TECHNISCHE UNIVERSITÄT DARMSTADT

Privacy and Trust for Mobile Users

IPAT SEMINAR – FINAL PRESENTATIONS

TECHNISCHE UNIVERSITÄT DARMSTADT

SCHEDULE

Privacy and Trust for Mobile Users

iPAT Seminar WiSe23/24 – Final Presentation – Talks Schedule
When: Friday 16.02.2024 @10:00 – 12:30
Where: S202/C110

Start	End	1st Session	Discipline	Topic	Presenter(s)	Adivsor(s)
10:00	10:05			Greetings and Starting Note		(Simon Althaus, Ephraim Zimmer)
10:05	10:30		Psychology	Personalization of Privacy Assistants	Sebastian Gandenberger, Vahan Demirci, Bedirhan Sahin, Till Feldner	Simon Althaus, Sara Hahn, Fransisca Hapsari
10:30	10:50		Sociology	Kritik an Social Media und der Macht von Onlineplattformen	Katharina Worster	Florian Müller, Rebecca Heigl
10:50	11:10			Algorithmic Governance & Nudging	Marvin Fink	Florian Müller, Enno Steinbrink
11:10	11:20			BREAK (Tentative/Optional)		
		2nd Session	**Discipline**	**Topic**	**Presenter(s)**	**Adivsor(s)**
11:20	11:40		Computer Science	Privacy and Utility Perception Compared to Sensor Awareness and Their Actual Privacy Implications	Beliz Balim	Matthias Gazzari, Fransisca Hapsari
11:40	12:00			Attacking Privacy in Electric Vehicle Charging Stations	Joshua Moell	Carsten Schmidt, Sara Hahn
12:00	12:20			Civil Sensor Data During War Time And In Crises	Johanna Jarsch	Enno Steinbrink, Matthias Gazzari
12:20	12:30			Closing Remarks		(Simon Althaus, Ephraim Zimmer)

TECHNISCHE UNIVERSITÄT DARMSTADT

Privacy and Trust for Mobile Users

CUSTOMIZATION OPTIONS AND PERSONAL PREFERENCES

Development and survey of a questionnaire to optimize the Privacy Buddy

Sebastian Gandenberger, Vahan Demirci, Bedirhan Sahin & Till Feldner

Faculty of Human Sciences - Work and Engineering Psychology

TECHNISCHE UNIVERSITÄT DARMSTADT

Privacy and Trust for Mobile Users

AGENDA

1 Motivation & Goal

2 Theoretical background

3 Development of the questionnaire

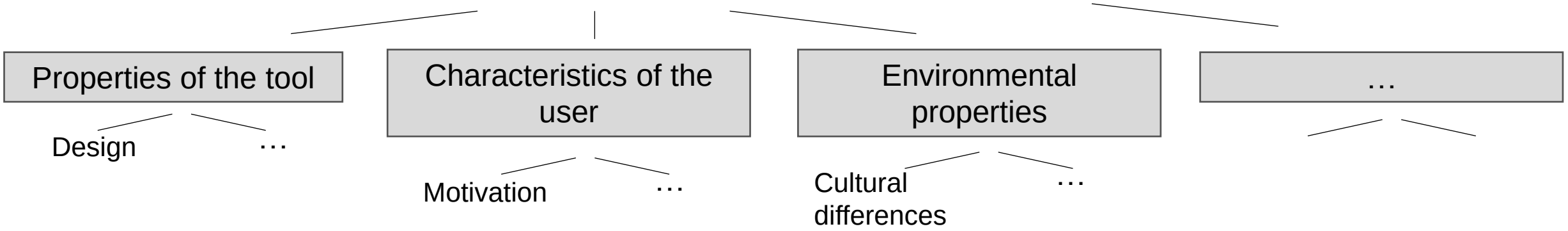
4 First results

5 Outlook

MOTIVATION

- Personal Privacy Assistants (PPA) are a promising approach to improve online privacy behavior [1][2][3]
- Limitiation of the current approach: users need to activly use the PPA

What determines whether a potential user actively uses the tool?



→It‘s a complex question and the current state of research doesn‘t give a clear answer!

TECHNISCHE UNIVERSITÄT DARMSTADT

MOTIVATION

Privacy and Trust for Mobile Users

- Personal Privacy Assistants (PPA) are a promising approach to improve online privacy behavior [1][2][3]
- Limitiation of the current approach: users need to activly use the PPA

What determines whether a potential user actively uses the tool?

→It‘s a complex question and the current state of research doesn‘t give a clear answer!

The main focus of research:

- Inter-individual differences in the wishes and needs regarding a PPA
- Identification of user groups with shared characteristics
- Evaluation of various features by potential users

GOAL

Inter-individual differences in the wishes and needs regarding a PPA

Identification of user groups with shared characteristics

Evaluation of various features by potential users

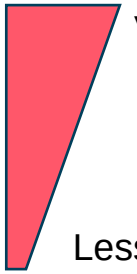
Concrete suggestions:

- **Which features** are generally supported by potential users
- **How** should the features be **designed**?
- **Where does individualization** make sense due to different wishes?
- **Common characteristics** of user groups

THEORETICAL BACKGROUND

1. Which **psychological needs** are the most relevant for a PPA?

Security, Autonomy, Competence
Meaning, Relatedness
Stimulation, Popularity



[1]

2. Are there **different groups** of potential users?

a)

Fundamentalists	**Pragmatists**
- *Age*: 31-50 years	-*Age*: under 30 and over 51 years
-*Technology affinity*: comparatively high	-*Technology affinity*: comparatively low
-*Privacy concerns*: comparatively high	-*Privacy concerns*: rather low

[2]

b)

Undecided	**Worried**	**Experienced**	**Insecure**	**Unconcered**
Low knowledge	High knowledge	High knowledge	Low knowledge	Low knowledge
Medium motivation	High motivation	Low motivation	Medium to low motivation	Lowest motivation
Low willingness to trust	Low willingness to trust	Low willingness to trust	Medium privacy concerns	Low privacy concerns

[3]

DEVELOPMENT OF THE QUESTIONNAIRE

TECHNISCHE UNIVERSITÄT DARMSTADT

Privacy and Trust for Mobile Users

Scientific questionaires (validity tested)
+ sociodemographic data

- Affinity for technology
- Privacy self-assessment
- Privacy concerns
- Computer security intentions
- Needs questionnaire

+

Newly developed questionaire

Specific questions

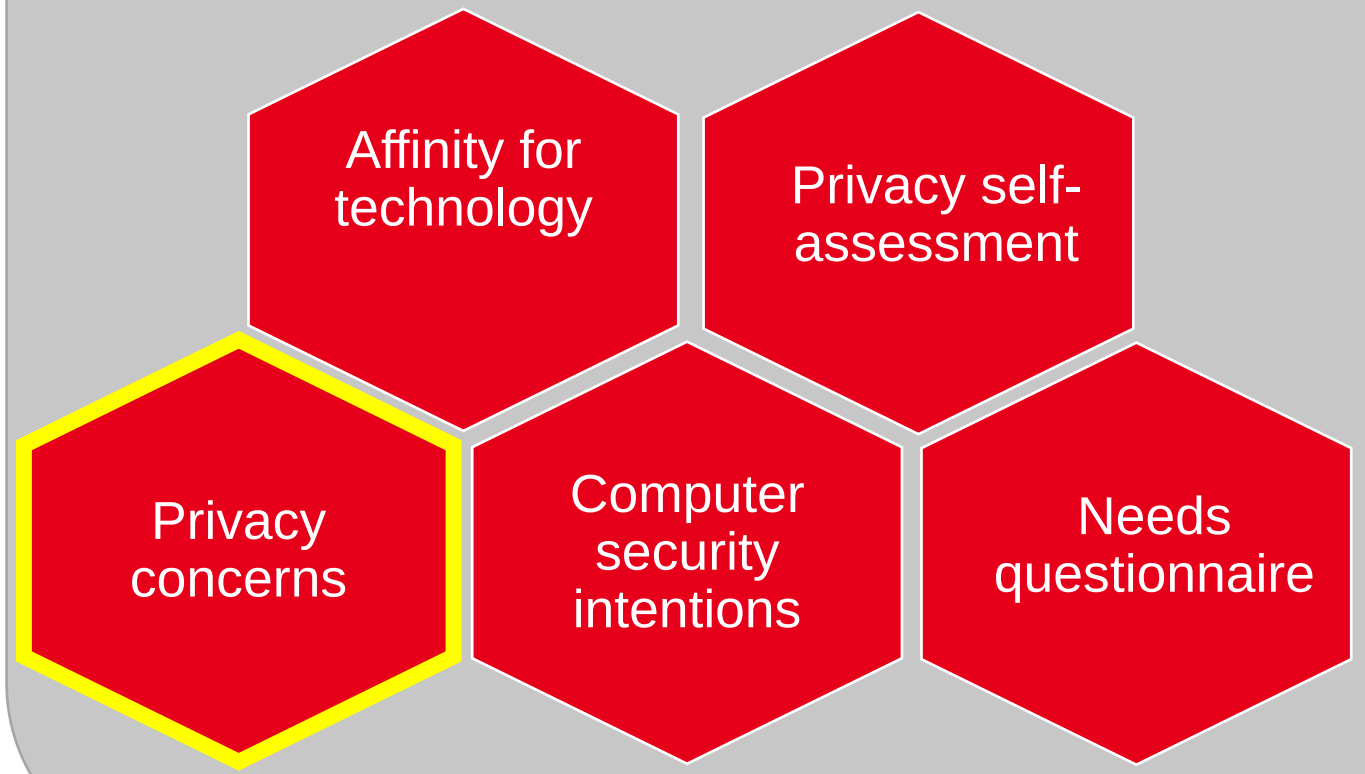
(learning content, user interface, leaderboard, data protection notifications and recommendations from contacts)

DEVELOPMENT OF THE QUESTIONNAIRE

TECHNISCHE UNIVERSITÄT DARMSTADT

Privacy and Trust for Mobile Users

Scientific questionaires (validity tested)



Newly developed questionaire

Specific questions

(learning content, user interface, leaderboard, data protection notifications and recommendations from contacts)

PRIVACY CONCERNS

“It bothers me to share my personal information with so many companies.”

Short instruction

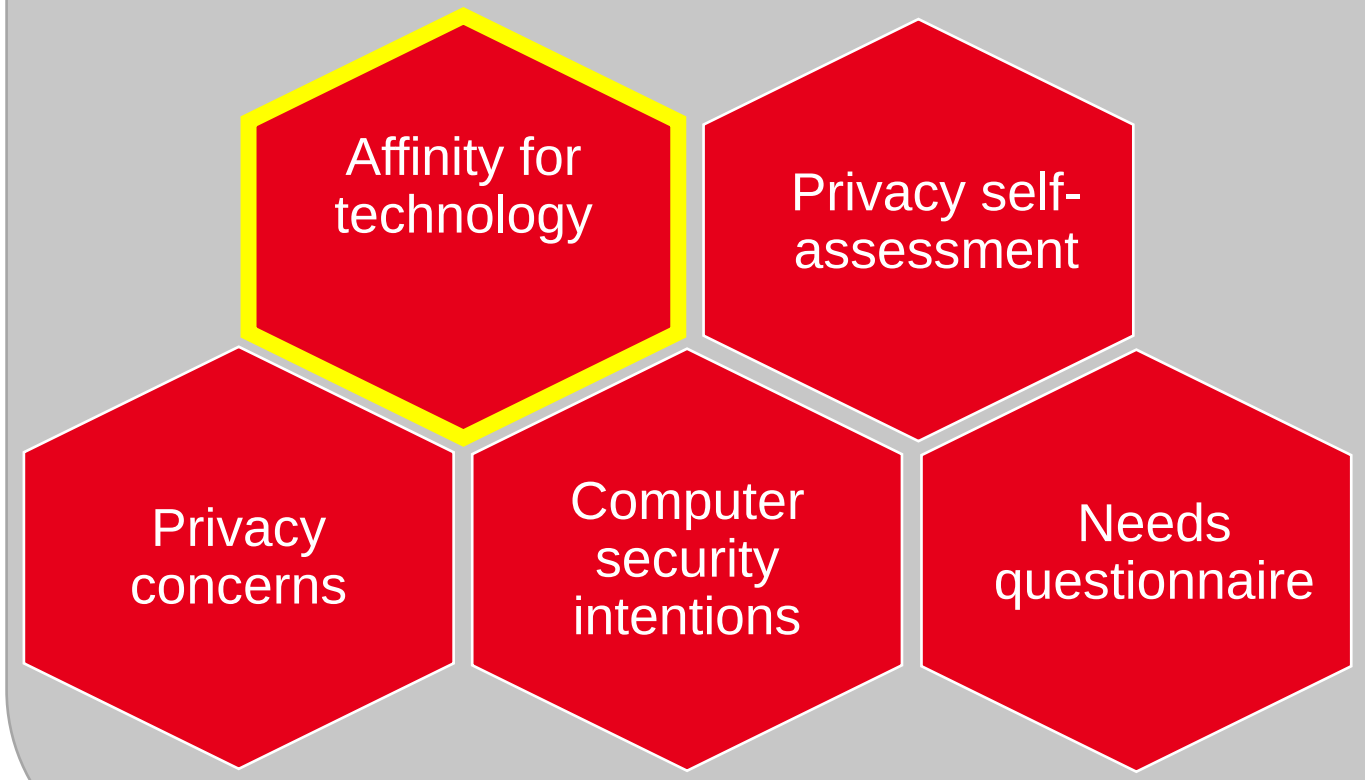
1 of 8 items

DEVELOPMENT OF THE QUESTIONNAIRE

TECHNISCHE UNIVERSITÄT DARMSTADT

Privacy and Trust for Mobile Users

Scientific questionaires (validity tested)

