A Design Space for Security Indicators for Behavioural Biometrics on Mobile Touchscreen Devices

Lukas Mecke
Munich University of Applied Sciences, Germany
LMU Munich, Germany
lukas.mecke@hm.edu

Daniel Buschek
LMU Munich, Germany
daniel.buschek@ifi.lmu.de

Sarah Prange
Munich University of Applied Sciences, Germany
LMU Munich, Germany
sarah.prange@hm.edu

Florian Alt
Munich University of Applied Sciences, Germany
LMU Munich, Germany
florian.alt@hm.edu

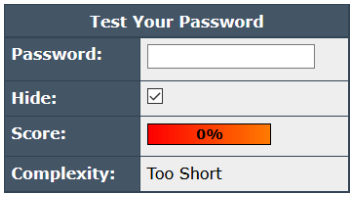
CHI'18 Extended Abstracts, April 21–26, 2018, Montreal, QC, Canada
ACM 978-1-4503-5621-3/18/04.
https://doi.org/10.1145/3170427.3188633

Abstract
We propose a design space for security indicators for behavioural biometrics on mobile touchscreen devices. Design dimensions are derived from a focus group with experts and a literature review. The space supports the design of indicators which aim to facilitate users' decision making, awareness and understanding, as well as increase transparency of behavioural biometrics systems. We conclude with a set of example designs and discuss further extensions, future research questions and study ideas.

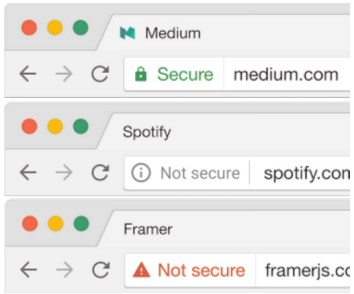
Author Keywords
Design Space; Behavioural Biometrics; Security Indicator; Mobile Touchscreen Devices; Focus Group

ACM Classification Keywords
H.5.2 [User Interfaces]; K.6.5 [Security and Protection]: Authentication

Introduction
Mobile devices nowadays often carry highly sensitive data like personal images, conversations or business information [4]. This raises the need for their protection. Beyond knowledge-based schemes likes PINs/patterns and tokens, behavioural biometrics have been introduced to the consumer market as another option or layer to facilitate mobile device security [6]. They authenticate users based on be-



(a)



(b)

Figure 1: Examples for classical security indicator approaches. The design of a security indicator for behavioural biometrics would possibly have to differ from that. In contrast to a password, security of behavioural biometrics depends on the individual person.
(a) Indicator of password strength using visual and textual feedback[a],
(b) Indication of a connection security proposed for the Chrome web browser by Felt et al. [3]

[a] www.passwordmeter.com

havioural characteristics like gait or typing patterns. However, it often remains unclear how to adequately communicate the security of such systems to the user.

Related work on visual indicators of password strength shows that users have misconceptions about what constitutes a strong password [9, 11]. The same trend was shown for behavioural biometrics by Ballard et al. [1], using handwriting recognition. Here, forgery was both more successful and harder to detect than users had expected.

Password meters address this by assessing and displaying a password's resilience against attacks (Fig. 1a). They can convince users to choose stronger passwords [5, 12]. Giving additional information and detailed, potentially sensitive feedback about the current strength can help users to improve their passwords [10]. Related work also showed that user awareness of password strength can be increased [9]. On the other hand, due to inconsistencies in current password strength estimations, more transparency might be needed to re-establish users trust in security indicators [2].

Existing work on security indication mainly covers passwords and websites [3] (Fig. 1b). Similar investigations for behavioural biometrics are mostly still missing. Moreover, in contrast to passwords, security of behavioural biometrics depends on the individual person; the same settings may lead to different security levels for different users. Thus, given potential impact and issues, adapting the design of security indicators is both relevant and challenging.

To make progress and support future designs, we present a design space for security indicators for behavioural biometrics on mobile touch screen devices. Our aim is to support the design of indicators which facilitate users' decision making, awareness and understanding, as well as increase transparency of behavioural biometrics systems.

