Manager</td>
<td>SAF Manager</td>
</tr>
</tbody>
</table>
Study Design

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

<table>
<thead>
<tr>
<th>Measure</th>
<th>Items</th>
<th>A</th>
<th>B</th>
<th>C</th>
<th>Total</th>
</tr>
</thead>
<tbody>
<tr>
<td>Gender</td>
<td>Female</td>
<td>13</td>
<td>12</td>
<td>4</td>
<td>29</td>
</tr>
<tr>
<td></td>
<td>Male</td>
<td>7</td>
<td>8</td>
<td>16</td>
<td>31</td>
</tr>
<tr>
<td>Age</td>
<td>18-24</td>
<td>4</td>
<td>1</td>
<td>1</td>
<td>6</td>
</tr>
<tr>
<td></td>
<td>25-34</td>
<td>7</td>
<td>5</td>
<td>9</td>
<td>20</td>
</tr>
<tr>
<td></td>
<td>35-44</td>
<td>5</td>
<td>4</td>
<td>2</td>
<td>11</td>
</tr>
<tr>
<td></td>
<td>45-54</td>
<td>2</td>
<td>5</td>
<td>4</td>
<td>11</td>
</tr>
<tr>
<td></td>
<td>55+</td>
<td>2</td>
<td>4</td>
<td>2</td>
<td>9</td>
</tr>
</tbody>
</table>
## Results - Success Rate

<table>
<thead>
<tr>
<th>Group</th>
<th>Tool Used</th>
<th>Success Rate</th>
</tr>
</thead>
<tbody>
<tr>
<td>A</td>
<td>Existing Websites</td>
<td>75% - (15)</td>
</tr>
<tr>
<td>B</td>
<td>SAF Manager</td>
<td>100% - (20)</td>
</tr>
<tr>
<td>C</td>
<td>SAF Manager</td>
<td>90% - (18)</td>
</tr>
</tbody>
</table>
# Results - Completion Time

<table>
<thead>
<tr>
<th>Group</th>
<th>Tool Used</th>
<th>Completion Time</th>
</tr>
</thead>
<tbody>
<tr>
<td>A</td>
<td>Existing Websites</td>
<td>7 minutes 52 seconds</td>
</tr>
<tr>
<td>B</td>
<td>SAF Manager</td>
<td>5 minutes 15 seconds</td>
</tr>
<tr>
<td>C</td>
<td>SAF Manager</td>
<td>4 minutes 22 seconds</td>
</tr>
</tbody>
</table>
## Results - System Usability Scale

<table>
<thead>
<tr>
<th>Setup Method</th>
<th>2FA Experience</th>
</tr>
</thead>
<tbody>
<tr>
<td>Manual</td>
<td>Novice</td>
</tr>
<tr>
<td>SAF Manager</td>
<td>Novice</td>
</tr>
<tr>
<td>SAF Manager</td>
<td>Experienced</td>
</tr>
</tbody>
</table>

### Setup Method Details
- **Group A**: Manual
- **Group B**: SAF Manager
- **Group C**: SAF Manager

### Setup Method Examples
- **Manual**: Removal
- **SAF Manager**: SAF w/o, SAF w/

### Percentile Scale

<table>
<thead>
<tr>
<th>Percentile</th>
<th>Grade</th>
</tr>
</thead>
<tbody>
<tr>
<td>C</td>
<td>Good</td>
</tr>
<tr>
<td>B</td>
<td>Acceptable</td>
</tr>
<tr>
<td>A</td>
<td>Excellent</td>
</tr>
<tr>
<td>A+</td>
<td>Best</td>
</tr>
<tr>
<td>Marginal</td>
<td></td>
</tr>
</tbody>
</table>

### Study Group

<table>
<thead>
<tr>
<th>Study Group</th>
<th>Manual</th>
<th>SAF W/o</th>
<th>SAFE W/</th>
</tr>
</thead>
<tbody>
<tr>
<td>Group A</td>
<td>Group B</td>
<td>Group C</td>
<td></td>
</tr>
</tbody>
</table>

**USENIX 2023**
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.

Enable two-step verification

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

6-digit code
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. li07 6zqm
2. varx rhyj
3. ye6a pqj7
4. r3li 3dp9
5. f89u cesb
6. oszf zjk0
7. w6e7 5w50
8. vrtg zlrm
9. ud51 ilmi
10. v1z5 tjbs

Write these down and keep them safe.

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.
Design Limitations

- Limited Scalability
- Adoption
How can we address scalability?

- Web API
- Crowdsourcing
- Web Standards

<table>
<thead>
<tr>
<th>Method</th>
<th>Endpoint</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>GET</td>
<td>/supportedMethods</td>
<td>Lists all supported 2FA methods</td>
</tr>
<tr>
<td>GET</td>
<td>/enabledMethods</td>
<td>Lists all 2FA methods currently enabled by the user</td>
</tr>
<tr>
<td>POST</td>
<td>/requestSetup</td>
<td>Request enrollment for a 2FA method</td>
</tr>
<tr>
<td>POST</td>
<td>/response</td>
<td>Return response to challenge</td>
</tr>
<tr>
<td>DELETE</td>
<td>/remove</td>
<td>Unregisters a second factor</td>
</tr>
</tbody>
</table>
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!