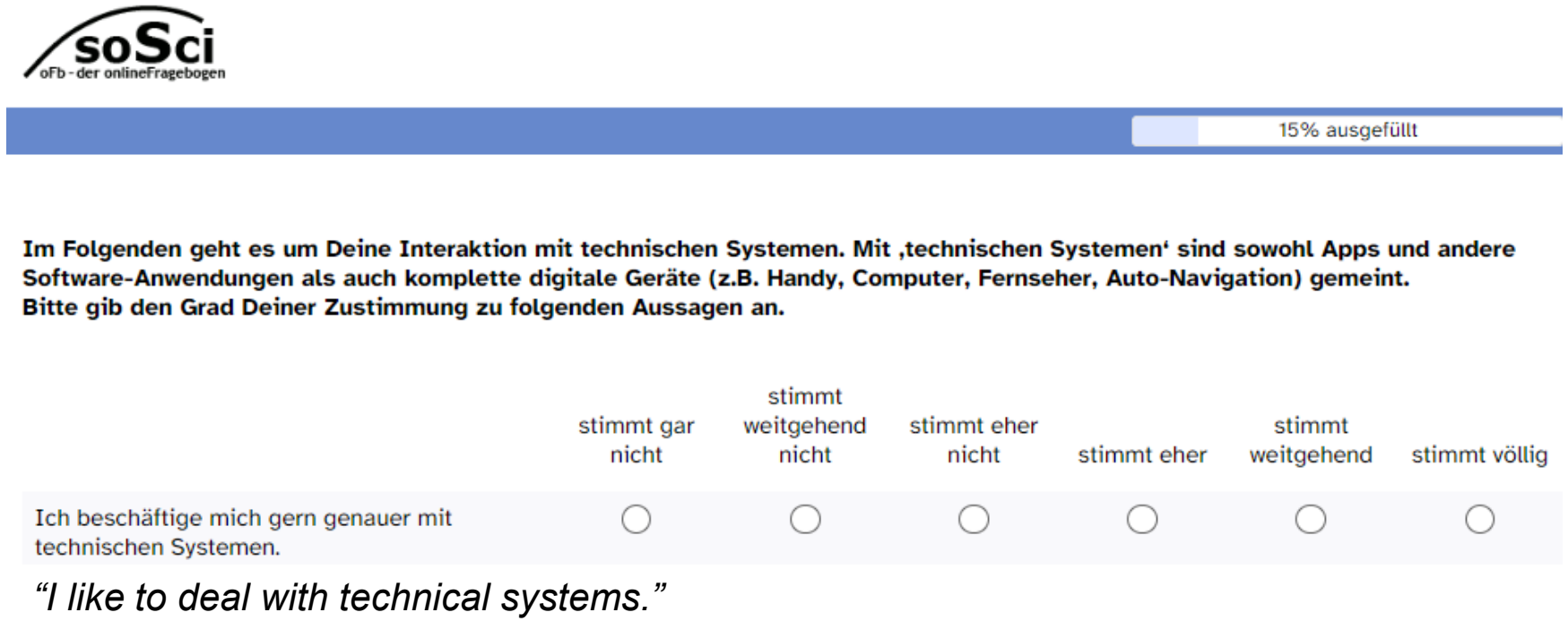


Newly developed questionaire

Specific questions

(learning content, user interface, leaderboard, data protection notifications and recommendations from contacts)

AFFINITY FOR TECHNOLOGY



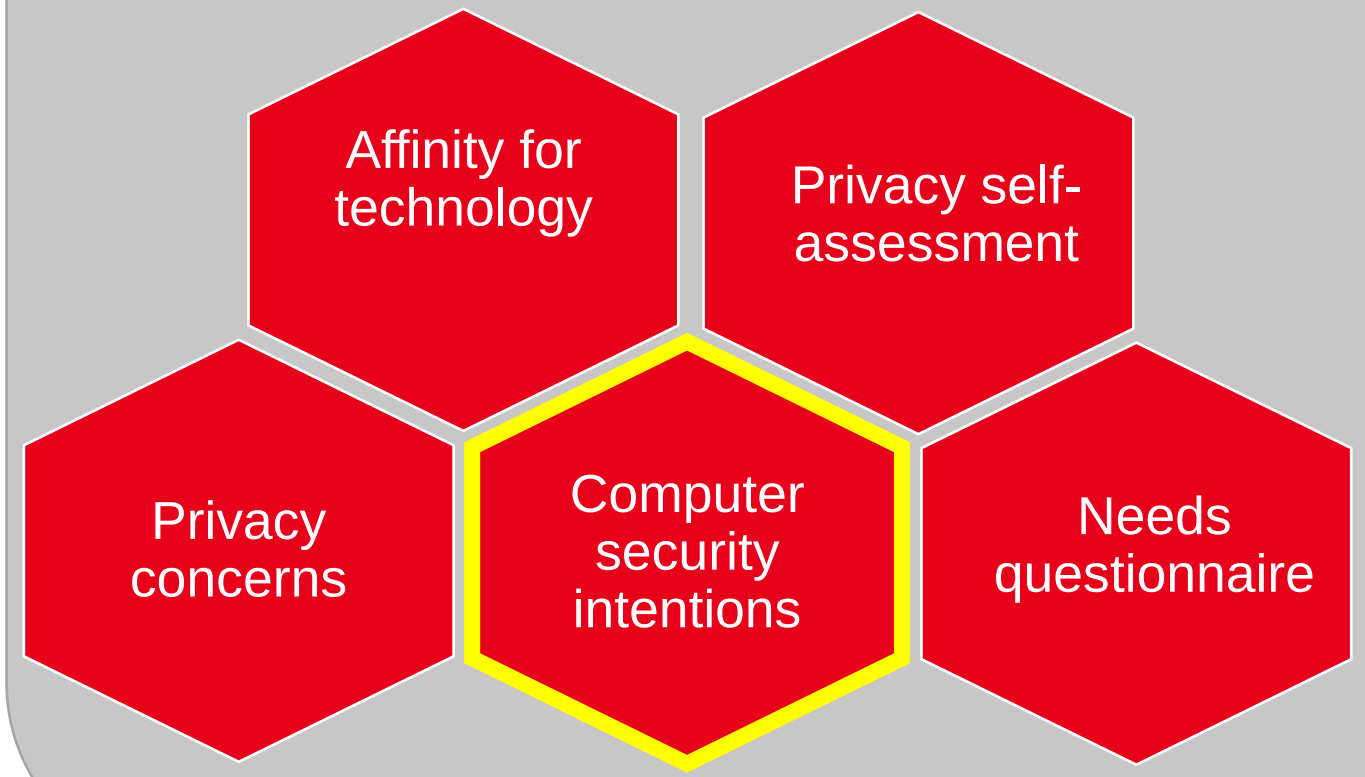
"I like to deal with technical systems."

DEVELOPMENT OF THE QUESTIONNAIRE

TECHNISCHE UNIVERSITÄT DARMSTADT

Privacy and Trust for Mobile Users

Scientific questionaires (validity tested)



Newly developed questionaire

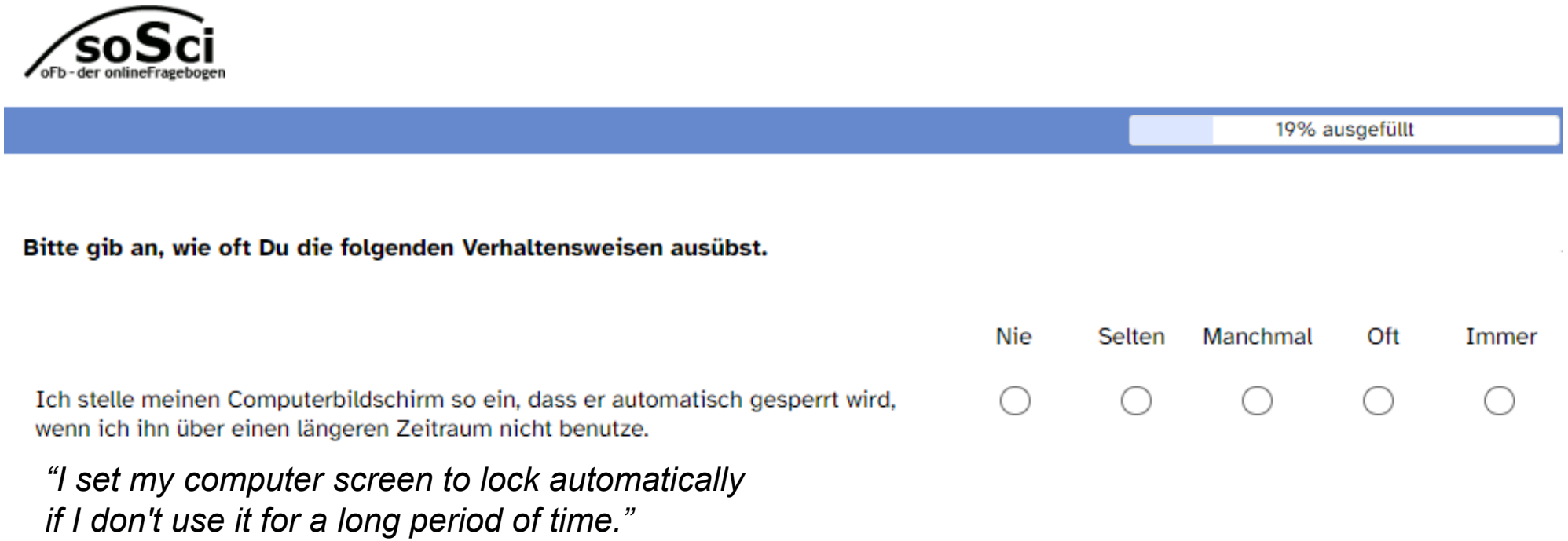
Specific questions

(learning content, user interface, leaderboard, data protection notifications and recommendations from contacts)

COMPUTER SECURITY INTENTIONS

TECHNISCHE UNIVERSITÄT DARMSTADT

Privacy and Trust for Mobile Users



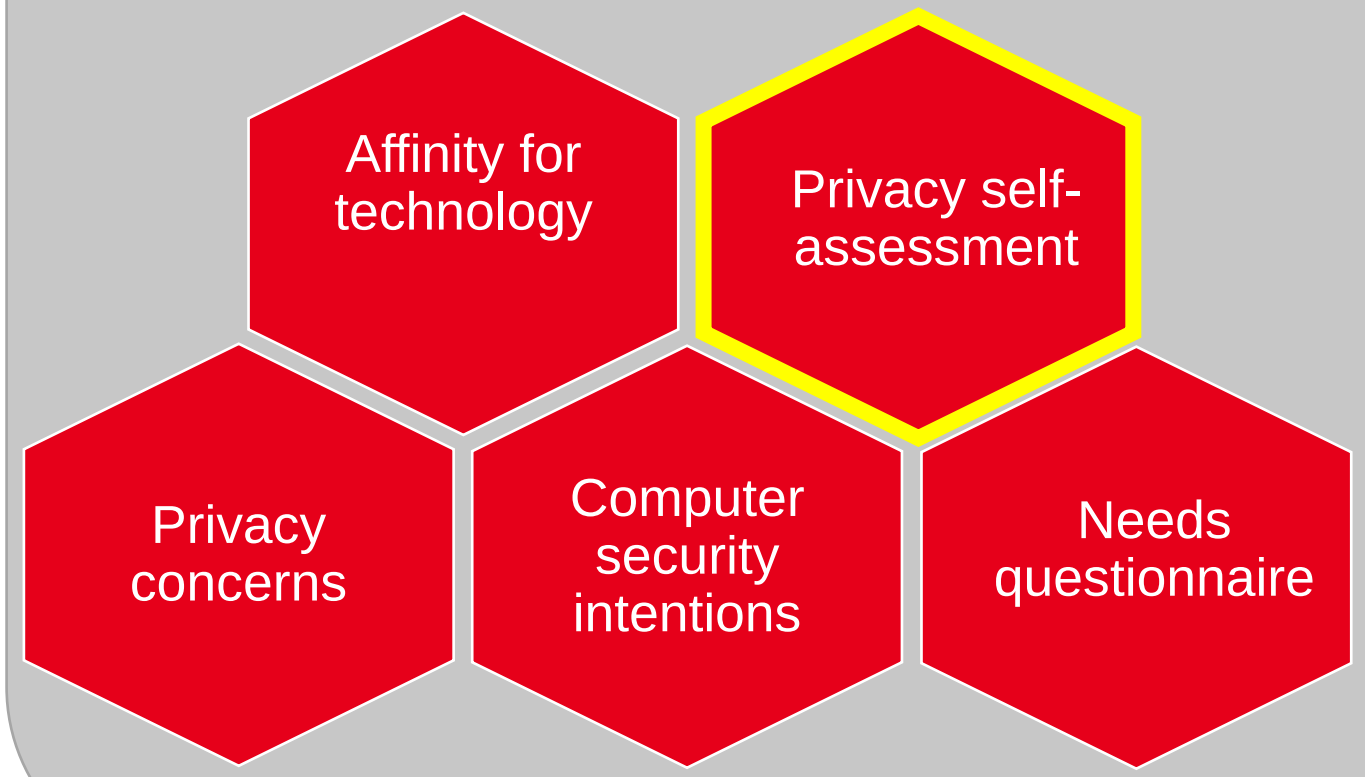
"I set my computer screen to lock automatically if I don't use it for a long period of time."