The contribution of this work is two-fold: First we introduce a design space for security indicators for behavioural biometrics on mobile touch devices, which we derived from a focus group with experts and the literature. Second, we provide a set of examples on how our design space could be applied in future work for the development of security indicators.

Approach

To identify the design space we conducted a focus group with eight experts from, but not limited to, the fields of password meters, machine learning, user behaviour prediction and context-aware technology. Participants were introduced to the concepts of security indicators and behavioural biometrics. Subsequently they were asked to think of how a security indicator for behavioural biometrics would have to differ from classical approaches and what possible benefits they could have both for users and providers. Based on those results participants were asked to come up with concrete ideas and cluster those, filling missing design dimensions as needed.

Design Space

Our focus group discussions revealed several design dimensions. We clustered those dimensions, taking into account the related work, resulting in an additional layer of abstraction with three categories. Categories and dimensions are depicted in Figure 2 and described in detail below:

Purpose

The category that should be considered first is the purpose of the indicator in question. This includes two dimensions:

Goals: Potential goals designers might try to achieve include, but are not limited to: 1) *User Guidance:* By providing (personalised) security information, indicators may

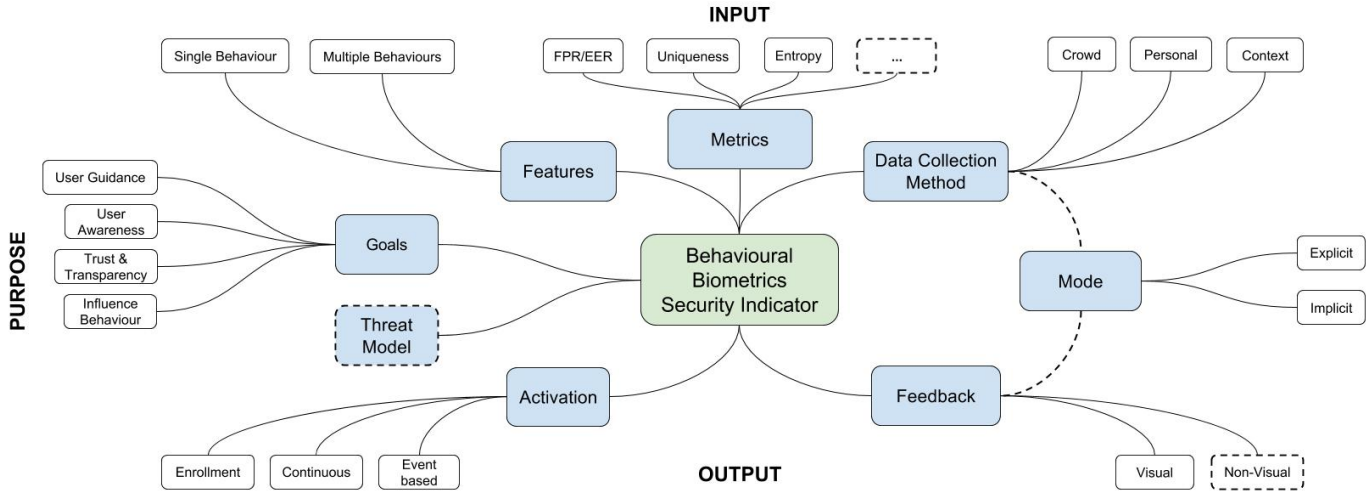


Figure 2: Our proposed design space consists of eight main dimensions. We classify dimensions in three categories: purpose-, input- and output-related. Dimensions added based on the literature review are indicated with dashed borders.

guide a user, for example, when choosing (a combination of) biometrics to select a more secure/unique behavioural feature. 2) *User Awareness*: By communicating levels of security and the system's internal reasoning, indicators may aim to increase user awareness (e.g., risks and benefits of the current settings w.r.t. behavioural biometrics). 3) *Trust & Transparency*: Taking the previous goal a step further, indicators may be designed to increase transparency and trust in the system [2] (i.e. by explaining how and why security assessments are made). This might in turn improve acceptance of the underlying behavioural biometric system. 4) *Influence Behaviour*: Similar to password meters, a behavioural biometrics indicator might aim to improve security by altering the user's behaviour in a way that generates more unique, and hence secure, user behavior.

