PassBeat authentication

Oskar Grönqvist
Judith Treffler
Group 24

[1]

Challenge

The goal of our project is to develop a prototype for PassBeat - a rhythm-based authentication method for a music streaming app. This prototype serves as a mean to conduct research on retentiveness, convenience, and perceived security of rhythm-based authentication.

Figure 1: How well a design respresents the two concepts of memorization and security can be seen lying somewhere on a spectrum.

Prototypes

The prototypes shown later in this deck are designed in ways that are supposed to represent the conflict of the two most important concepts in this study, security and memorization (See Figure 1). For example, one study has shown that visualization can help people memorize a musical piece (or rhythm) [2], but visual and auditory feedback will make it easier for potential intruders to identify the rhythm by shoulder-surfing.

Prototype 1 will act as the “normal” option, or as a benchmark. Only visual feedback on the button will be given when the user presses it.

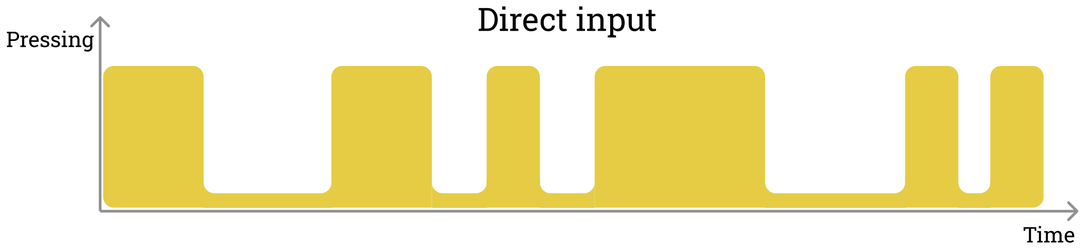
Prototype 2 is the secure option. No feedback will be given, except for an optional vibration.

Prototype 3 is the option with maximum feedback. This version will give the user both visual, on all elements of the layout, and auditory feedback.

[1] http://www.onlinewebfonts.com
[2] Reichling, M. (1989). Memorizing piano music: what the research offers teachers. *Update: Applications of Research in Music Education*, 8(1), 9-14.

How are PassBeats made?

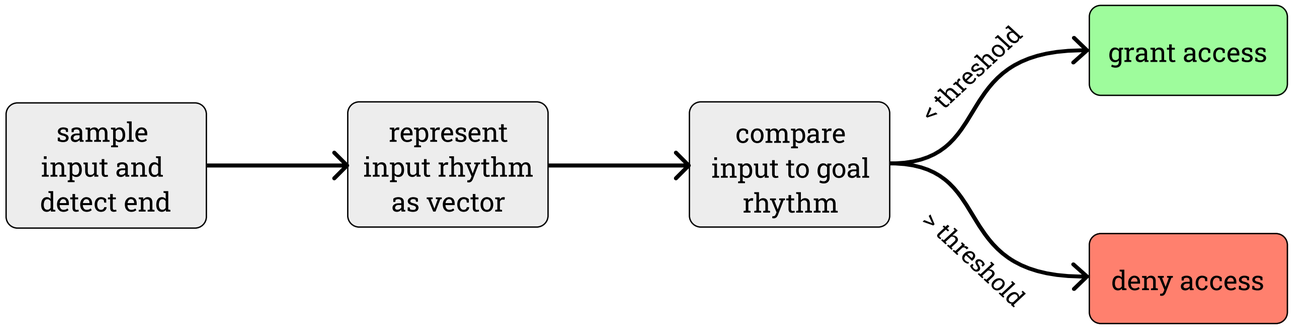
When a user enters their PassBeat authentication code the length of each press and the pauses between them are save measured in milliseconds and saved in a vector. This means that every other value in the resulting vector represents the length of a press, and every other value represents the length of a pause.



Generated vector

`(520,680,520,210,200,210,1050,680,200,80,200)`

For each value in the vector a certain margin of error is allowed, for example 5% or 50ms. This should make it possible to calculate the maximum number of possible and unique rhythms, and in turn makes it possible to find comparable text-based passwords. This must be done in order to realistically measure the difference in security between the two types of authentication.