DEVELOPMENT OF THE QUESTIONNAIRE

TECHNISCHE UNIVERSITÄT DARMSTADT

Privacy and Trust for Mobile Users

Scientific questionaires (validity tested)



Newly developed questionaire

Specific questions

(learning content, user interface, leaderboard, data protection notifications and recommendations from contacts)

TECHNISCHE UNIVERSITÄT DARMSTADT

PRIVACY SELF-ASSESSMENT

Privacy and Trust for Mobile Users

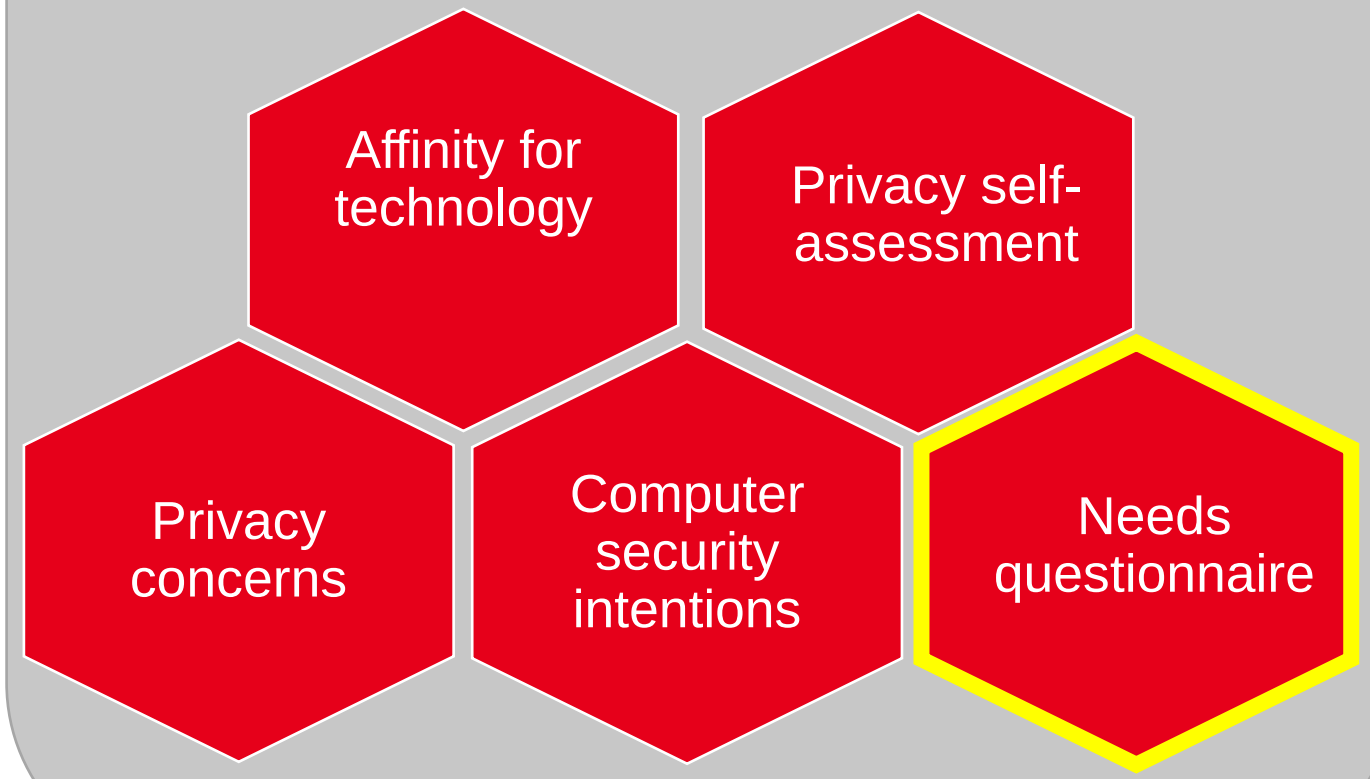
“How important do you consider your own digital privacy?

DEVELOPMENT OF THE QUESTIONNAIRE

TECHNISCHE UNIVERSITÄT DARMSTADT

Privacy and Trust for Mobile Users

Scientific questionaires (validity tested)

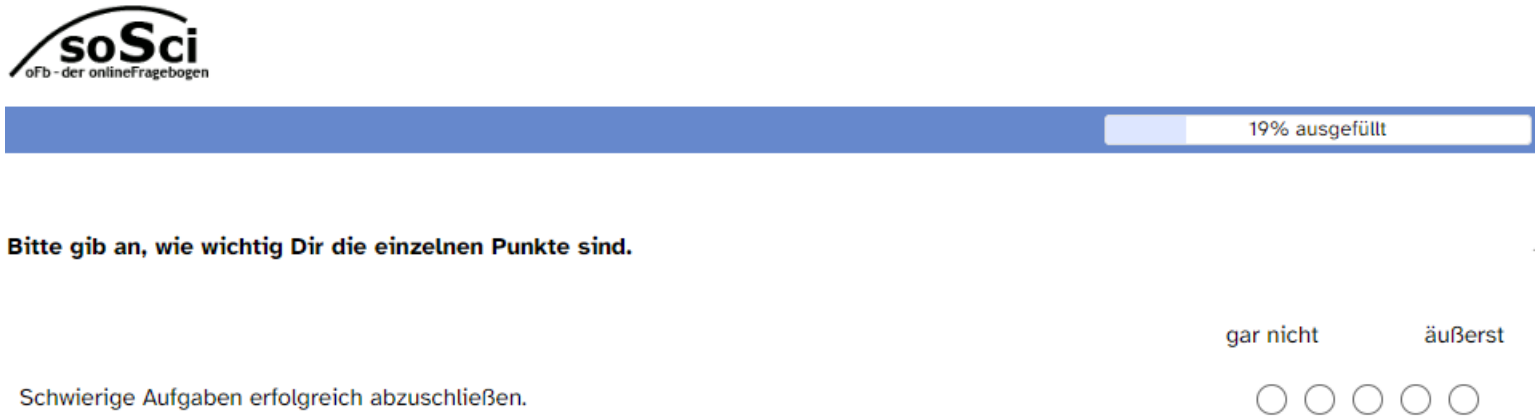


Newly developed questionaire

Specific questions

(learning content, user interface, leaderboard, data protection notifications and recommendations from contacts)

NEEDS QUESTIONAIRE



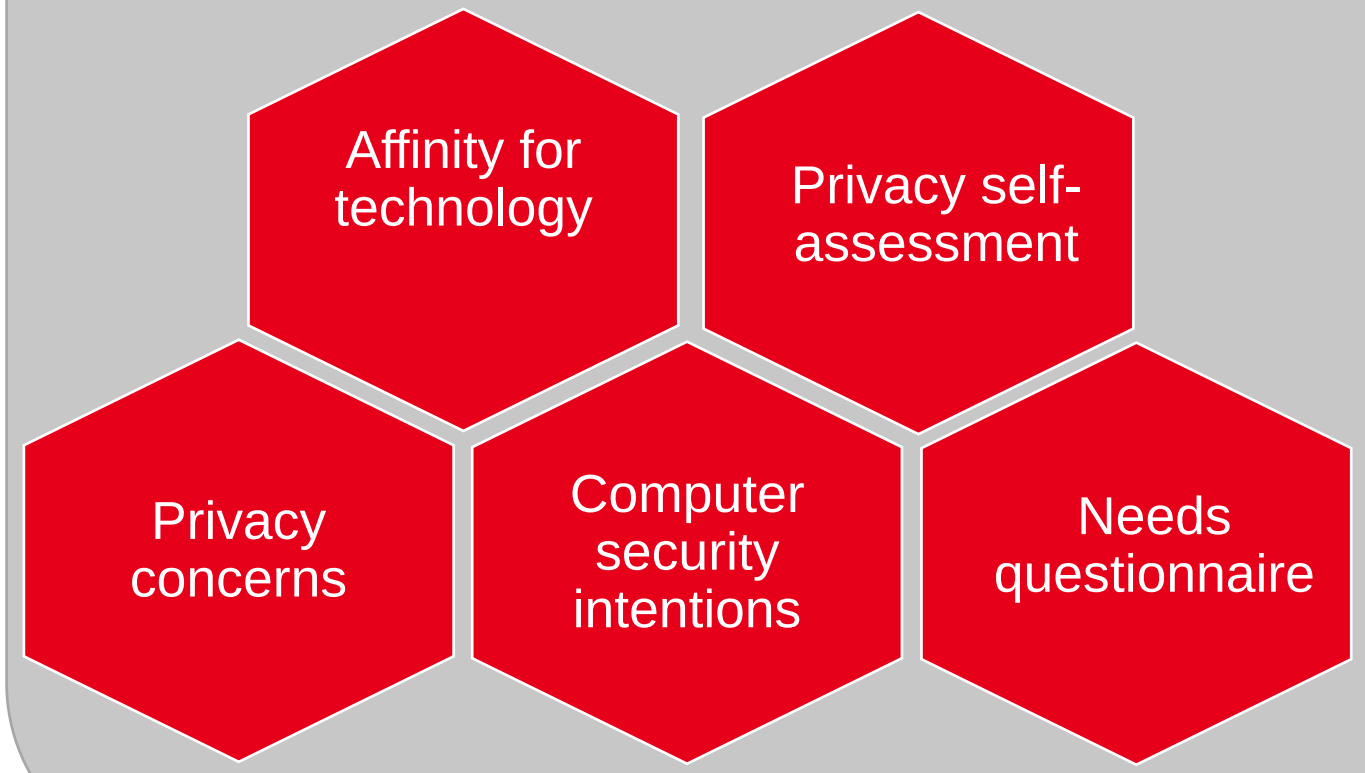
“Successfully complete difficult tasks.”

DEVELOPMENT OF THE QUESTIONNAIRE

TECHNISCHE UNIVERSITÄT DARMSTADT

Privacy and Trust for Mobile Users

Scientific questionaires (validity tested)



Newly developed questionaire

Specific questions

(learning content, user interface, leaderboard, data protection notifications and recommendations from contacts)

TECHNISCHE UNIVERSITÄT DARMSTADT

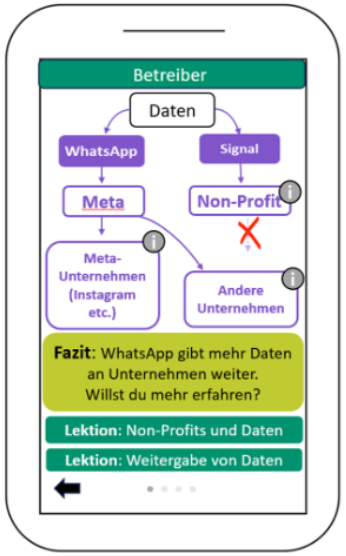
Privacy and Trust for Mobile Users

SHORT INTRODUCTION

1. Der Privacy Buddy führt Dich in einem Tutorial durch alle Funktionen:

Weiter

4. Du kannst ausgewählte Apps über Datenfluss Diagramme und Tabellen vergleichen:



Weiter

TECHNISCHE UNIVERSITÄT DARMSTADT

Specific questions

Likert-Scale from 1 "I do not agree at all" - 5 "I entirely agree"

Learning Content:

"I would like to be able to choose the topics of the learning content in the Privacy Buddy myself."

Recommendations:

"I would like to receive general recommendations from experts regarding privacy settings from the Privacy Buddy."

User Interface:

"I would like to be able to create my own avatar in the Privacy Buddy, which represents the Privacy Buddy and interacts with me."

Data protection notifications:

"I would like to be notified by the Privacy Buddy when an app accesses my location."

Leaderboard:

"I find it useful to rate my general progress in the Privacy Buddy."

FIRST RESULTS

SAMPLE

Sample:

- Samplesize: *N* = 71
- Age
  - *mean* = 23.13
  - *SD* = 5.14
- Gender
  - *N(Female)* = 46
  - *N(Male)* = 24
  - *N(Non-binary)* = 1

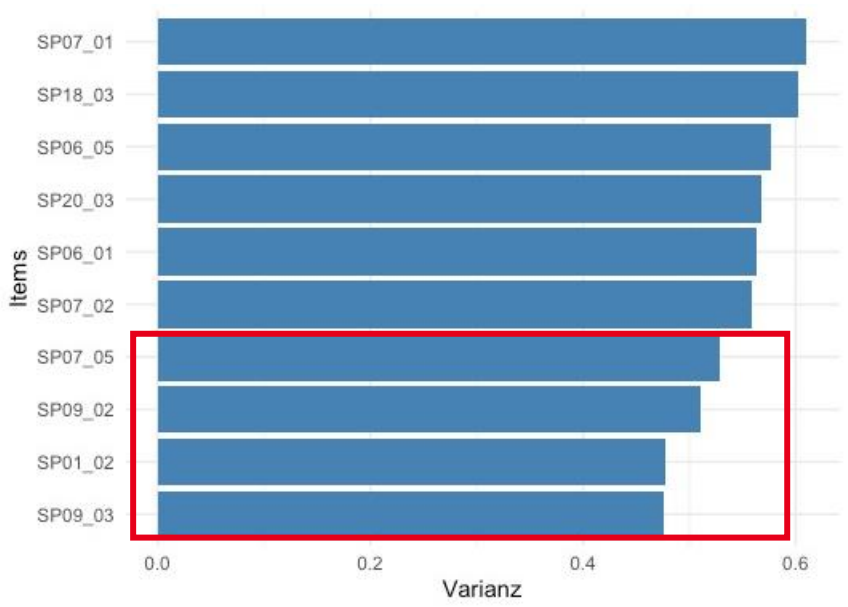
FIRST RESULTS

SPECIFIC QUESTIONS

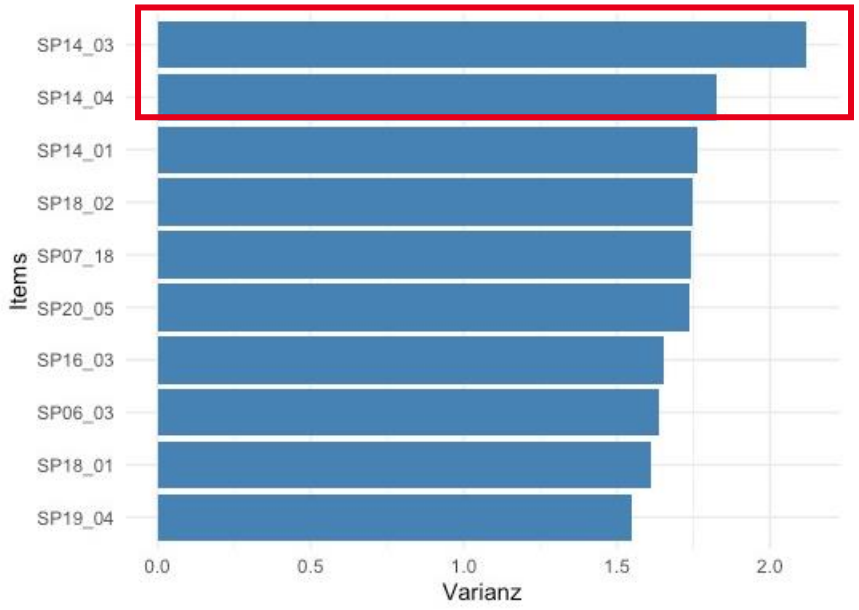
Inspection of variance:

- Where did the test participants agree?
- Where were there major differences in response behavior?