Threat Model: When designing a security indicator we need to think about the threat model to which the indicated security is related. A comprehensive list of possible attacks on biometric systems can be found in [7]. A related aspect, for example, is the distinction between user verification/authentication and identification – different threats exist for both of them and indicator designs might differ as well.

Input

Several aspects of the underlying biometric system may be considered as input dimensions to inform the design of a corresponding indicator.

Features: The first choice is which biometric(s) should actually be used. This can be either a *single behaviour* or a combination of multiple behavioural traits (e.g., typing speed and pressure). In the latter case, further decisions

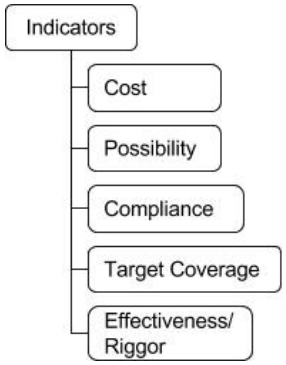


Figure 3: Classification of metrics for security indicators as proposed by Rudolph and Schwarz [8]. Some of these metrics are partially applicable to measure strength of behavioural biometrics.

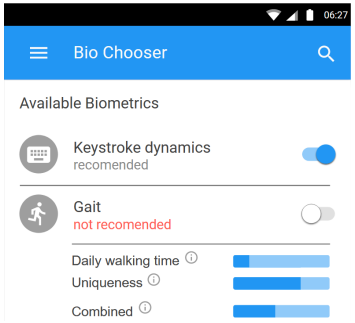


Figure 4: "Bio Chooser": A possible design for a security indicator to support users when deciding which behavioural biometrics to use, avoiding unnecessary collection of data (w.r.t. usability/security).

have to be made with respect to how those traits should be combined (*feature fusion*). This is relevant for the indicator, which, for example, might be designed to inform the user about the currently considered combination of behaviours.

Metric: There are several metrics to estimate the security of a biometric approach, such as system error rates (e.g., false positive rate, equal error rate), "uniqueness" of behaviour, and its entropy (similar to entropy as a measure of password strength). Beyond these metrics from our focus group, Rudolph and Schwarz [8] provide an extensive list of indicator metrics (compare Fig. 3).

Data Collection Method: Any metric to indicate security of a behavioural biometric system requires data on which to operate. This data can be either provided by the respective *user*, acquired from the user's *context* or collected from a *crowd*. The first option is likely the most common one (e.g., data from enrollment or past use). However, the use of crowd data can enable instant feedback without a "cold start", and context information enables adaptive estimation.

Output
Based on the input and purpose of the security indicator there are several ways to design the output.

Feedback: Similar to password strength, *visual* feedback can be used to represent the assessed security (Fig. 1). One possible option is textual feedback given in the form of scores ("90%"), assessments ("strong") or metaphors ("One in ten strangers might get access to your data using this behaviour for authentication"). Other representations might be diagrams or abstract. Additionally feedback might be given in a *non-visual* way, e.g., auditory or haptic.

Activation: There are several points in time when a security indicator might appear. We distinguish *enrollment* (i.e. only once at the beginning), *continuous* (may also be periodical) and *event based* (i.e., as a reaction to context changes, e.g. upon launching an app).

Mode: We distinguish *implicit* and *explicit* modes for two parts of the design space: 1) Data collection can happen either implicitly (e.g., background logging) or explicitly (e.g., enrollment procedure); 2) the indicator itself can be either implicit (e.g., an informative icon) or explicit (e.g., demanding a user action). In the case of an icon further considerations might be needed to ensure that users notice and understand [3, 13] the information. Different modes may be chosen for data source and feedback.

Using the Design Space

We illustrate the use of the design space with a set of examples, which cover different design choices along the identified dimensions. These examples were inspired by ideas from the focus group.