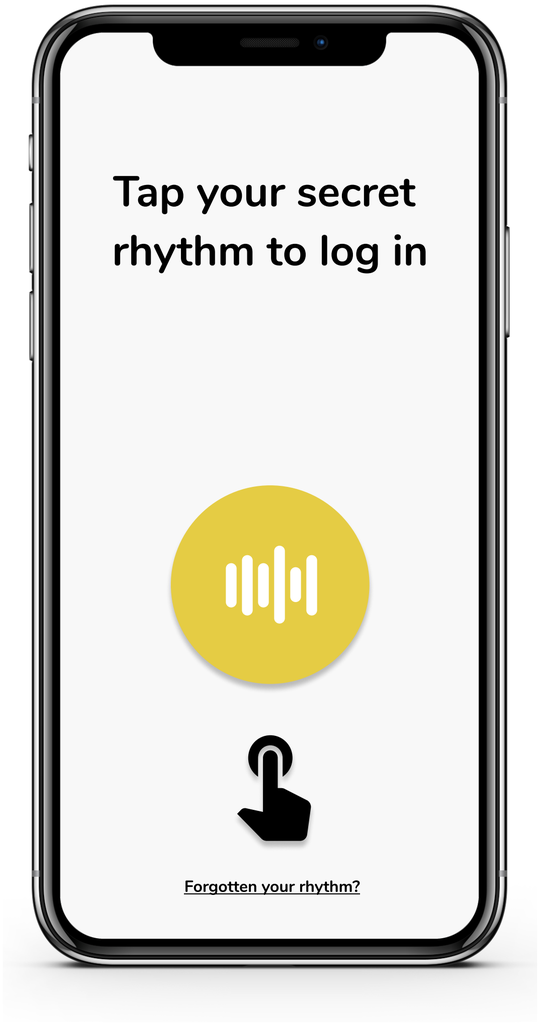
Prototype 1

- Users can enter their secret rhythm by taping the button.
- The input button gives visual feedback when tapped.
- The level of feedback is on par with what is generally available on the market.

Hypothesis:

A rhythm should be relatively easy to remember. This design will mainly be used when comparing prototypes 2 & 3.

Memory — Security



PROS:

Usability

- Input button easy to understand
- Button placement convenient for left and right handed users on various screen sizes [1]

CONS:

Accessibility

- user needs to see the button

1. Nick Babich (2017), https://www.uxpin.com/studio/blog/guide-mobile-app-design-best-practices-2018-beyond/

Prototype 2

- Users can enter their secret rhythm by taping anywhere on the screen.
- For increased security, input feedback is optional and users can choose between different feedback options:
  - vibration
  - “thumb print” display
  - no feedback

Hypothesis:

Minimal feedback reduces risk of over-the-shoulder attacks. Can make rhythms more difficult to remember.

Memory — Security

PROS:

Security
- Allows hidden passcode entry e.g. input with covered screen.
- Lack of feedback reduces risk of over-the-shoulder attacks.

Accessibility
- Input possible without seeing the screen increases accessibility for the visually impared [1].
- Whole screen acts as one large button.

CONS:

Usability
- App might appear frozen due to lack of response
- Passcode might harder to remember without visual / auditory feedback

1. Chen, Y., Sun, J., Zhang, R., & Zhang, Y. (2015). Your song your way: Rhythm-based two-factor authentication for multi-touch mobile devices. *2015 IEEE Conference on Computer Communications, IEEE INFOCOM 2015,* 2686-2694

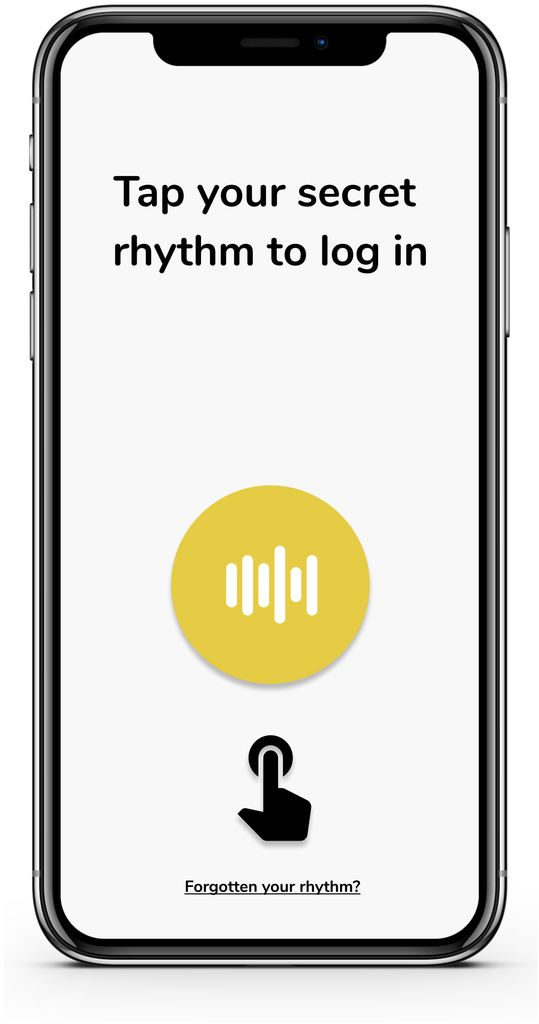
Prototype 3

- Users can enter their secret rhythm by taping the button.
- The app provides visual of auditory feedback in form of:
  - moving or morphing elements
  - vibration and auditory responses

Hypothesis:

Rich visual and auditory feedback helps users memorize their rhythm. But can be more vulnerable to over-the-shoulder attacks.

Memory — Security



PROS:

Usability
- Rich feedback might improve passcode memorization

Accessibility
- Visualization might help users with early stage dementia
- Visualization makes authentication more appealing for children

CONS:

Security
- increased risk for over-the-shoulder attacks