Items with the **lowest** variance:



Items with the **highest** variance:



More information on the next slides

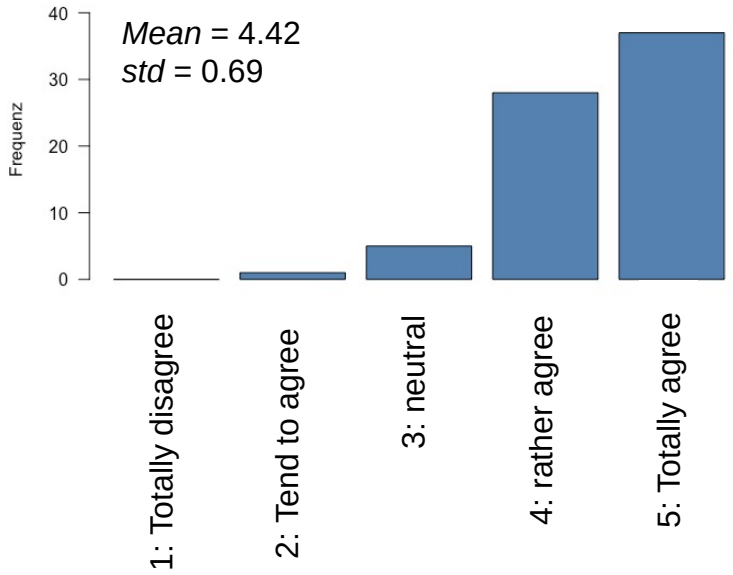
FIRST RESULTS

SPECIFIC QUESTIONS

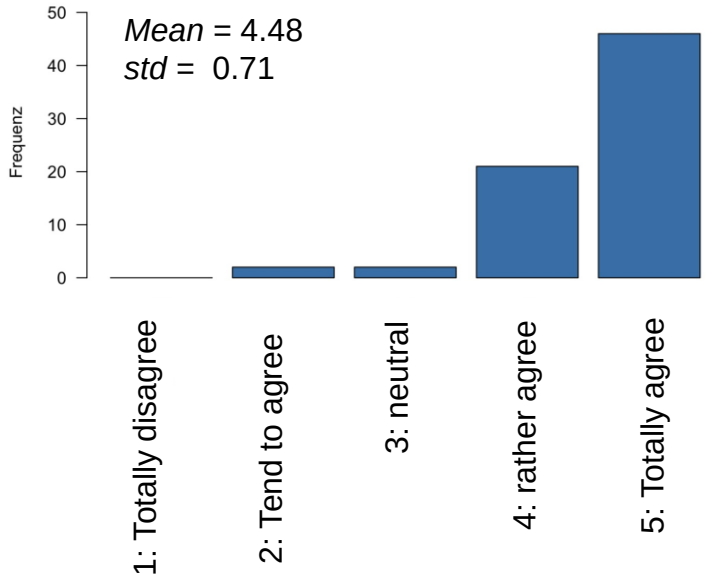
Items with the lowest variance: (original questions and answer scales were german)

Feature: **Quiz**

I think **assignment tasks** are a good way to test yourself.



I think **multiple-choice questions** are a good way to test yourself.



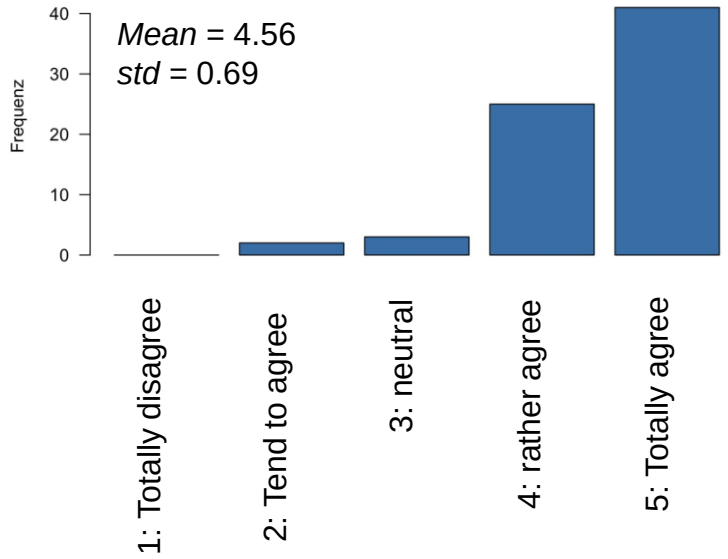
FIRST RESULTS

SPECIFIC QUESTIONS

Items with the lowest variance: (original questions and answer scales were german)

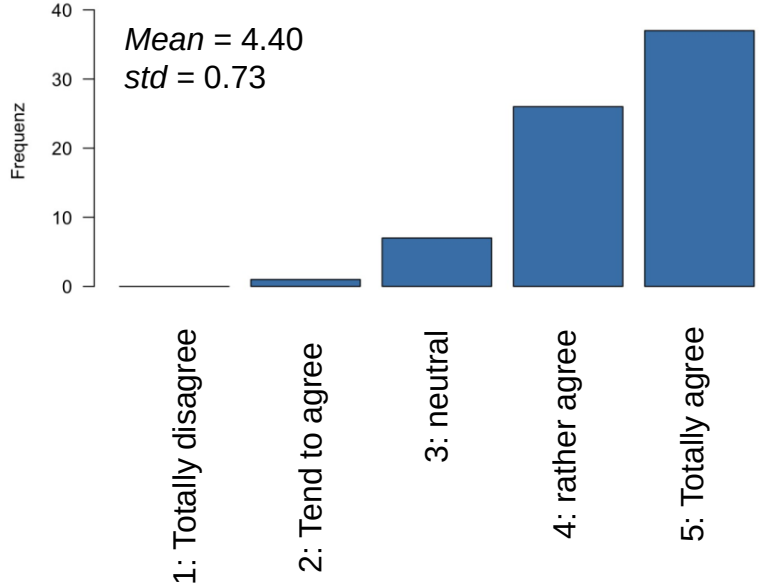
Feature: **Lections**

Learning content should be **supported by images.**



Feature: **Learning content**

I want to learn more about **malicious browser extensions.**



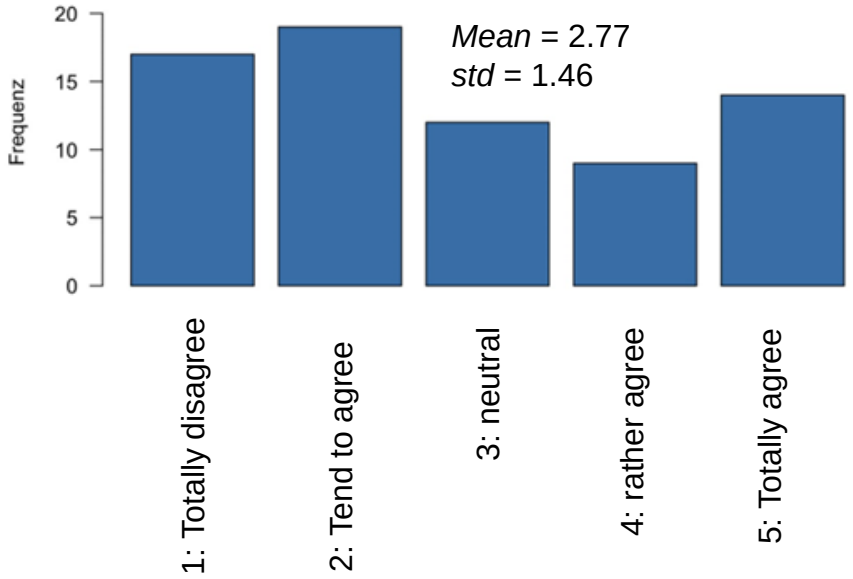
FIRST RESULTS

SPECIFIC QUESTIONS

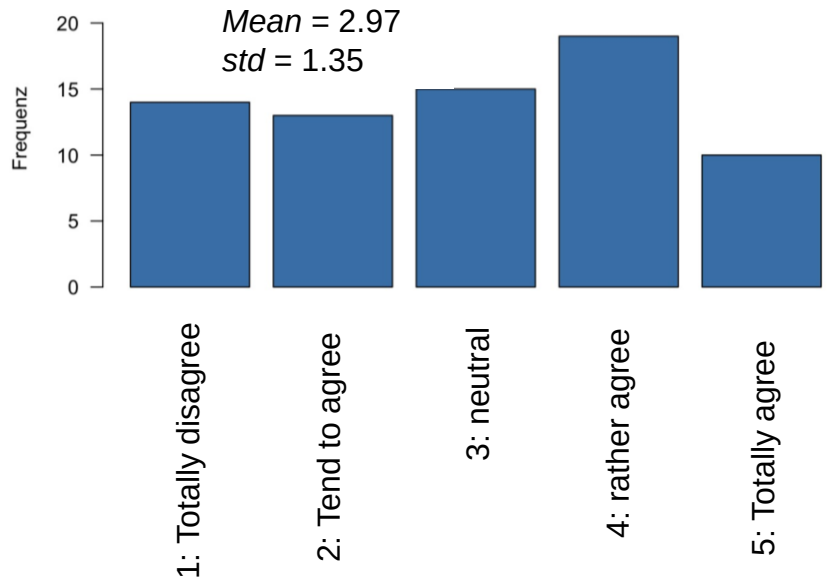
Items with the highest variance: (original questions and answer scales were german)

Feature: **UI**

I would like to be able to create **my own avatar** that represents the Privacy Buddy.



I would like to have an **individually chosen username**.



FIRST RESULTS

SCIENTIFIC QUESTIONNAIRES

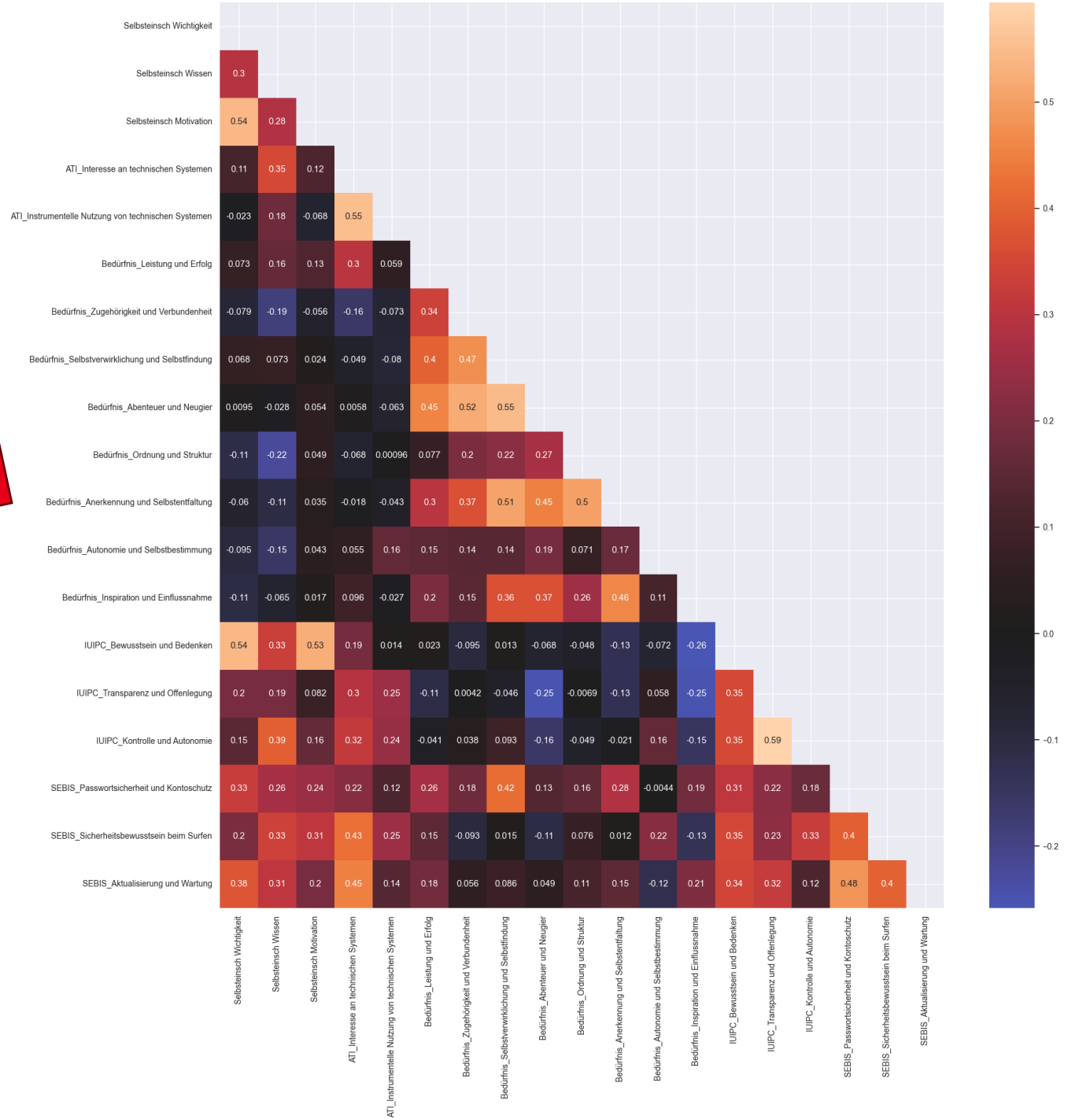
Analysis:

- **Reliability** of scales and **correlations** between scales

  →compare to literature

Current state

- Custeranalysis:
  - Can user groups be identified?
  - How can these be characterized?
  - How do these compare to the literature?



FURTHER ANALYSIS

- **Specific questions**
  - More analysis about **generally supported** and **generally not supported features**
  - Can items be combined? → **Factor analysis**
  - Can groups with similar response behavior be identified? → **Clusteranalysis**
- **Scientific questionnaires**
  - **Clusteranalysis**
  - **Comparison** of the results to the **literature**
- **Combining the questionnaires**
  - **Correlations** between specific items and scales from the existing questionnaires
  - Are **comparable clusters** found in both data sets?