Example 1: "Bio Chooser" – Decision Support System
This indicator supports setup and *enrollment* of a multi-biometric system. Given multiple available biometrics, it indicates how each of them affects security, based on the individual user's behaviour (e.g., *personal* data from past usage or an enrollment sample). It could also include behaviour frequencies to "weight" the usefulness of certain biometrics (e.g., keystroke biometrics more useful if user types a lot), as well as common *contexts* (e.g., gait recognition might be less useful if user commutes via train). The indicator could *visually* present security implications like expected error rates. In this way, it aims to increase *awareness* and *guide* the user's choice. (compare Figure 4).

Example 2: "Crowd Radar" – Local Crowd-based Indicator
This indicator compares (local) *crowd* data with the user's own behaviour. It indicates the *uniqueness* of the user's

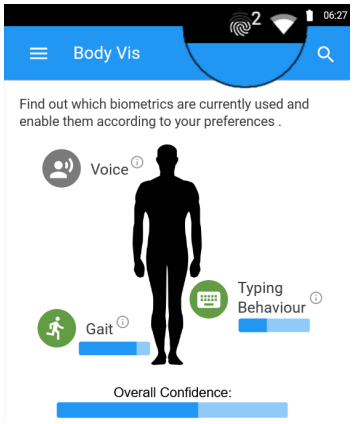


Figure 5: "Body Vis": A design giving continuous indication of the currently used biometrics and the system's confidence (both in the status bar and in detail).

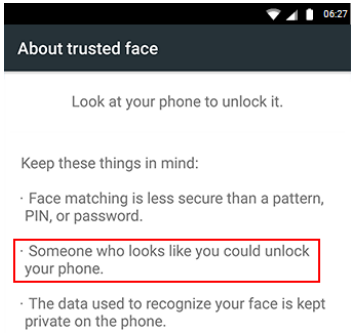


Figure 6: An example for a state of the art (static) biometric enrollment screen (Android Trusted Face) that might be improved by adding dynamic security indication.

behaviour in the vicinity and context. *Visual feedback* is presented as text: "x people in your vicinity have very similar behaviour". Beyond *awareness*, this could be extended towards *guidance*, for example, with recommendations on which (combinations of) biometrics to activate in this (crowd-)context.

Example 3: "Body Vis" – Visualizing Activated Biometrics
This indicator (Fig. 5) *continuously* displays the parts of the body that are currently tracked as a *personal data source* for continuous implicit authentication. This aims to facilitate *awareness* and *transparency*. The indicator might map confidence to colour or brightness to prepare the user for possible explicit (re-)authentications.

Discussion

Based on our focus group and literature research, we defined a comprehensive design space. Nevertheless, it should be regarded as a starting point with opportunities for extension, as discussed below.

Extending the Design Space
From studying our examples we found that indicating only security might not be enough. We hypothesize that usability would have a strong impact on user decisions regarding the use of behavioural biometrics as well and thus propose to extend the design space to account for that. For example, an indicator might display the amount of explicit authentication time saved with certain biometrics settings. It might also indicate how often the user would have to go through some overhead due to limited reliability. User preferences (e.g., speech input vs typing) might be considered, too. Overall, indicators focusing on such aspects could support users in finding individually suitable usability/security trade-offs.

Research Questions for Behavioural Biometric Indicators
This work lays the foundation for future investigation of indicator designs regarding specific research questions. These might include, for example, questions from password meters, such as: How can we nudge users to choose more secure settings? Do indicators support understanding (i.e. can users better judge the security of behavioural biometrics systems after using indicators)? Do users understand how attackers could try to gain access to their data? Does the content of the security indicator facilitate new threat models?

Concrete Example: Integration into Android Smart Lock
Google's behavioural biometrics system for Android devices displays a static text message to inform users about its security and related issues (e.g., "Someone who looks like you could unlock your phone", compare Fig. 6). This is an example for a concrete integration opportunity: We could replace the static text with a dynamic security indicator designed by considering our space. For example, this indicator might compare newly registered users with existing ones in the database to indicate how likely an unintended or malicious unlock from a stranger actually is. We could study the impact of this change on user perception and choices (e.g., with a mockup in the lab or in-the-wild replacement app).

