A Study of Authentication in Daily Life

Shrirang Mare
Dartmouth College

Mary Baker
HP Labs, Palo Alto

Jeremy Gummeson
Disney Research, Pittsburgh
Authentication
Authentication

Authenticators

Authentication Targets
Authentication behavior studies

• Password habits [Adams and Sasse 1999]

• Web password habits [Florenicio and Herley 2007]

• Access control in real world [Sinclair and Smith 2010]

• Password diary study [Hayashi and Hong 2011]

• Phone lock habits [Egelman et al. 2014, Harbach et al. 2014]

• Authentication diary study, NIST report [Steves et al. 2014]

• Understanding biometric authentication on smartphones [Luca et al. 2015]

• Understanding people’s security practices [Ion et al. 2015]
Study goal

Gain a better understanding of people’s daily authentication behavior and opinion through interviews and tracking their authentication events to inform future projects that aim at reducing users’ authentication burden.
Study goal

Gain a better understanding of people’s daily authentication behavior and opinion through interviews and tracking their authentication events to inform future projects that aim at reducing users’ authentication burden.

- **What** do people authenticate to, **how**, **when**, and **where**?
- Which authentications are **error-prone**?
- What do they **think** about authentication, and what do they **like** and **dislike**?
Study contributions

• Design of a wearable digital diary study

• Findings from the participant’s authentication logs and the semi-structured interviews with them

• Study data: Participants’ authentication logs and summarized interviews
An authentication event is an act where an individual must demonstrate, \textit{actively}, that he is the right person to gain access to a resource or service through something he is (or does), something he knows, or something he has.
Study methodology

- Pre-logging interview
- Logging: Participants log authentications for 7 days
- Post-logging interview
Logging authentication events

Authentication event details:

1. Time
2. Authentication target
3. Authenticator
4. Success/failure
5. Number of attempts, if successful
6. Location
Logging: Watch app

• Only 2 taps to log an event in common case

• Slot-machine interface

• Most participants preferred logging on the watch

“I didn’t used to wear a watch. [...] Now I want a watch”

“Anything more than 2-3 taps is effort for me.”
Logging: Watch app

• Only 2 taps to log an event in common case
• Slot-machine interface
• Most participants preferred logging on the watch

“Anything more than 2-3 taps is effort for me.”

“I didn’t used to wear a watch. [...] Now I want a watch”
Logging: Watch app

- Only 2 taps to log an event in common case
- Slot-machine interface
- Most participants preferred logging on the watch

“Anything more than 2-3 taps is effort for me.”

“I didn’t used to wear a watch. [...] Now I want a watch”
Logging: Phone app

• Syncs data with the watch

• Uploads data to our server

• Logs participants’ location

• Shows daily event log so participants can edit events and add missed events

• Administers daily survey
Limitations

- **Under-reporting**: Minimized effort to log an event, but cannot rule out under-reporting.

- **Small sample size**: A “convenience” sample of 26 participants.

- **Self-logged vs. auto-logged**: Phone events are auto-logged and rest are self-logged.

- **A snapshot of a week**: May not be representative of the participant’s typical week.

- **Possible change in participants’ behavior**: Participation in the study could affect participant behavior.

"A couple of times I left my PC unlocked when I stepped away for just a minute because I didn't want to have to log it"

"I found myself typing my passwords slower so I'd get them right the first time."
Participants

Age group

- Under 21 years
- 21 - 30 years
- 31 - 40 years
- 41 - 50 years
- 51 - 60 years
- Over 60 years

Number of participants

- Male
- Female
Distribution of events by authenticators

- **Secret**: Pink bars
- **Token**: Green bars
- **Other**: Blue bars

The graph shows the distribution of authentication events across different participant IDs. Each bar represents the number of authentication events for a specific participant ID, categorized by the type of authenticator used (Secret, Token, Other). The y-axis represents the number of authentication events, and the x-axis represents the participant ID.
Opinions about authentication