TECHNISCHE UNIVERSITÄT DARMSTADT

Privacy and Trust for Mobile Users

LITERATURE

[1] Author(s), A. Persuasive Privacy Assistant: Need-Sensitive Design of Privacy Support Tools Through Persuasive System Principles From a Users' and Experts' Perspective. In: *ACM Conference on Human Factors in Computing Systems*, May 11–16, 2024, Honolulu, Hawai'i. ACM, New York, 2024.

[2] Stöver, A., Hahn, S. M., Kretschmer, F., & Gerber, N. (2023). Investigating how users imagine their personal privacy assistant. *Proceedings on Privacy Enhancing Technologies*, 2023(2), 384–402. https://doi.org/10.56553/popets-2023-0059

[3] Schmidt, J. M. (2020). *"Privatsphären Paradoxon": Eine Analyse unterschiedlicher Faktoren zur Kategorisierung von Internetnutzern* [unpublished thesis].

TECHNISCHE UNIVERSITÄT DARMSTADT

Privacy and Trust for Mobile Users

GEFAHREN UND RISIKEN VON ALGORITHMEN & SOCIAL MEDIA

Von Katharina Worster

Fachbereich Soziologie

TECHNISCHE UNIVERSITÄT DARMSTADT

Privacy and Trust for Mobile Users

Global NEWS

Watch World Canada Local Politics Money Health Entertainment

TECH

Family sues Meta, blames Instagram for daughter's eating disorder, self-harm

By Michelle Butterfield · Global News
Posted June 8, 2022 3:01 pm · 4 min read

Global NEWS

Watch World Canada Local Politics Money Health

LIFESTYLE

Snapchat filters may seem harmless, but they're creating a new form of body dysmorphia

By marilisaraccoglobal · Global News
Posted August 10, 2018 3:29 pm · 3 min read

Support the Guardian
Fund independent journalism with €5 per month
Support us

The Guardian

News Opinion Sport Culture Lifestyle More

Social media

This article is more than 8 months old

US surgeon general issues advisory on 'profound' risks of child social media use

Dr Vivek Murthy calls on tech companies and policymakers to take 'immediate action' to protect children's mental health

Most viewed

Russia puts Estonian prime minister Kaja Kallas on wanted list

Russia-Ukraine war live: Zelenskiy hails US Senate

Judge rules fentanyl overdoses lawsuit against Snapchat can move forward

Is social media harming kids? New study offers guidance to parents

YouTuber Terrell Grice on how the stars aligned for his success

Whistleblower warns about risks teens face on social media

Tik' Lad

TECHNISCHE UNIVERSITÄT DARMSTADT

FORSCHUNGSINTERESSE

Privacy and Trust for Mobile Users

- Forschungsleitende Frage => Welche Gefahren und Risiken bergen Social Media Plattformen für Gesellschaft und Individuen, die möglicherweise nicht direkt als solche erkannt werden?

Erkenntnismotivation:

- Zunehmende Beliebtheit und Alltäglichkeit von Social Media
- Neben der Nützlichkeit gibt es offensichtliche, aber auch versteckte Gefahren und Risiken
- Geraten immer mehr in den Fokus und in öffentliche Debatten

TECHNISCHE UNIVERSITÄT DARMSTADT

Privacy and Trust for Mobile Users

VORGEHEN

- Literaturrecherche: Wissenschaftliche Artikel, Forschungsarbeiten
- Analyse, Vergleich und Zusammenfassung der Ergebnisse
- Verschiedene Schwerpunkte in der Literatur

TECHNISCHE UNIVERSITÄT DARMSTADT

ERGEBNISSE

Privacy and Trust for Mobile Users

- Algorithmen können Interessen, Präferenzen und vergangenes wie auch zukünftiges Verhalten berücksichtigen und vorhersagen
- Aber: Gefahren & verursachter Schaden durch Algorithmen bzw. zentrale Regulierungsmechanismen von Plattformen
- Verschiedene Arten von Schäden:
  - Fehler/Errors
  - Manipulation
  - Verstärkungseffekte
  - Ermöglichung von schädigenden Verhaltensweisen
  - Macht von Plattformen

TECHNISCHE UNIVERSITÄT DARMSTADT

Privacy and Trust for Mobile Users

ERGEBNISSE

- Verbreitung von Hassreden online als eine negative Folge von Social Media
- Verschiedene Arten von Hassreden im Internet sind z.B.:
  - religiöse Hassreden
  - Online Rassismus
  - Politischer Online-Hass
  - Geschlechtsspezifischer Online-Hass
  - Terrorismus als Auslöser für Hass im Internet
- Kann in Hassverbrechen im realen Leben münden

TECHNISCHE UNIVERSITÄT DARMSTADT

ERGEBNISSE

Privacy and Trust for Mobile Users

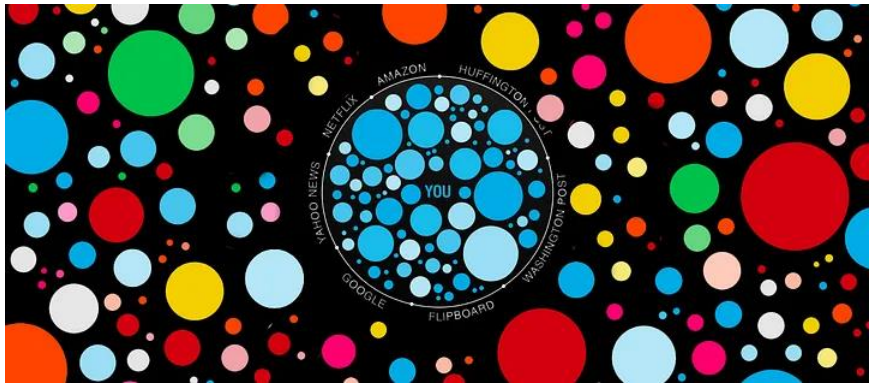
- Studie zu Auswirkungen von Social Media auf die mentale Gesundheit von Kindern und Jugendlichen
- Teilnehmende erkannten negative Effekte auf die mentale Gesundheit und das Wohlergehen durch die Internetnutzung:
  - Geringes Selbstwertgefühl und suizidale Gedanken
  - Cybermobbing
  - Trolling
  - Suchtpotential & daraus resultierender Schlafmangel

TECHNISCHE UNIVERSITÄT DARMSTADT

Privacy and Trust for Mobile Users

ERGEBNISSE

- Ideologische Polarisierung => politisch extremere Positionen
- Unterschiedliche Umweltwahrnehmungen durch Konsum unterschiedlicher Nachrichten/Medien
- Algorithmen als Quelle des Problems
  - Personalisierte Plattformnutzung
  - Daraus resultieren Filterblasen und Echokammern
  - Selektive Auseinandersetzung mit Themen
  - Verfügbarkeitsverzerrung
  - „Nachrichten-finden-mich“-Wahrnehmung



- Beispiele sind die US-Präsidentschaftswahl 2016 und die Brexit-Debatte 2016

TECHNISCHE UNIVERSITÄT DARMSTADT

WEITERES VORHABEN

Privacy and Trust for Mobile Users

- Weiterführende Auseinandersetzung mit Folgen für mentale Gesundheit (insbesondere bei Kindern und Jugendlichen)
- Mehr Literatur zu Fehlinformationen, Fake News und daraus resultierenden politischen und gesellschaftlichen Folgen
- Mehr Literatur zu Filterblasen, Echokammern und deren gesellschaftlichen Folgen
- Evtl. Auseinandersetzung mit Datensammlung und Stalking

TECHNISCHE UNIVERSITÄT DARMSTADT

DISKUSSION

Privacy and Trust for Mobile Users

- => Besteht ein Zusammenhang zwischen den verschiedenen vorgestellten Kategorien?
- => Inwiefern lassen sich die verschiedenen Folgen miteinander verknüpfen?

- Gibt es Anregungen und Vorschläge zu weiteren Gefahren und Risiken bzw. negativen Folgen von Social Media?

TECHNISCHE UNIVERSITÄT DARMSTADT

SCHEDULE

Privacy and Trust for Mobile Users

iPAT Seminar WiSe23/24 – Final Presentation – Talks Schedule
When: Friday 16.02.2024 @10:00 – 12:30
Where: S202/C110

Start	End	1st Session	Discipline	Topic	Presenter(s)	Adivsor(s)
10:00	10:05			Greetings and Starting Note		(Simon Althaus, Ephraim Zimmer)
10:05	10:30		Psychology	Personalization of Privacy Assistants	Sebastian Gandenberger, Vahan Demirci, Bedirhan Sahin, Till Feldner	Simon Althaus, Sara Hahn, Fransisca Hapsari
10:30	10:50		Sociology	Kritik an Social Media und der Macht von Onlineplattformen	Katharina Worster	Florian Müller, Rebecca Heigl
10:50	11:10			Algorithmic Governance & Nudging	Marvin Fink	Florian Müller, Enno Steinbrink
11:10	11:20			BREAK (Tentative/Optional)		
		2nd Session	**Discipline**	**Topic**	**Presenter(s)**	**Adivsor(s)**
11:20	11:40		Computer Science	Privacy and Utility Perception Compared to Sensor Awareness and Their Actual Privacy Implications	Beliz Balim	Matthias Gazzari, Fransisca Hapsari
11:40	12:00			Attacking Privacy in Electric Vehicle Charging Stations	Joshua Moell	Carsten Schmidt, Sara Hahn
12:00	12:20			Civil Sensor Data During War Time And In Crises	Johanna Jarsch	Enno Steinbrink, Matthias Gazzari
12:20	12:30			Closing Remarks		(Simon Althaus, Ephraim Zimmer)

TECHNISCHE UNIVERSITÄT DARMSTADT

Privacy and Trust for Mobile Users

ALGORITHMIC GOVERNANCE & NUDGING

Marvin Fink

TECHNISCHE UNIVERSITÄT DARMSTADT

SCHEDULE

Privacy and Trust for Mobile Users

iPAT Seminar WiSe23/24 – Final Presentation – Talks Schedule
When: Friday 16.02.2024 @10:00 – 12:30
Where: S202/C110

Start	End	1st Session	Discipline	Topic	Presenter(s)	Adivsor(s)
10:00	10:05			Greetings and Starting Note		(Simon Althaus, Ephraim Zimmer)
10:05	10:30		Psychology	Personalization of Privacy Assistants	Sebastian Gandenberger, Vahan Demirci, Bedirhan Sahin, Till Feldner	Simon Althaus, Sara Hahn, Fransisca Hapsari
10:30	10:50		Sociology	Kritik an Social Media und der Macht von Onlineplattformen	Katharina Worster	Florian Müller, Rebecca Heigl
10:50	11:10			Algorithmic Governance & Nudging	Marvin Fink	Florian Müller, Enno Steinbrink
11:10	11:20			BREAK (Tentative/Optional)		
		2nd Session	**Discipline**	**Topic**	**Presenter(s)**	**Adivsor(s)**
11:20	11:40		Computer Science	Privacy and Utility Perception Compared to Sensor Awareness and Their Actual Privacy Implications	Beliz Balim	Matthias Gazzari, Fransisca Hapsari
11:40	12:00			Attacking Privacy in Electric Vehicle Charging Stations	Joshua Moell	Carsten Schmidt, Sara Hahn
12:00	12:20			Civil Sensor Data During War Time And In Crises	Johanna Jarsch	Enno Steinbrink, Matthias Gazzari
12:20	12:30			Closing Remarks		(Simon Althaus, Ephraim Zimmer)

TECHNISCHE UNIVERSITÄT DARMSTADT

Privacy and Trust for Mobile Users

PRIVACY AND UTILITY PERCEPTIONS ABOUT SENSORS COMPARED TO SENSOR AWARENESS AND ACTUAL PRIVACY IMPLICATIONS

IPAT-Seminar

Beliz Balim

AGENDA

1 Introduction

2 Research Questions and Research Approach

3 R1: Comparison of Utility and Privacy Perceptions with Actual Privacy Risks and Utility

4 R2: Sensor Awareness, Awareness Measures and Coping Mechanisms

5 Conclusion

TECHNISCHE UNIVERSITÄT DARMSTADT

Privacy and Trust for Mobile Users

MOTIVATION

Widespread presense of sensors in our lives
e.g. smart homes, fitness trackers

Benefits
such as increasing convenience in daily tasks, monitoring health metrics

Potential violation of user and bystander privacy

Balance
between the benefits of sensor technologies and individual privacy

RESEARCH QUESTIONS

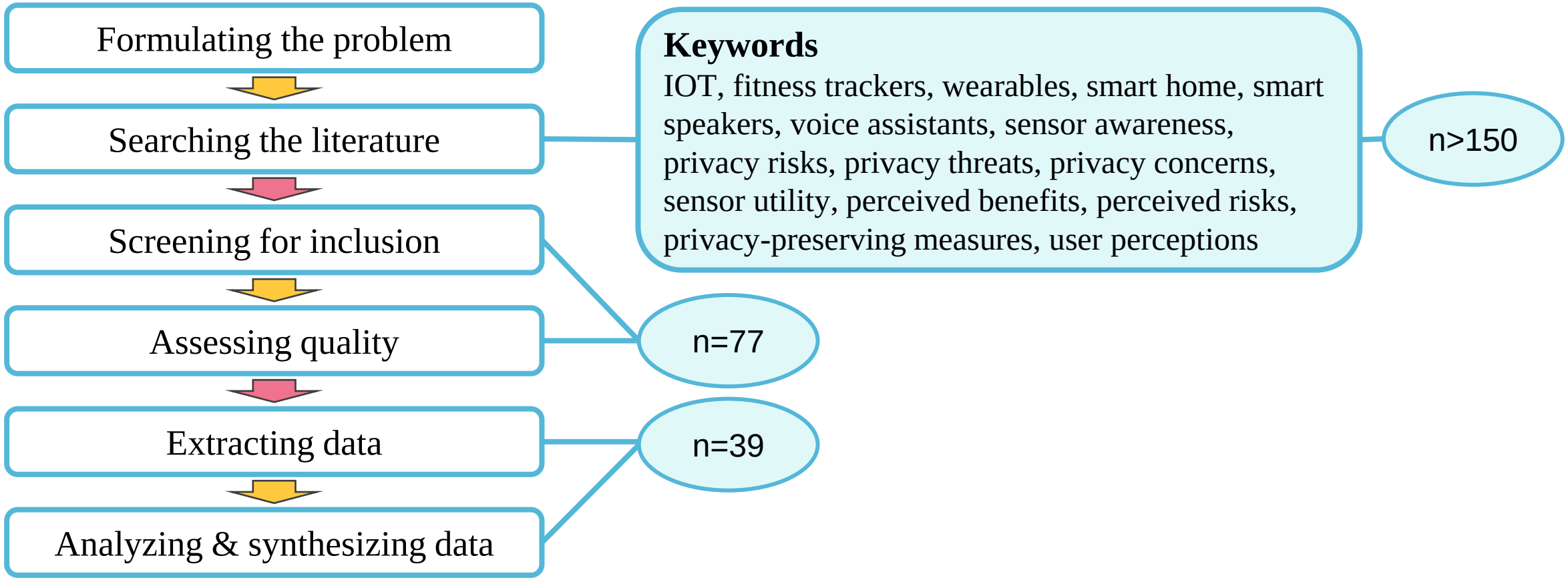
R1: Does the perceived privacy threat and expected utility match the actual risks and benefits of sensors?