Conclusion

We presented a design space for security indicators for behavioural biometrics on mobile touch screen devices. We derived its dimensions from a focus group and literature review. Our aim is to support the design of such indicators not only to increase users' understanding and awareness towards the security of new authentication methods using behavioural biometrics, but also to increase trust and transparency. We propose to extend this with usability aspects as a next step.

Acknowledgements

Work on this project was partially funded by the Bavarian State Ministry of Education, Science and the Arts in the framework of the Centre Digitisation.Bavaria (ZD.B). This research was supported by the Deutsche Forschungsgemeinschaft (DFG), Grant No. AL 1899/2-1.

REFERENCES

1. Lucas Ballard, Daniel Lopresti, and Fabian Monrose. 2007. Forgery quality and its implications for behavioral biometric security. *IEEE Transactions on Systems, Man, and Cybernetics, Part B (Cybernetics)* 37, 5 (2007), 1107–1118.
2. Xavier de Carné de Carnavalet and Mohammad Mannan. 2014. From Very Weak to Very Strong: Analyzing Password-Strength Meters. In *NDSS*, Vol. 14. Internet Society, 23–26.
3. Adrienne Porter Felt, Robert W Reeder, Alex Ainslie, Helen Harris, Max Walker, Christopher Thompson, Mustafa Embre Acer, Elisabeth Morant, and Sunny Consolvo. 2016. Rethinking Connection Security Indicators. In *Proc. of SOUPS'16*. USENIX Association, Denver, CO, 1–14.
4. Amy K Karlson, AJ Brush, and Stuart Schechter. 2009. Can i borrow your phone?: understanding concerns when sharing mobile phones. In *Proc. of CHI'09.* ACM, ACM, New York, NY, USA, 1647–1650.
5. Saranga Komanduri, Richard Shay, Lorrie Faith Cranor, Cormac Herley, and Stuart E Schechter. 2014. Telepathwords: Preventing Weak Passwords by Reading Users' Minds. In *USENIX Security Symposium*. USENIX Association, San Diego, CA, 591–606.
6. Lawrence O'Gorman. 2003. Comparing passwords, tokens, and biometrics for user authentication. *Proc. IEEE* 91, 12 (2003), 2021–2040.
7. Chris Roberts. 2007. Biometric attack vectors and defences. *Computers & Security* 26, 1 (2007), 14 – 25.
8. Manuel Rudolph and Reinhard Schwarz. 2012. A critical survey of security indicator approaches. In *Proc. of ARES'12*. IEEE, 291–300.
9. Tobias Seitz and Heinrich Hussmann. 2017. PASDJO: Quantifying Password Strength Perceptions with an Online Game. In *Proc. of OzCHI'17*. ACM, New York, NY, USA, 117–125.
10. Blase Ur, Felicia Alfieri, Maung Aung, Lujo Bauer, Nicolas Christin, Jessica Colnago, Lorrie Faith Cranor, Henry Dixon, Pardis Emami Naeini, Hana Habib, and others. 2017. Design and evaluation of a data-driven password meter. In *Proc. of CHI 2017*. ACM, ACM, New York, NY, USA, 3775–3786.
11. Blase Ur, Jonathan Bees, Sean M Segreti, Lujo Bauer, Nicolas Christin, and Lorrie Faith Cranor. 2016. Do Users' Perceptions of Password Security Match Reality?. In *Proc. of CHI'16*. ACM, ACM, New York, NY, USA, 3748–3760.
12. Blase Ur, Patrick Gage Kelley, Saranga Komanduri, Joel Lee, Michael Maass, Michelle L Mazurek, Timothy Passaro, Richard Shay, Timothy Vidas, Lujo Bauer, and others. 2012. How does your password measure up? The effect of strength meters on password creation. In *USENIX Security Symposium*. USENIX, Bellevue, WA, 65–80.
13. Min Wu, Robert C Miller, and Simson L Garfinkel. 2006. Do security toolbars actually prevent phishing attacks?. In *Proc. of CHI'06*. ACM, ACM, New York, NY, USA, 601–610.