How frustrating is authentication? | N
---|---
1. I don’t notice them | 1
2. | 9
3. | 10
4. | 5
5. Extremely frustrating | 1

Most liked authenticators:
- Fingerprint: 23%
- Keyfobs: 16%
- PINs: 16%
- Keys: 10%
- Passwords: 6%
- Badges: 19%
- Other: 10%

Most disliked authenticators:
- Passwords: 50%
- Badges: 16%
- Fingerprint: 19%
- PINs: 9%
- Keys: 10%
- Other: 16%

"It’s important – necessary, so you just do it"
Opinions about authentication

<table>
<thead>
<tr>
<th>How frustrating is authentication?</th>
<th>N</th>
<th>N*</th>
</tr>
</thead>
<tbody>
<tr>
<td>I don’t notice them</td>
<td>1</td>
<td>1</td>
</tr>
<tr>
<td></td>
<td>9</td>
<td>6</td>
</tr>
<tr>
<td></td>
<td>10</td>
<td>8</td>
</tr>
<tr>
<td></td>
<td>5</td>
<td>7</td>
</tr>
<tr>
<td>Extremely frustrating</td>
<td>1</td>
<td>4</td>
</tr>
</tbody>
</table>

Most liked authenticators
- Passwords: 16%
- Fingerprint: 23%
- Keys: 10%
- PINs: 16%
- Keyfobs: 16%
- Other: 9%

Most disliked authenticators
- Passwords: 50%
- Keyfobs: 19%
- Fingerprint: 16%
- Badges: 6%
- PINs: 9%
- Keys: 19%
- Other: 16%

"It’s important – necessary, so you just do it"
Opinions about authentication

<table>
<thead>
<tr>
<th>How frustrating is authentication?</th>
<th>N</th>
<th>N*</th>
</tr>
</thead>
<tbody>
<tr>
<td>(1) I don’t notice them</td>
<td>1</td>
<td>1</td>
</tr>
<tr>
<td>(2)</td>
<td>9</td>
<td>6</td>
</tr>
<tr>
<td>(3)</td>
<td>10</td>
<td>8</td>
</tr>
<tr>
<td>(4)</td>
<td>5</td>
<td>7</td>
</tr>
<tr>
<td>(5) Extremely frustrating</td>
<td>1</td>
<td>4</td>
</tr>
</tbody>
</table>

Most liked authenticators:
- Passwords: 50%
- Fingerprint: 23%
- Keyfobs: 16%
- Badges: 19%
- Keys: 10%
- PINs: 9%

Most disliked authenticators:
- Passwords: 50%
- Keyfobs: 16%
- Badges: 16%
- Keys: 19%
- PINs: 9%

"It’s important – necessary, so you just do it"

"[Most effort are physical keys] first you have to find it in your purse, then pick out the right key from the ring. [...] So keys were a lot of effort, and the phone unlock wasn’t."
Acknowledgements

- Sunny Consolvo
- April Mitchell
- Iris Beneli
- Alvin AuYoung
- Ben Eric Andow
- Animesh Srivastava
- Cormac Herley
- SOUPS reviewers
- Kassem Fawaz
- Jim Mann
- Aarathi Prasad
- Denise Anthony
“The creativity in me makes them [passwords] more complicated – part of my frustration is that.”

“[Authentication] It’s kind of evil. It’s a constant reminder that there are bad people.”

“I’m also not happy with door key unlocking.”

“How do I log this event? I entered my password and my laptop crashed.”

“I always have to search in my purse for my keys or my badge. It’s a giant black hole.”

“How do I log this event? I entered my password and my laptop crashed.”

“[Locked keys in the car] But a guy in the parking lot was able to break into my car for me. I was never happier in my life to meet a competent criminal.”

“Also, I feel embarrassed wearing it [badge ID] — kind of like I’m a kid in kindergarten with a name tag. And I hate my photo that’s on it.”