R2: How much is the perception dependent on sensor awareness and how can we positively influence it?

TECHNISCHE UNIVERSITÄT DARMSTADT

Privacy and Trust for Mobile Users

RESEARCH APPROACH



Framework by Templier and Pare

2 Research Questions and Research Approach

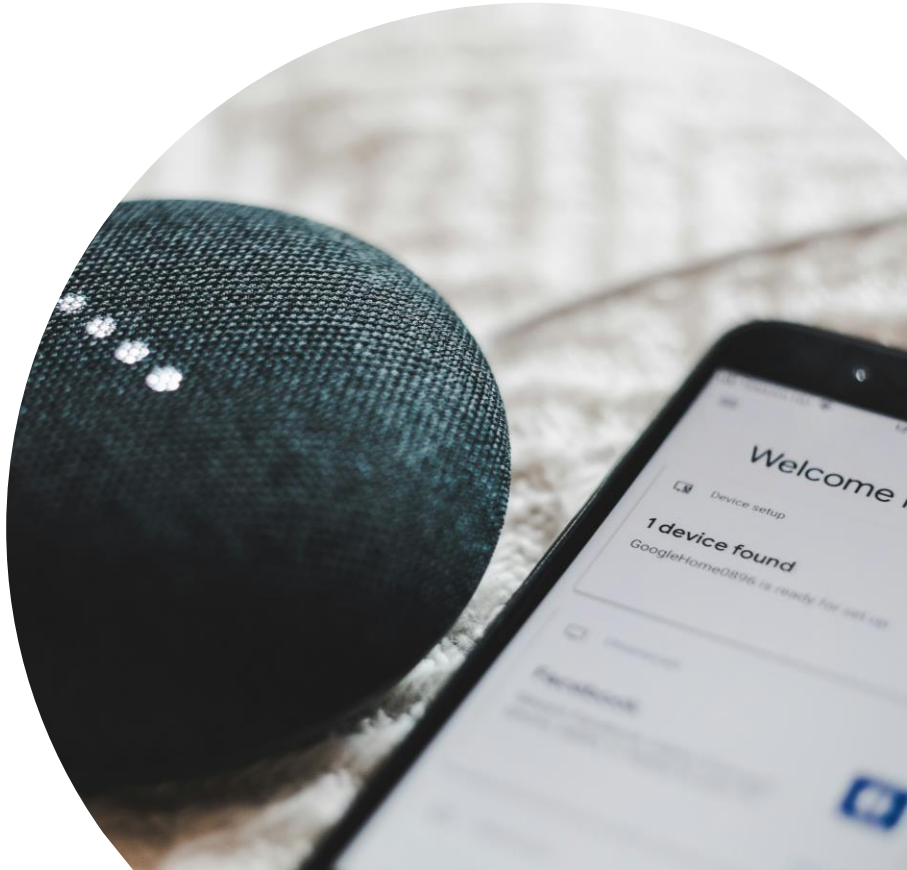
RESEARCH FOCUS

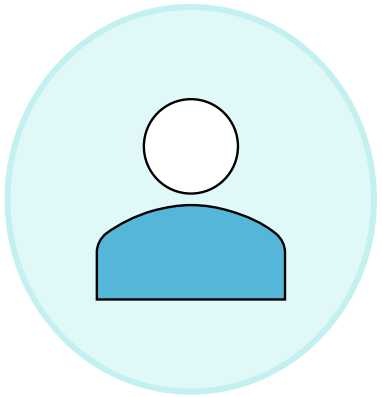
TECHNISCHE UNIVERSITÄT DARMSTADT

Privacy and Trust for Mobile Users

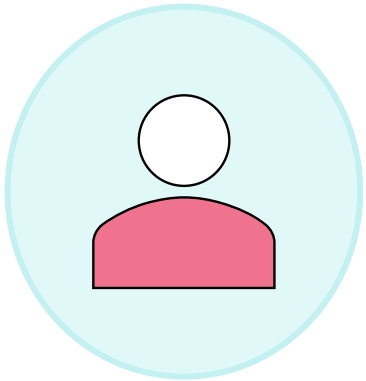
privacy perceptions depend on **sensor type & type of collected data**

Focus on fitness trackers & smart speakers
due to their raising popularity

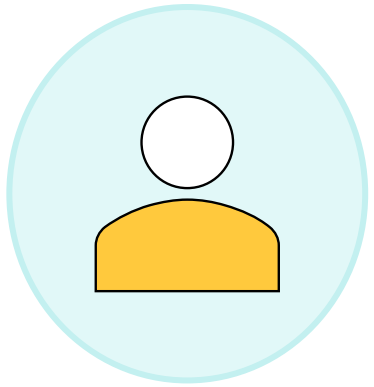




fitness trackers from users' perspective



smart speakers from users' perspective



Smart speakers from bystanders' perspective

R1: Comparison of Utility and Privacy Perceptions with Actual Privacy Risks and Utility

TECHNISCHE UNIVERSITÄT DARMSTADT

Privacy and Trust for Mobile Users

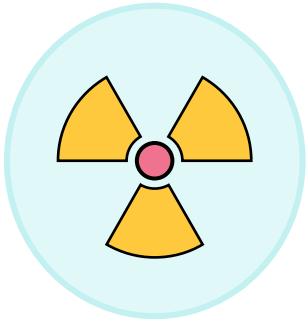
FITNESS TRACKERS FROM USERS´ PERSPECTIVE

Collected Data

physiological data such as hearth-rate and step-count

Perceived Utility

benefits to health through tracking physiological metrics and activities



Perceived Risks

users tend to underestimate the privacy risks

Users think that the expected benefits outweigh the risks

Mismatch between actual & perceived risks

due to

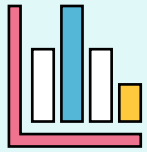
lack of knowledge regarding possible inference of further information

TECHNISCHE UNIVERSITÄT DARMSTADT

Privacy and Trust for Mobile Users

SMART SPEAKERS

From User Perspective



Collected Data
voice recordings, conversations

Perceived Utility
- convenience
- fulfill basic information needs
- manage schedule

Actual Risks

Mismatch between actual & perceived risks
- Low level of concern
- Unawareness about the real extent and criticality of the privacy threats

From Bystander Perspective

bystanders are **more concerned** with their privacy than owners
(contradictory stances in literature)

Bystanders perceive less **utility** than the owners

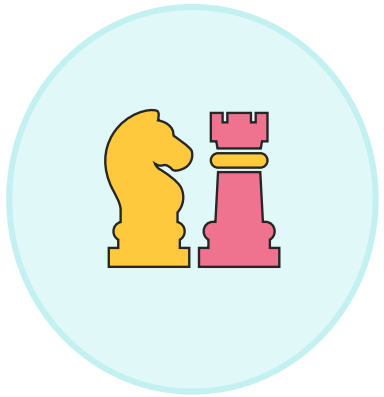
Imbalance between high concerns & low perceived utility

Role of trust

TECHNISCHE UNIVERSITÄT ADT

Definition of sensor awareness

Influence of Sensor Awareness on Privacy Perceptions



Awareness measures & Coping strategies

R2: How much is the perception dependent on sensor awareness and how can we positively influence it?

DEFINITION OF SENSOR AWARENESS

Sensor awareness includes individuals' knowledge about all factors related to the collection, processing and sharing of sensor data.

E.g. knowledge about …

- …the presence of sensors
- …collected data types
- …potential of information inference from collected data
- …possible privacy threats,
- … involved third parties,
- … data storage and sharing etc.

TECHNISCHE UNIVERSITÄT DARMSTADT

Privacy and Trust for Mobile Users

INFLUENCE OF SENSOR AWARENESS ON PRIVACY PERCEPTIONS

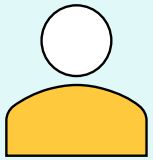
Fitness Trackers

Incomplete and partly inaccurate understanding of users about….

- collected data types
- possible ways of further information inference
- possible privacy threats

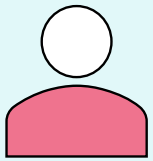
Incomplete sensor awareness leads to underestimation of privacy risks

Smart Speakers



User perspective

Results similar to fitness trackers
+ uncertainty, if the smart speakers are always listening and recording data
+ some users deliberately avoid thinking about their privacy



Bystander perspective

Majority of users also don't inform bystanders about the existence of smart home devices

Most of the bystanders do not expect the owners to inform them about the data practices

Contradiction: high privacy concerns but low information expectancy

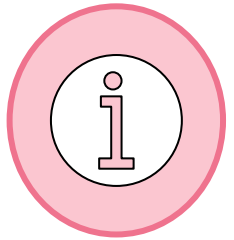
AWARENESS MEASURES AND COPING STRATEGIES

TECHNISCHE UNIVERSITÄT DARMSTADT

Privacy and Trust for Mobile Users

Awareness measures

increase users' and bystanders' sensor awareness

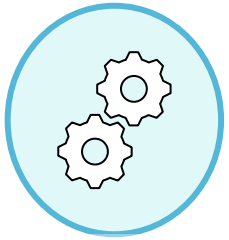


Provision information about data collection and possible risks

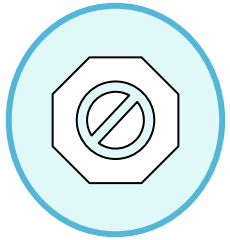
Manufacturers should inform users
Owners should inform bystanders

Coping strategies

reduce perceived and actual privacy threats

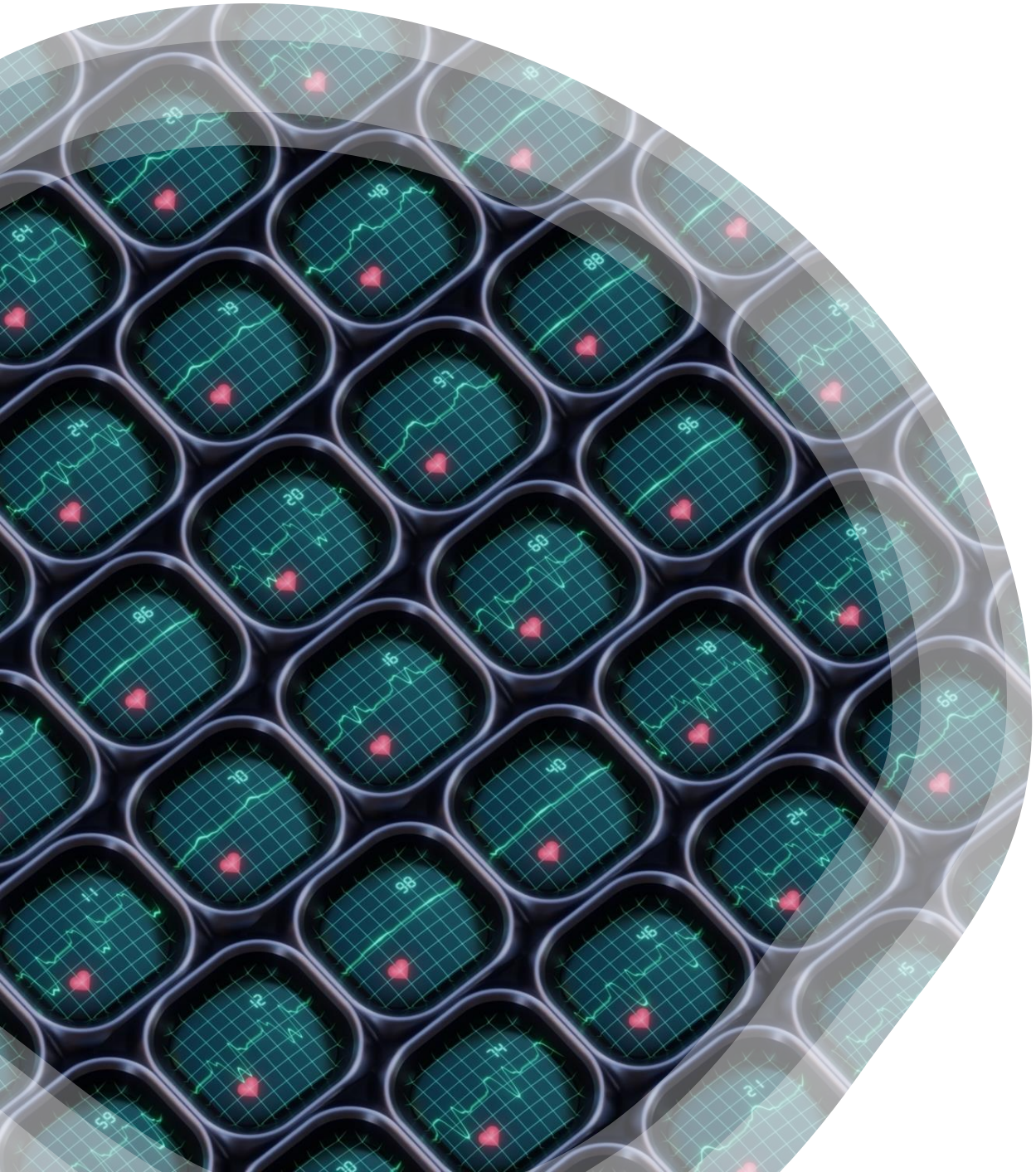


Control through **privacy settings**



Sharing no sensitive information

Unplugging smart speakers temporarily
Adjusting conversations around smart speakers



CONCLUSION

- Two different research questions are connected
  - R1: Privacy and utility perceptions do not match actual privacy implications due to lack of sensor awareness
  - R2: Lack of sensor awareness leads to an underestimation of privacy risks
- Practical Implication:
  high need for raising awareness about data practices

TECHNISCHE UNIVERSITÄT DARMSTADT

SCHEDULE

Privacy and Trust for Mobile Users

iPAT Seminar WiSe23/24 – Final Presentation – Talks Schedule
When: Friday 16.02.2024 @10:00 – 12:30
Where: S202/C110

Start	End	1st Session	Discipline	Topic	Presenter(s)	Adivsor(s)
10:00	10:05			Greetings and Starting Note		(Simon Althaus, Ephraim Zimmer)
10:05	10:30		Psychology	Personalization of Privacy Assistants	Sebastian Gandenberger, Vahan Demirci, Bedirhan Sahin, Till Feldner	Simon Althaus, Sara Hahn, Fransisca Hapsari
10:30	10:50		Sociology	Kritik an Social Media und der Macht von Onlineplattformen	Katharina Worster	Florian Müller, Rebecca Heigl
10:50	11:10			Algorithmic Governance & Nudging	Marvin Fink	Florian Müller, Enno Steinbrink
11:10	11:20			BREAK (Tentative/Optional)		
		2nd Session	**Discipline**	**Topic**	**Presenter(s)**	**Adivsor(s)**
11:20	11:40		Computer Science	Privacy and Utility Perception Compared to Sensor Awareness and Their Actual Privacy Implications	Beliz Balim	Matthias Gazzari, Fransisca Hapsari
11:40	12:00			Attacking Privacy in Electric Vehicle Charging Stations	Joshua Moell	Carsten Schmidt, Sara Hahn
12:00	12:20			Civil Sensor Data During War Time And In Crises	Johanna Jarsch	Enno Steinbrink, Matthias Gazzari
12:20	12:30			Closing Remarks		(Simon Althaus, Ephraim Zimmer)

TECHNISCHE UNIVERSITÄT DARMSTADT

Privacy and Trust for Mobile Users

ATTACKING YOUR PRIVACY IN ELECTRIC VEHICLE CHARGING STATIONS

Joshua Moell

Computer Science

TU Darmstadt

TECHNISCHE UNIVERSITÄT DARMSTADT

Privacy and Trust for Mobile Users

CHARGING PROCESS

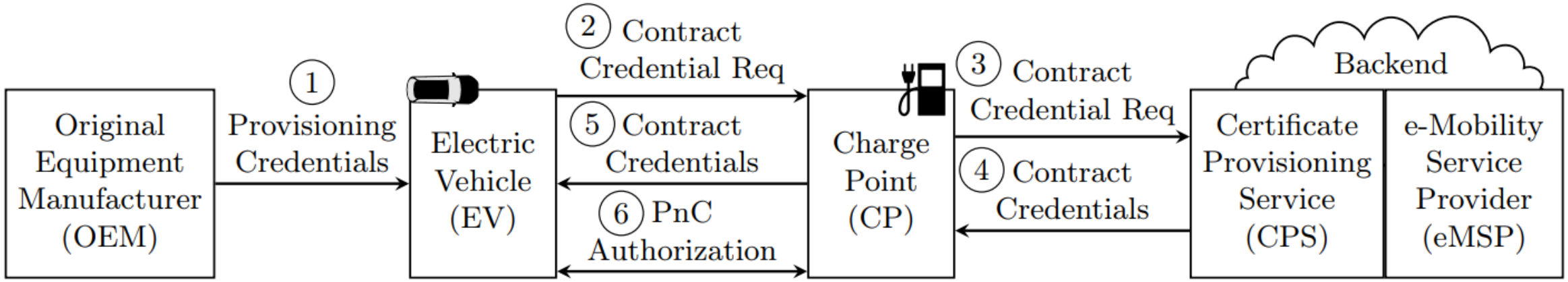


Fig. 1. E-mobility architecture.

Protect your Privacy at Charging Stations

Personal Data

Your Personal Data e.g. name, address and payment information could be stolen and shared with 3rd parties.

Location Tracking

If an attacker would get information about where you charge at which time your location could be tracked

Financial Damage

Your payment information could be used to cause severe financial Damage. Somebody could charge another Vehicle at your cost.

What you can do to protect your privacy

- Keeping **track** of **account activity** and reporting any suspicious activity.
- Only use **official apps** from reputable providers and keep them updated.
- Use **two-factor authentication** if possible and strong passwords for accounts used for your charging process.
- If you observe any **physical change** on your Charging station it could mean it is compromised.
- If you are using the RFID Scanner check that scanner for **manipulation** and don't use it

In general, do not use a suspicious Charging Station and inform the provider and the authorities.

Other threads

In addition to the privacy risks there are also other threads not related to privacy.

if an attacker could get full control of multiple charging stations the power grid could be compromised, or the charged car could be overcharged and damaged.

A successful Denial of Service Attack would prevent you from being able to charge your Vehicle.

More Information

TECHNISCHE UNIVERSITÄT DARMSTADT

Privacy and Trust for Mobile Users

What you can do to protect your privacy

- Keeping **track** of **account activity** and reporting any suspicious activity.
- Only use **official apps** from reputable providers and keep them updated.
- Use **two-factor authentication** if possible and strong passwords for accounts used for your charging process.
- If you observe any **physical change** on your Charging station it could mean it is compromised.
- If you are using the RFID Scanner check that scanner for **manipulation** and don't use it

In general, do not use a suspicious Charging Station and inform the provider and the authorities.

Other threads

In addition to the privacy risks there are also other threads not related to privacy.

if an attacker could get full control of multiple charging stations the power grid could be compromised, or the charged car could be overcharged and damaged.

A successful Denial of Service Attack would prevent you from being able to charge your Vehicle.

More Information

TECHNISCHE UNIVERSITÄT DARMSTADT

SCHEDULE

Privacy and Trust for Mobile Users

iPAT Seminar WiSe23/24 – Final Presentation – Talks Schedule
When: Friday 16.02.2024 @10:00 – 12:30
Where: S202/C110

Start	End	1st Session	Discipline	Topic	Presenter(s)	Adivsor(s)
10:00	10:05			Greetings and Starting Note		(Simon Althaus, Ephraim Zimmer)
10:05	10:30		Psychology	Personalization of Privacy Assistants	Sebastian Gandenberger, Vahan Demirci, Bedirhan Sahin, Till Feldner	Simon Althaus, Sara Hahn, Fransisca Hapsari
10:30	10:50		Sociology	Kritik an Social Media und der Macht von Onlineplattformen	Katharina Worster	Florian Müller, Rebecca Heigl
10:50	11:10			Algorithmic Governance & Nudging	Marvin Fink	Florian Müller, Enno Steinbrink
11:10	11:20			BREAK (Tentative/Optional)		
		2nd Session	**Discipline**	**Topic**	**Presenter(s)**	**Adivsor(s)**
11:20	11:40		Computer Science	Privacy and Utility Perception Compared to Sensor Awareness and Their Actual Privacy Implications	Beliz Balim	Matthias Gazzari, Fransisca Hapsari
11:40	12:00			Attacking Privacy in Electric Vehicle Charging Stations	Joshua Moell	Carsten Schmidt, Sara Hahn
12:00	12:20			Civil Sensor Data During War Time And In Crises	Johanna Jarsch	Enno Steinbrink, Matthias Gazzari
12:20	12:30			Closing Remarks		(Simon Althaus, Ephraim Zimmer)

TECHNISCHE UNIVERSITÄT DARMSTADT

Privacy and Trust for Mobile Users

CIVIL SENSOR DATA DURING WAR TIME AND IN CRISES

Final presentation 16.02.2024

TECHNISCHE UNIVERSITÄT DARMSTADT

Privacy and Trust for Mobile Users

MOTIVATION

BBC

Snowden NSA: Germany to investigate Merkel 'phone tap'

4 June 2014

Source: https://www.bbc.com/news/world-europe-27695634

NATO OTAN

***„NATO declared cyberspace as a domain of operations** – just like air, land, sea, and space at the Warsaw summit in 2016.“*

Source: https://www.nato.int/nato_static_fl2014/assets/pdf/pdf_2019_02/20190208_1902-factsheet-cyber-defence-en.pdf

Deutschlandfunk

10 Jahre Snowden-Enthüllungen

Die Überwachung ist immer noch überall

Am 5. Juni 2013 schreckten die Enthüllungen von Edward Snowden die Weltöffentlichkeit auf: Nicht nur Terroristen gerieten demnach ins Schleppnetz der NSA und ihrer Partner, sondern potentiell jeder. Auch der BND geriet in den Fokus. Was bleibt?

Source: https://www.deutschlandfunk.de/10-jahre-snowden-enthuellungen-allgegenwaertige-ueberwachung-trotz-nsa-skandal-dlf-4fe76758-100.html

BBC

Ukraine mobile network Kyivstar hit by 'cyber-attack'

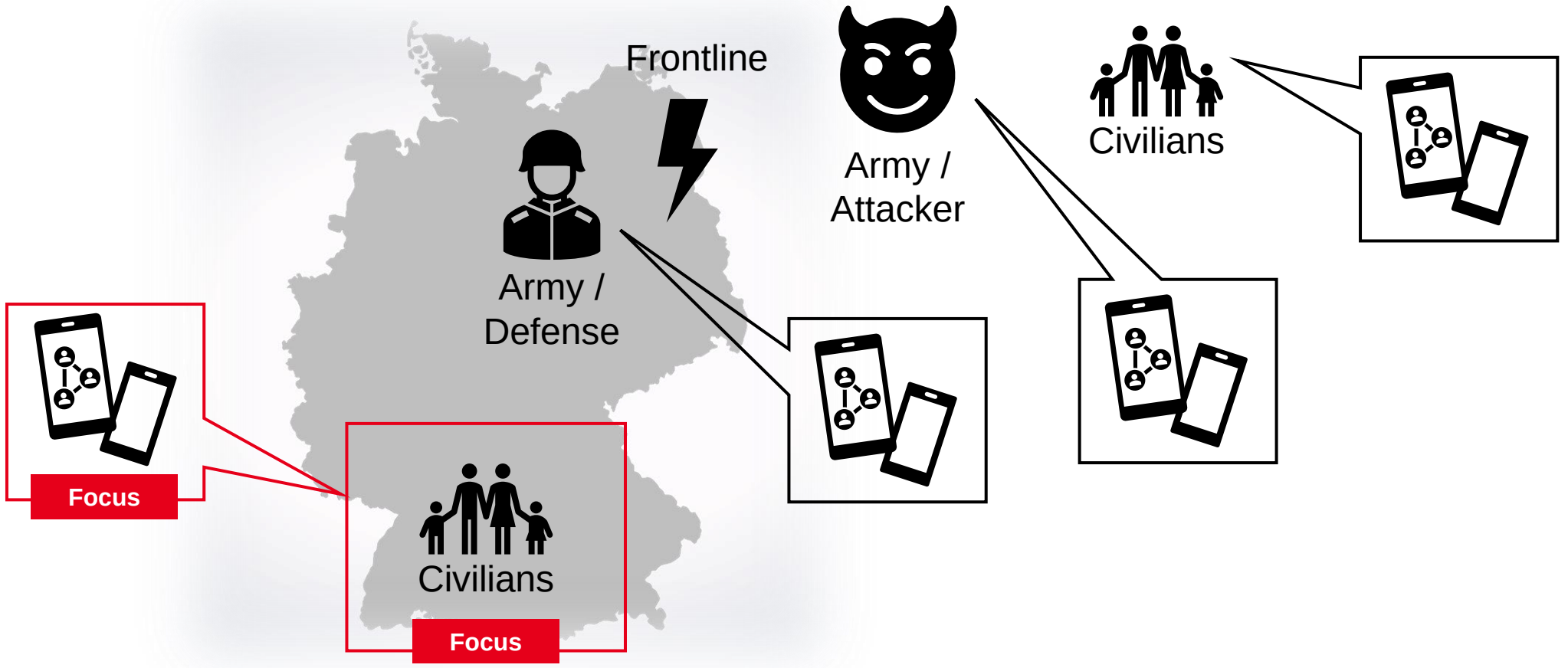
12 December 2023

Source: https://www.bbc.com/news/world-europe-67691222

TECHNISCHE UNIVERSITÄT DARMSTADT

FICTIONAL SCENARIO

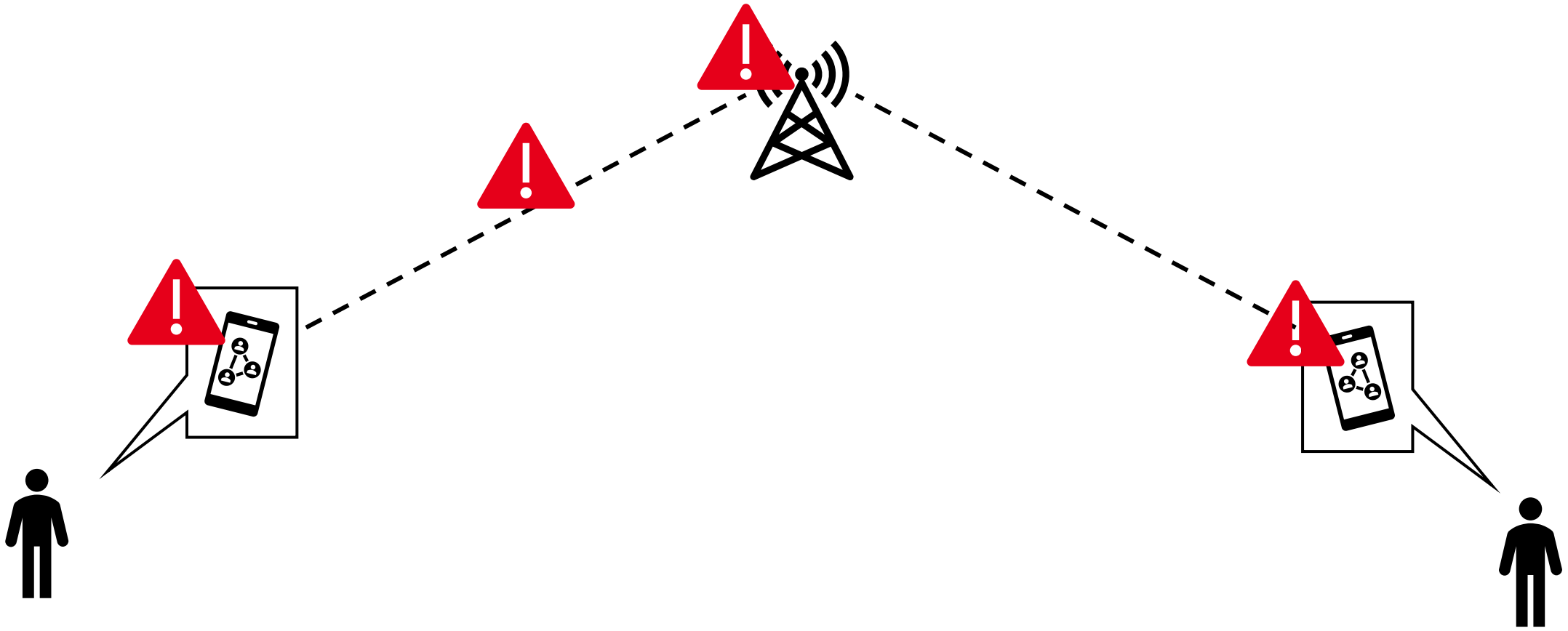
Privacy and Trust for Mobile Users



TECHNISCHE UNIVERSITÄT DARMSTADT

Privacy and Trust for Mobile Users

ATTACK VECTORS ON PHONE CALLS

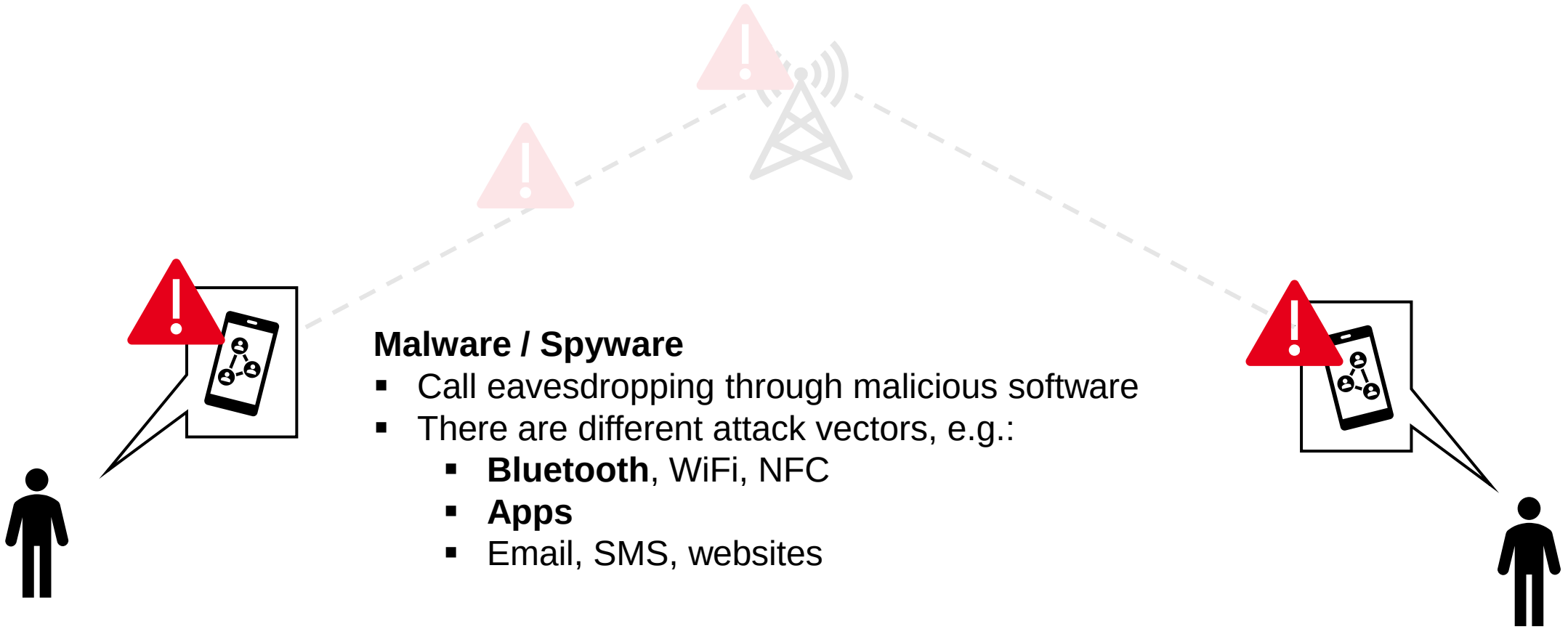


Note: Sources can be taken from the seminar paper

TECHNISCHE UNIVERSITÄT DARMSTADT

Privacy and Trust for Mobile Users

ATTACK VECTORS ON PHONE CALLS - SOFTWARE



Malware / Spyware

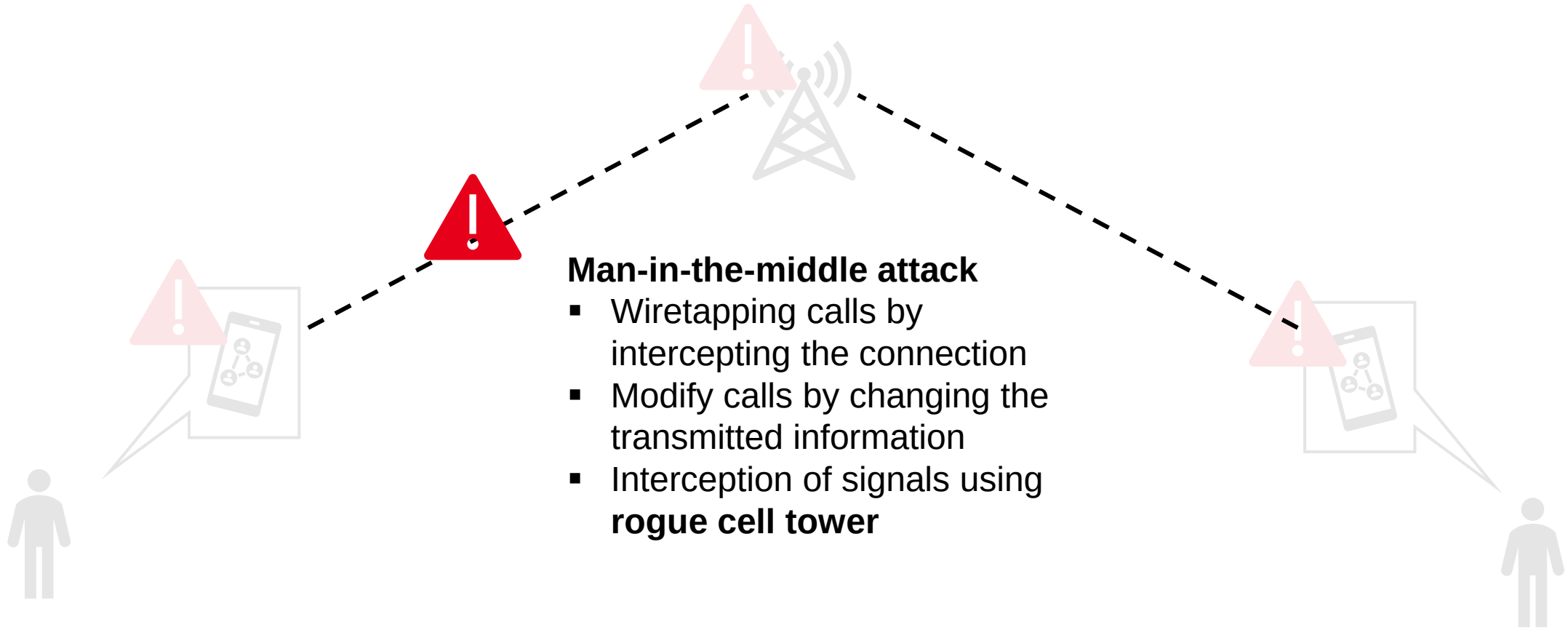
- Call eavesdropping through malicious software
- There are different attack vectors, e.g.:
  - **Bluetooth**, WiFi, NFC
  - **Apps**
  - Email, SMS, websites

Note: Sources can be taken from the seminar paper

TECHNISCHE UNIVERSITÄT DARMSTADT

Privacy and Trust for Mobile Users

ATTACK VECTORS ON PHONE CALLS - CONNECTION



Man-in-the-middle attack

- Wiretapping calls by intercepting the connection
- Modify calls by changing the transmitted information
- Interception of signals using **rogue cell tower**

Note: Sources can be taken from the seminar paper

TECHNISCHE UNIVERSITÄT DARMSTADT

Privacy and Trust for Mobile Users

ATTACK VECTORS ON PHONE CALLS - CELL TOWER

Denial of Service attack

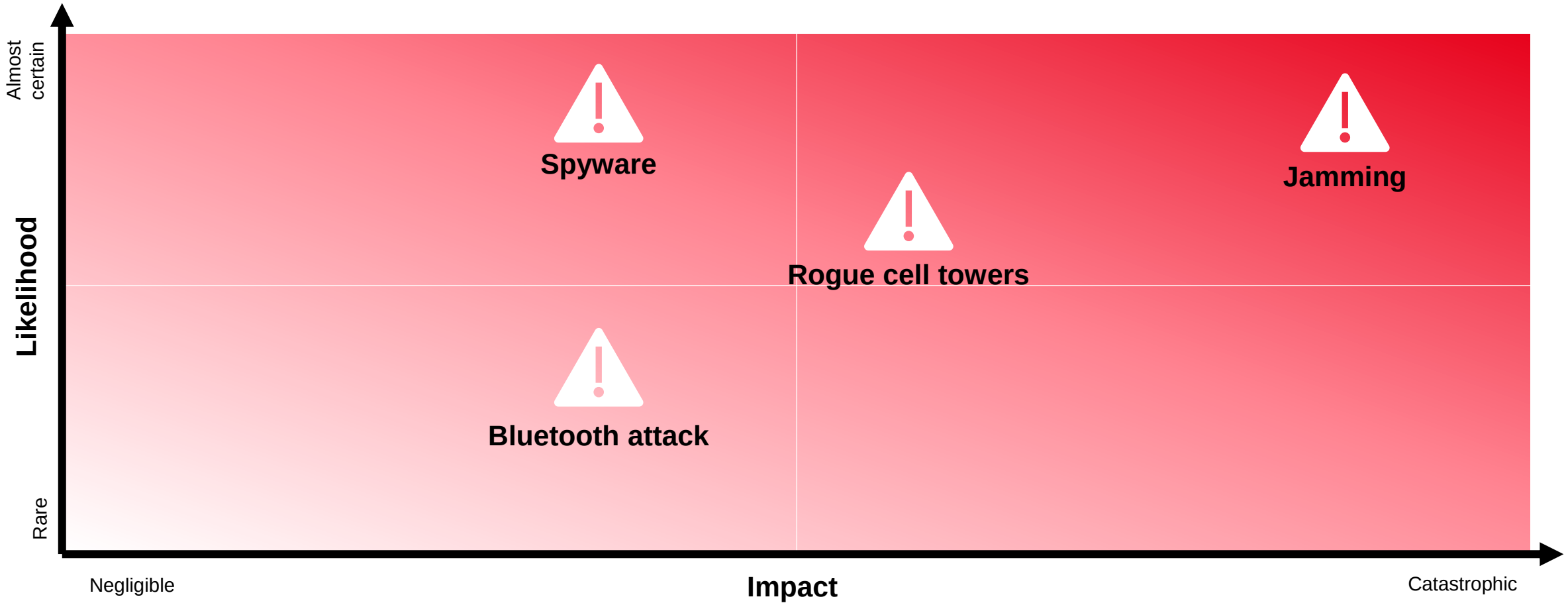
- Blocks calls from being received and initiated
- Blocking calls by, e.g.:
  - **Jamming**
  - Call flooding

Note: Sources can be taken from the seminar paper

TECHNISCHE UNIVERSITÄT DARMSTADT

Privacy and Trust for Mobile Users

RISK ASSESSMENT – QUALITATIVE RISK MATRIX



Note: Sources can be taken from the seminar paper

TECHNISCHE UNIVERSITÄT DARMSTADT

COUNTERMEASURES AGAINST NETWORK CONNECTIVITY ATTACKS

Privacy and Trust for Mobile Users

Avoidance of telephone calls and codes	*Is easy to implement without technical expertise and at low cost but requires prior agreement* *> This does not prevent surveillance, but it gives people a sense of control.*
User education	*Raise awareness for cyber attacks and provide information on easy-to-implement safety measures.* *> Achieve good basic security with little effort and cost.*
Instal mobile security software and frequently update OS and apps	*Increases the basic security of the smartphone but does not protect the connection.* *> Simple application, low effort and low costs, but protection is limited to the smartphone.*
Strong and secure encryption	*Securing the systems and data on the smartphone as well as transmitted data and connections.* *> Protection depends on the encryption. However, it is still possible to intercept and block messages.*
Monitoring mechanism for detection of malicious attacks	*Suitable for limiting the damage of attacks but does not prevent the attack.* *> This is not a measure against the realization of an attack.*
Detect Malware using machine learning or deep neural network	*Suitable for limiting the damage of attacks but does not prevent the attack.* *> