LMU LUDWIG-MAXIMILIANS-UNIVERSITÄT MÜNCHEN
Media Informatics munich
CODE RI Research Institute Cyber Defence Bundeswehr University Munich
Usable Security and Privacy Group

Communicating Device Confidence Level and Upcoming Re-Authentications in Continuous Authentication Systems on Mobile Devices

Lukas Mecke, Sarah Delgado Rodriguez, Daniel Buschek, Sarah Prange and Florian Alt

Imagine…

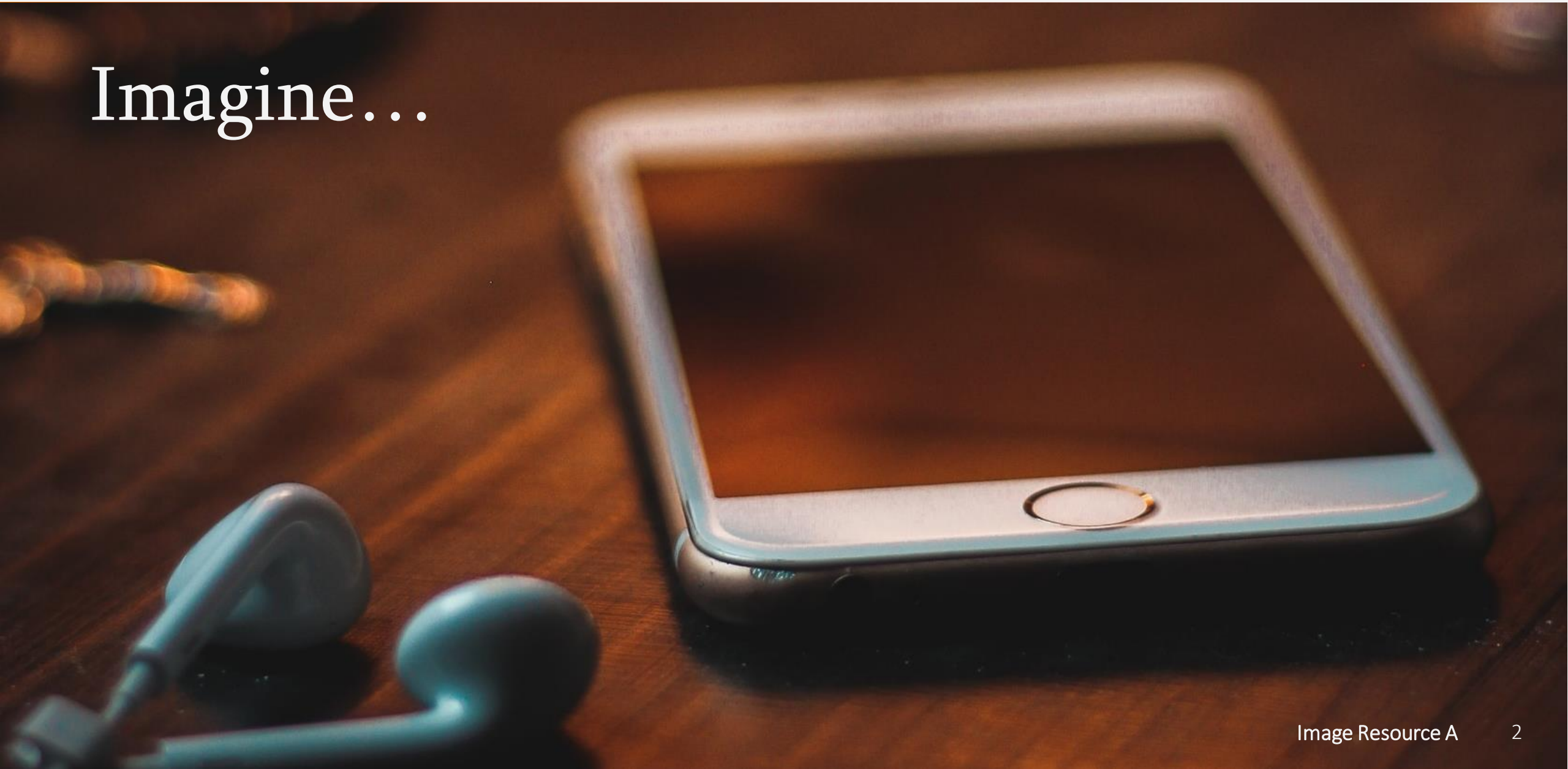


Image Resource A

LMU LUDWIG-MAXIMILIANS-UNIVERSITÄT MÜNCHEN
Media Informatics munich
CODE RI Research Institute Cyber Defence Bundeswehr University Munich
Usable Security and Privacy Group

Communicating Device Confidence Level and Upcoming Re-Authentications in Continuous Authentication Systems on Mobile Devices

Lukas Mecke, Sarah Delgado Rodriguez, Daniel Buschek, Sarah Prange and Florian Alt

Authentication on Smartphones

- Explicitly for each session
  - Secret
  - Token
  - Biometrics

Image Resource B

Authentication on Smartphones

- Explicitly for each session
  - Secret
  - Token
  - Biometrics

Authentication overhead & limited security

Image Resource B

LMU LUDWIG-MAXIMILIANS-UNIVERSITÄT MÜNCHEN
Media Informatics munich
CODE RI Research Institute Cyber Defence Bundeswehr University Munich
Usable Security and Privacy Group

Communicating Device Confidence Level and Upcoming Re-Authentications in Continuous Authentication Systems on Mobile Devices

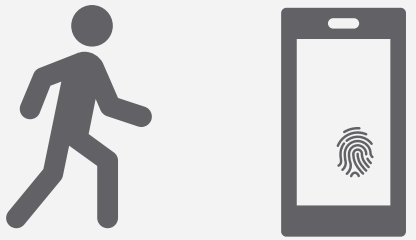
Lukas Mecke, Sarah Delgado Rodriguez, Daniel Buschek, Sarah Prange and Florian Alt

Continuous/Implicit Authentication

Context-Aware

- Pre-established authentication-settings for usage contexts

Behavioral Biometrics



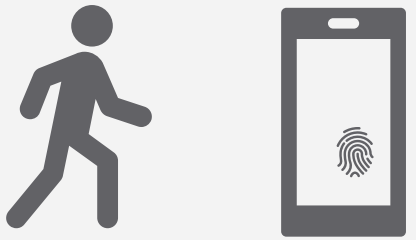
- Comparison to owners' behavior
  → device confidence level

→ explicit (re-)authentication

Continuous/Implicit Authentication

Context-Aware

Behavioral Biometrics



Fewer explicit authentications?

Use Cases of Implicit Authentication

No-Authentication Users

sole method

Khan, 2014

→ few (re-)authentications

Explicit Authentication Users

second barrier

Li, 2013

→ additional re-authentications

Use Cases of Implicit Authentication

No-Authentication Users

Explicit Authentication Users

Extent of security increase?

Re-Authentication

Delayed

- (Re-)authentication at the beginning of next session

→ minor security increase

Immediate

Khan, 2015

- Direct (re-)authentication interruption

→ major security increase

Re-Authentication

Delayed

Immediate Khan, 2015

False rejects → usability challenges

Usability Issues of Implicit Authentication

- No influence on timing of re-authentications
- Unpredictable interruption
- No indication of system status

Agarwal, 2016; Crawford and Renaud, 2014; Khan, 2015; McFarlane, 2002

Image Resource C

Usability Issues of Implicit Authentication

- No influence on timing of re-authentications
- Unpredictable interruption
- No indication of system status

→ Annoyance

Image Resource C

Concept

- **Voluntary** re-authentications
- **Short Term:** announces interruptions & incl. grace period
- **Long Term:** indicates systems' state

Method: Focus Group (n = 5)

LMU LUDWIG-MAXIMILIANS-UNIVERSITÄT MÜNCHEN
Media Informatics munich
CODE RI Research Institute Cyber Defence Bundeswehr University Munich
Usable Security and Privacy Group

Communicating Device Confidence Level and Upcoming Re-Authentications in Continuous Authentication Systems on Mobile Devices

Lukas Mecke, Sarah Delgado Rodriguez, Daniel Buschek, Sarah Prange and Florian Alt

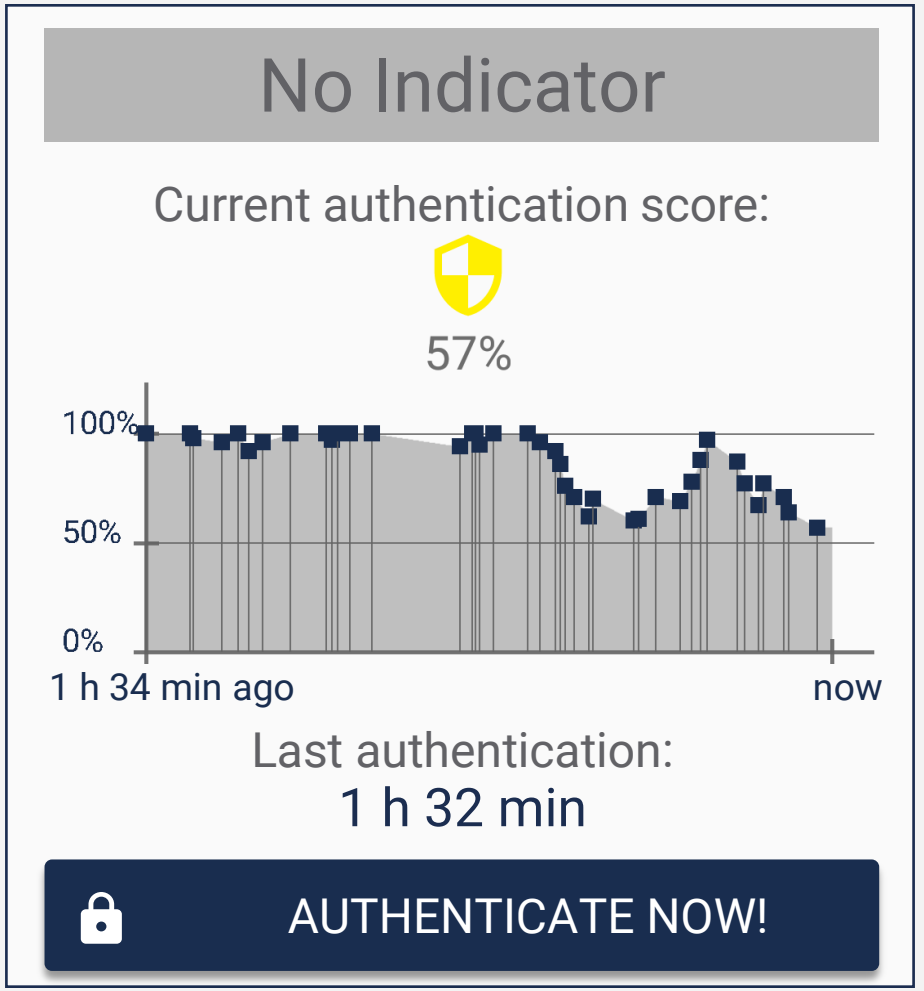
Research Questions

1. Can indicators **reduce annoyance** caused by re-authentications?
2. Do **other factors** influence this?
3. Do indicators **nudge users to voluntarily re-authenticate**?
4. How do users respond to the **introduction of voluntary re-authentication**?

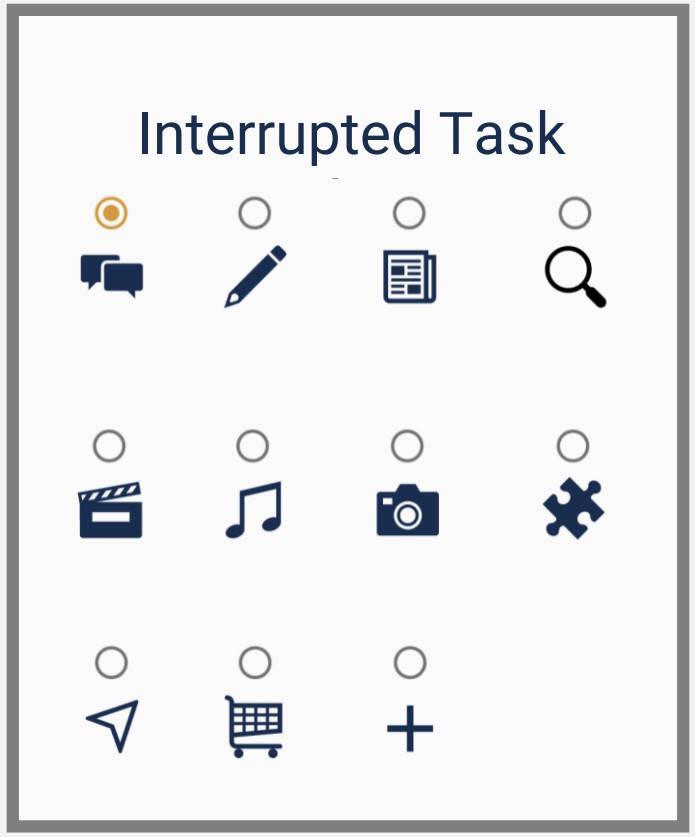
Prototype

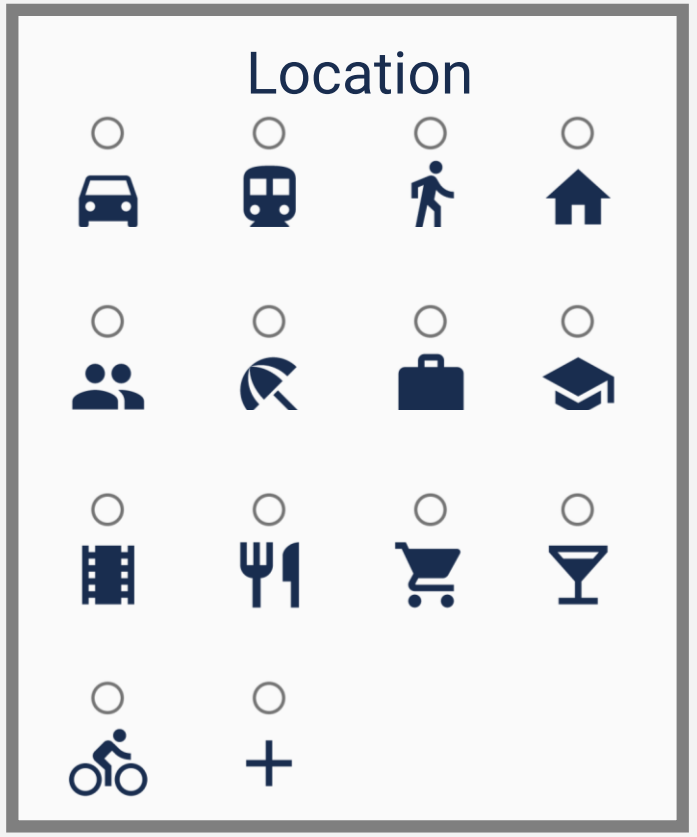
AUTHENTICATION INDICATOR

- Android App
- Chance-based simulated implicit authentication system
- Modifications of device confidence level triggered by touch interactions



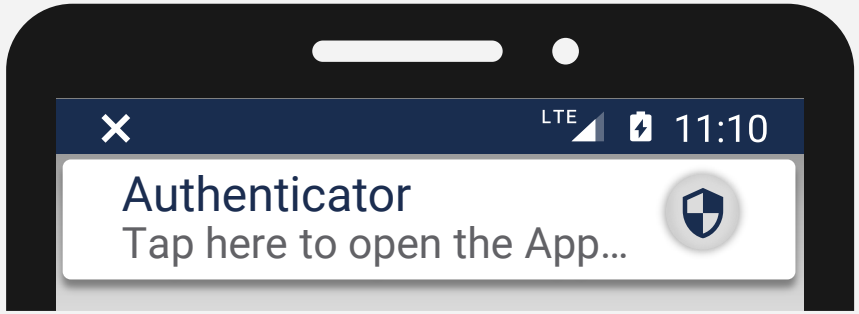
In-Situ Experience Sampling



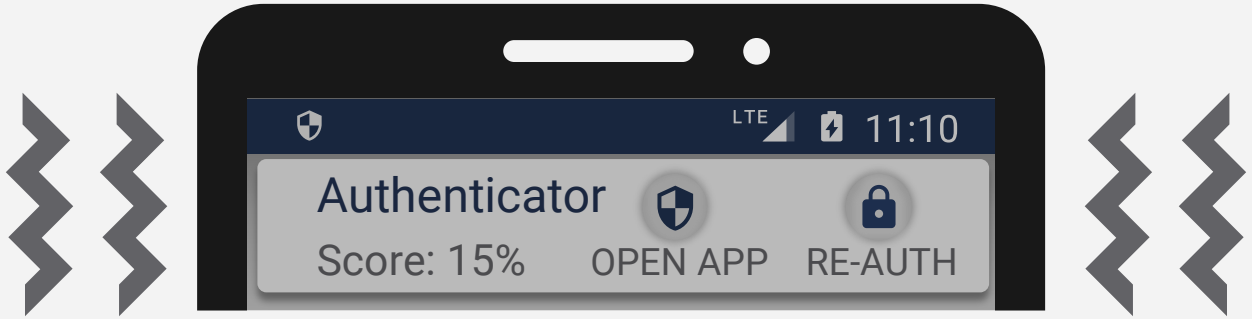


Experimental Conditions

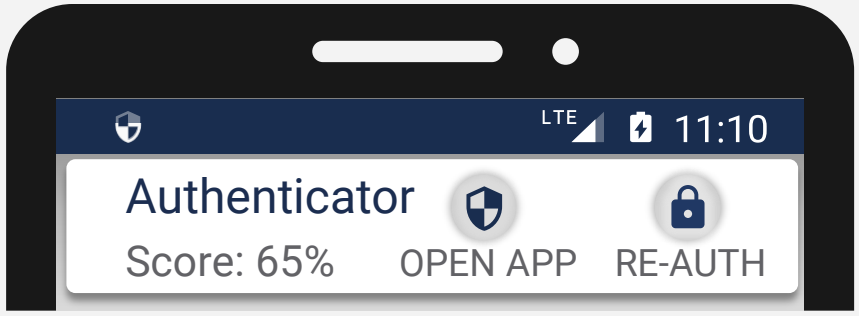
No Indicator



Short Term Indicator Agarwal, 2016



Long Term Indicator



Short & Long Term Indicator

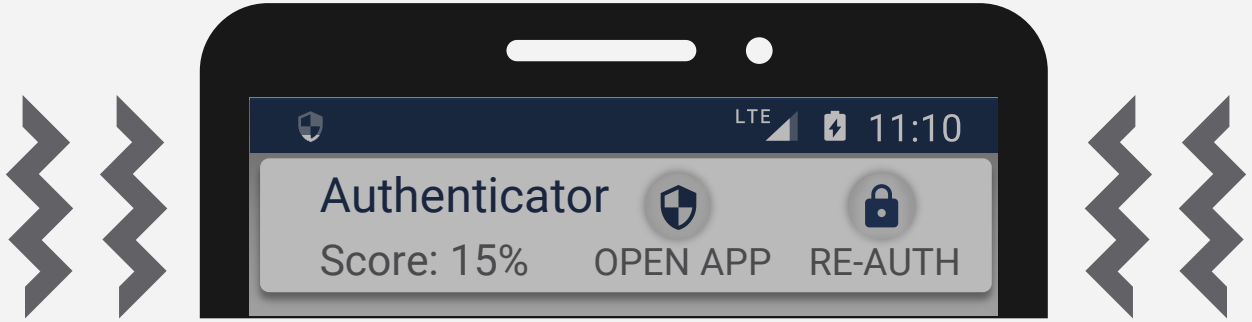
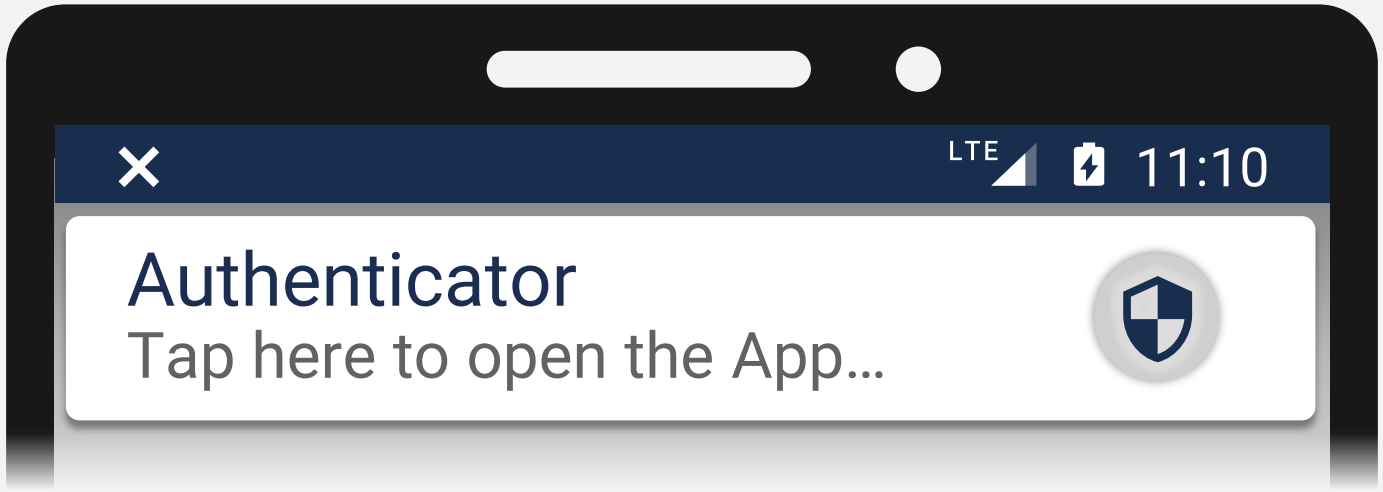


Image Resource D

No Indicator

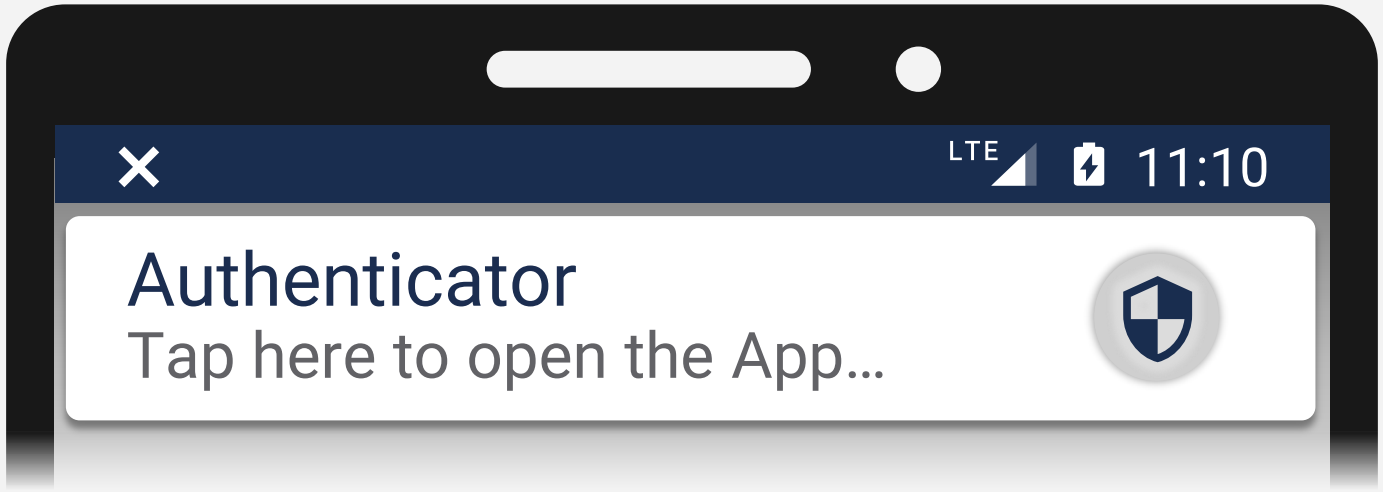
- Unannounced re-authentication
- No indication of the device confidence level
- Basic notification + neutral symbol in status bar



Short Term Indicator

No imminent re-authentication

- Identical to „No Indicator“-condition



Short Term Indicator

Imminent re-authentication

- Pop-up notification + vibration
- Gradual dimming out of the screen → 8s grace period

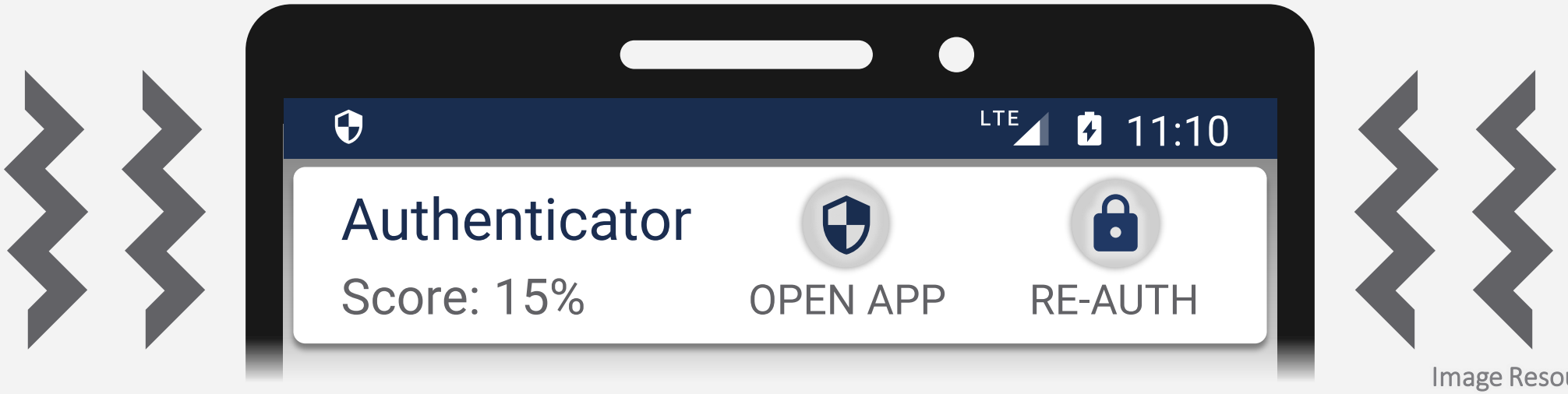
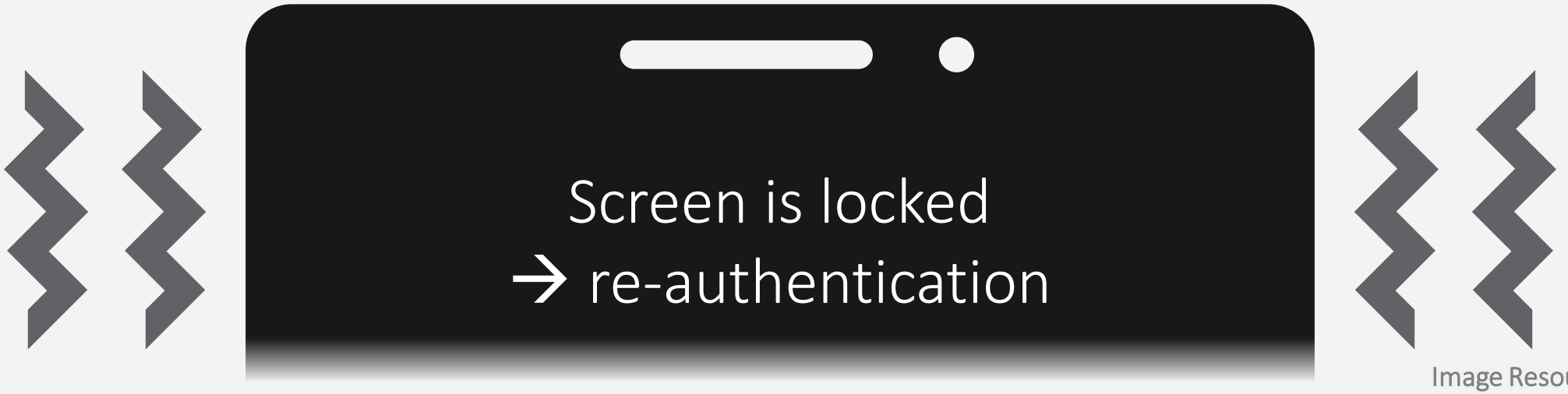


Image Resource D

Short Term Indicator

Imminent re-authentication

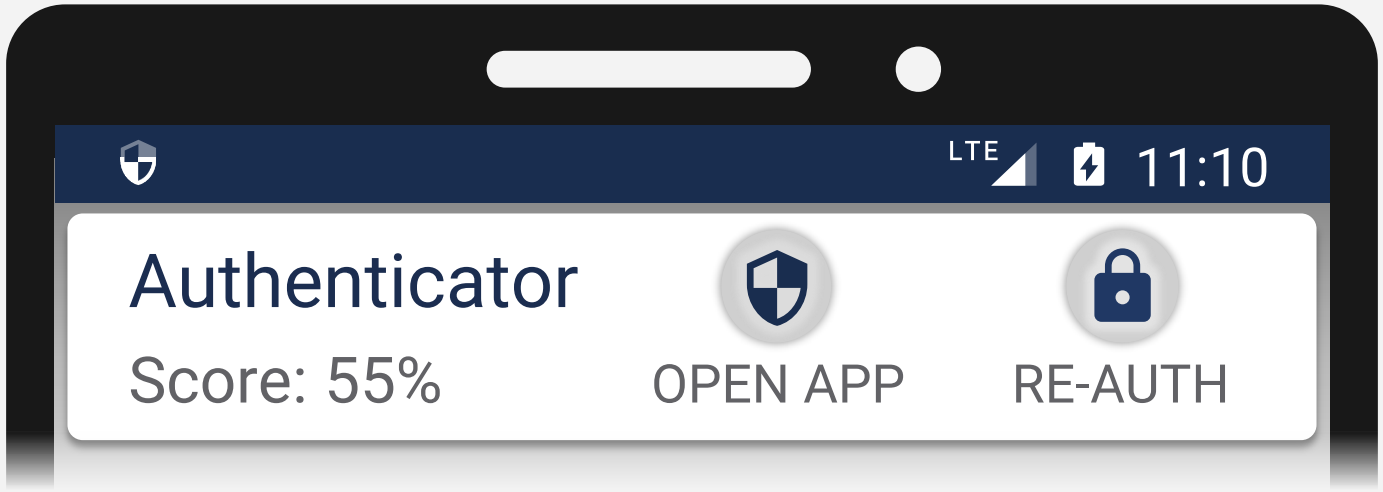
- Pop-up notification + vibration
- Gradual dimming out of the screen → 8s grace period



Long Term Indicator

Consistent indication at any time

- „Fuel“-visualization of the device confidence level
- Notification → identical to pop-up notification of the ST



Short & Long Term Indicator

Combination of Short and Long Term Indicators

Short & Long Term Indicator

Combination of Short and Long Term Indicators

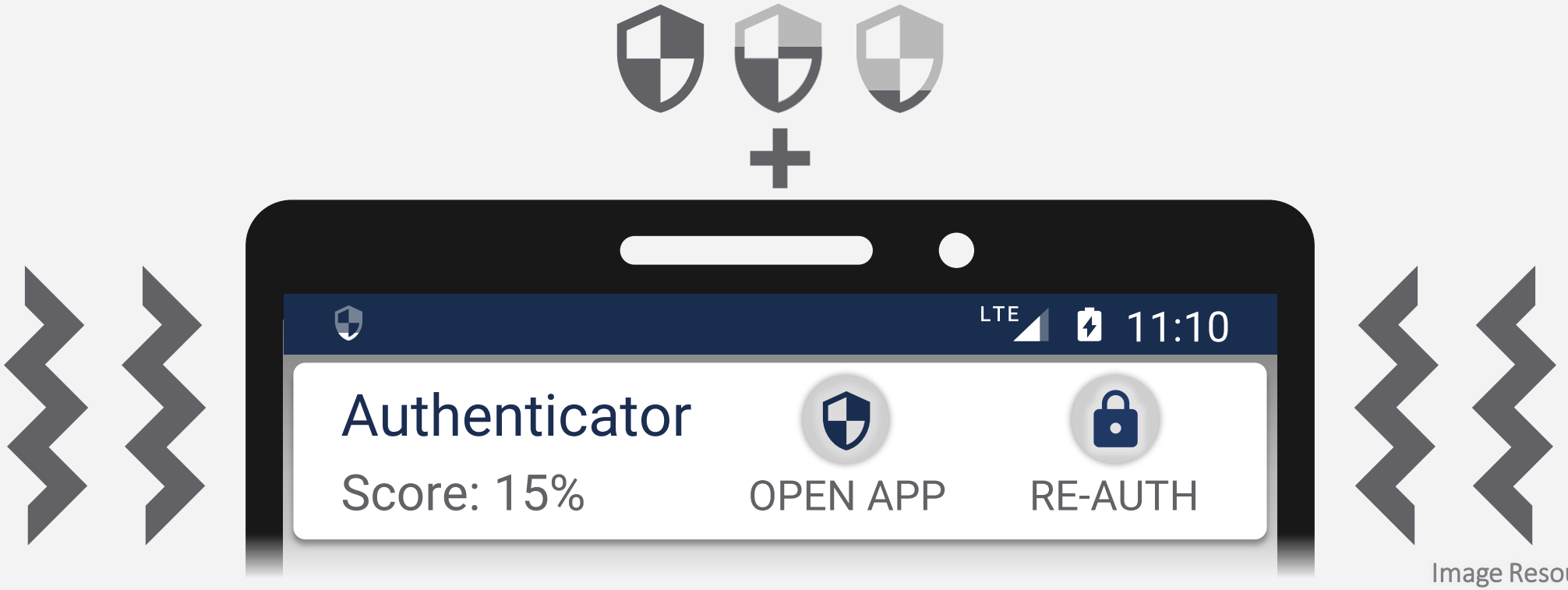


Image Resource D

Short & Long Term Indicator

Combination of Short and Long Term Indicators

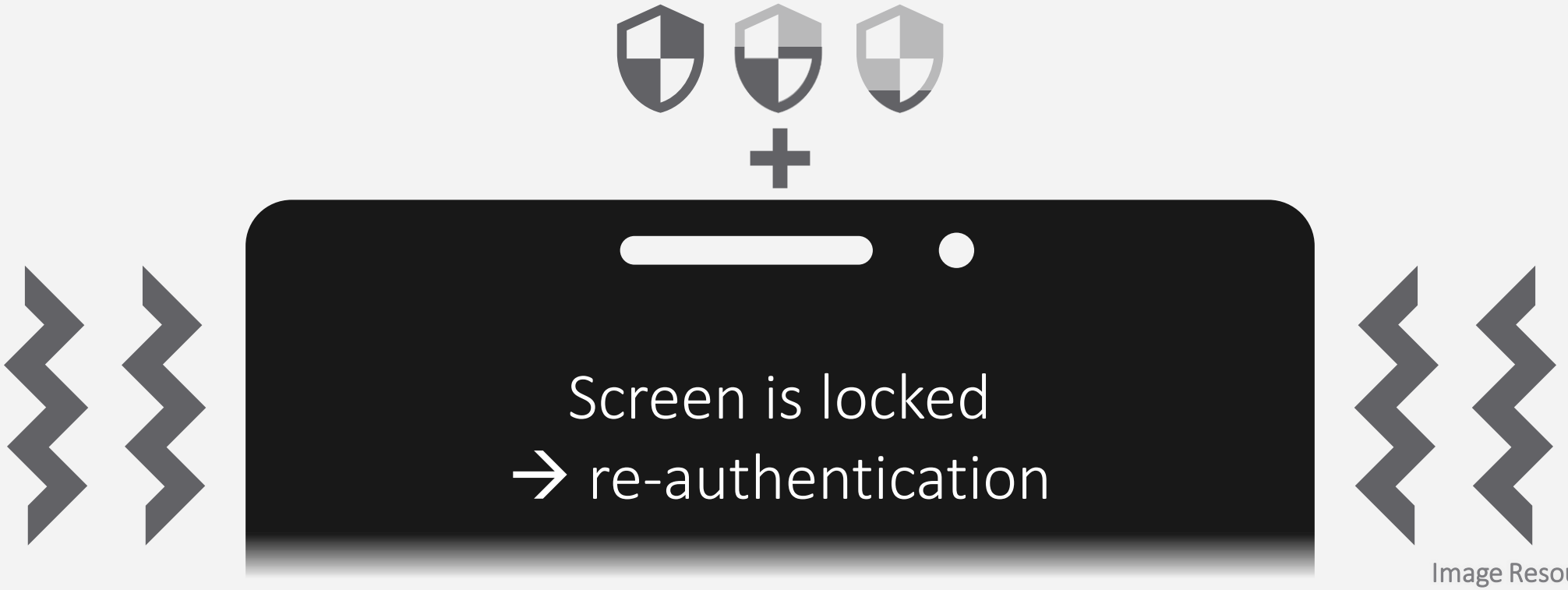


Image Resource D

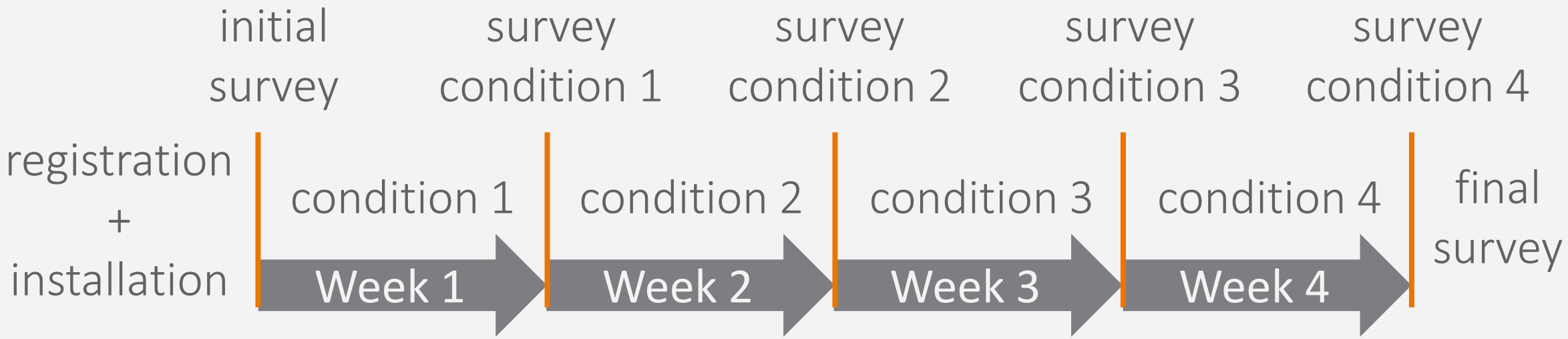
User Study

User Study

- Field study (n = 32)
- Within-subject design
- **Independent Variable:** Type of indicator (four conditions)

  → Two baselines:
  No Indicator and Short Term Indicator

Timeline of the Field Study



order counterbalanced

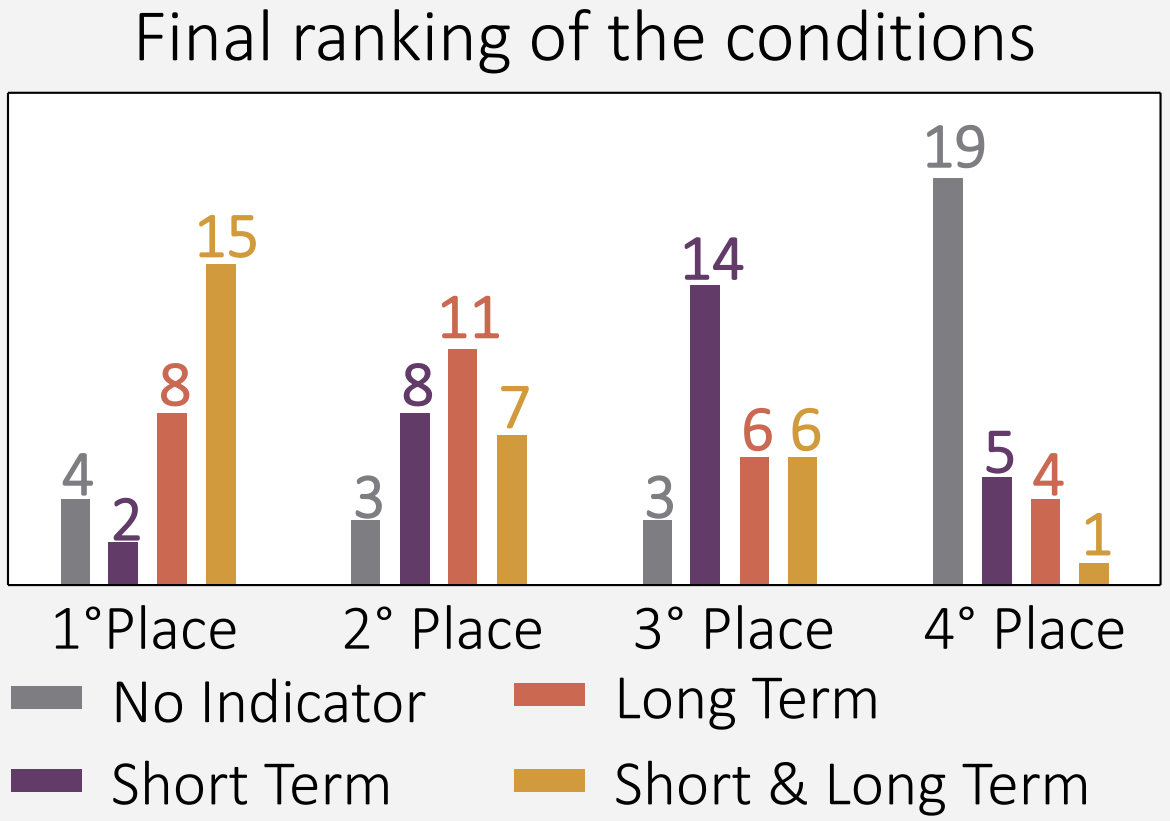
Dependent Variables

- Device usage (unlocks, touches, executed apps)
- Re-authentications (voluntary?, interrupted app)
- In-situ experience sampling
- Online questionnaires
- Optional final interview

Results

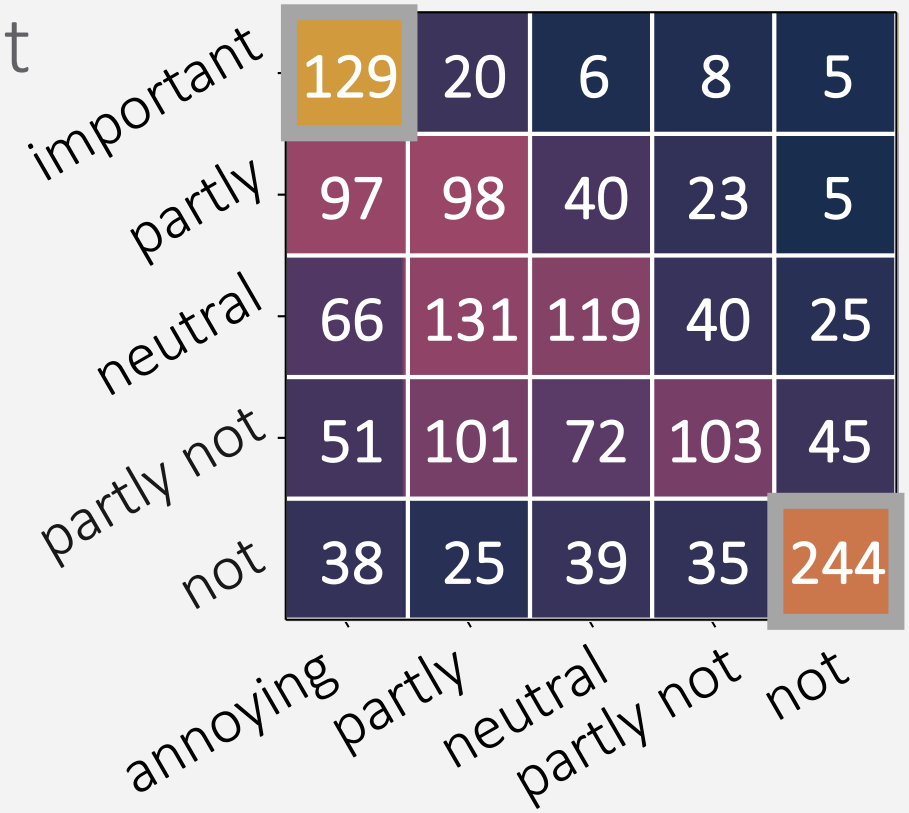
Perception of Indicators

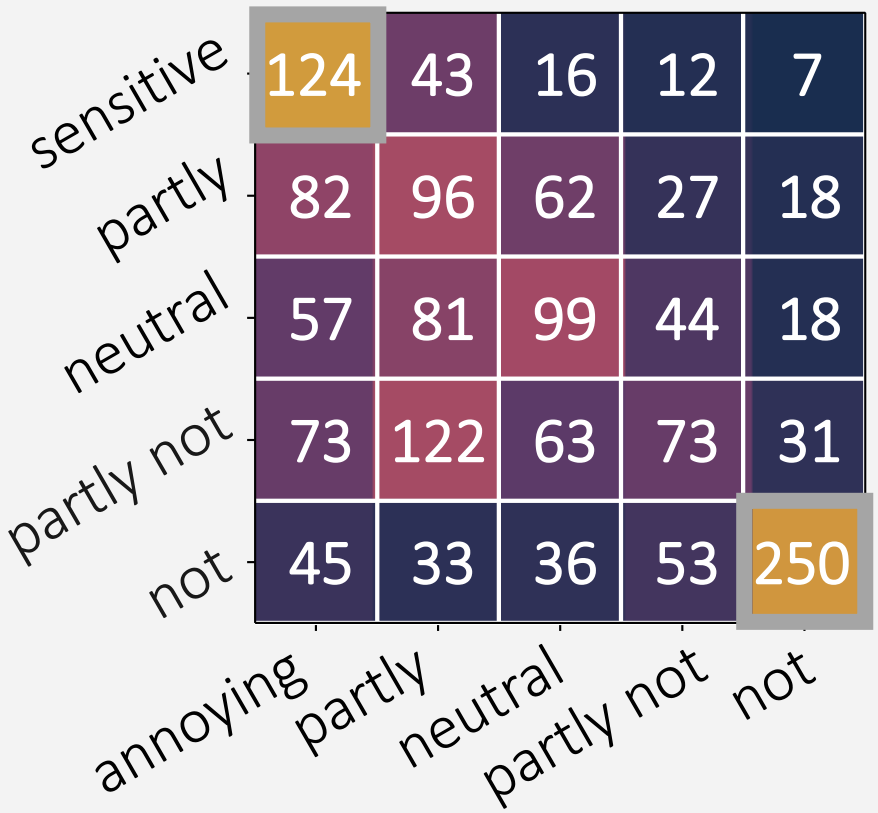
- All indicators preferred to no indication
- Users felt particularly motivated to voluntarily re-authenticate by the combination of both indicators



Insights on Annoyance

- No significant effect of indicators
- Impact of sensitivity & importance





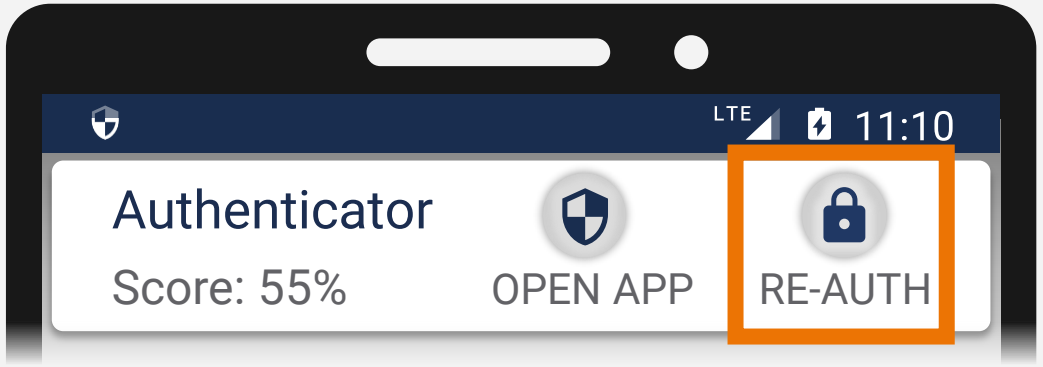
Insights on Annoyance

- Strongly influenced by interrupted task

Connover Post Hoc – only significant results			
		df	p_{bonf}
nothing/voluntary (Mdn = 5)	read (Mdn = 3)	100	0.002
	search (Mdn = 2)	100	< .001
	write (Mdn = 2)	100	< .001
	chat (Mdn = 2)	100	< .001
Medians of in-situ reported annoyance	others (Mdn = 2)	100	< .001

Voluntary Re-Authentications

- Not less annoying than forced interrupts
- Mentioned as positive feature
- Often used → 33.6% of all re-authentications
- Positively impacted by all indicators



Implications

Scheduling of Re-Authentications

- Sensitivity of the task

  → Delay if non-sensitive data is accessed
- Importance of the task

  → Delay interruptions of important tasks to improve usability
- Recent changes in device confidence level

  → Rapid decrease might indicate intruder → immediate

Take-Home Messages

Topic: Impact of **short- and long-term indication** and the possibility of **re-authenticating voluntarily** on users' perception.

Take-Home Messages

Topic: Impact of **short- and long-term indication** and the possibility of **re-authenticating voluntarily** on users' perception.

- **Indicators were preferred**, but did **not significantly reduce annoyance**
- **Annoyance** is influenced by **sensitivity, importance** and the **specific task**
- **All indicators** increased the use of **voluntary re-authentications**, which were perceived as **positive and frequently used**

Communicating Device Confidence Level and Upcoming Re-Authentications in Continuous Authentication Systems on Mobile Devices

Sarah Delgado Rodriguez
S.Delgado@campus.lmu.de

Image - Resources:

A. https://www.pexels.com/photo/blur-blurred-background-bokeh-cellphone-1156684/
B. https://www.pexels.com/photo/high-angle-shot-of-laptop-and-smartphone-257923/
C. https://www.pexels.com/photo/man-wearing-brown-suit-jacket-mocking-on-white-telephone-1587014/
D. Google Material Icons from https://material.io/resources/icons

All photos from www.pexels.com are available under the Creative Common Zero (CC0) License.

Resources

Please note that this list contains only the most important resources for this presentation. See our paper for all complete listing.

- Lalit Agarwal, Hassan Khan, and Urs Hengartner. Ask me again but don't annoy me: Evaluating reauthentication strategies for smartphones. In Symposium on Usable Privacy and Security (SOUPS), 2016.
- Heather Crawford and Karen Renaud. Understanding user perceptions of transparent authentication on a mobile device. Journal of Trust Management, 1(1):7, 2014.
- Hassan Khan, Aaron Atwater, and Urs Hengartner. Itus: an implicit authentication framework for android. In Proceedings of the 20th annual international conference on Mobile computing and networking, pages 507–518. ACM, 2014.
- Hassan Khan, Urs Hengartner, and Daniel Vogel. Usability and security perceptions of implicit authentication: Convenient, secure, sometimes annoying. In Eleventh Symposium On Usable Privacy and Security (SOUPS 2015), pages 225–239, Ottawa, 2015. USENIX Association.
- Lingjun Li, Xinxin Zhao, and Guoliang Xue. Unobservable re-authentication for smartphones. In NDSS, volume 56, pages 57–59, 2013.
- Daniel C McFarlane. Comparison of four primary methods for coordinating the interruption of people in humancomputer interaction. Human-Computer Interaction, 17(1):63–139, 2002.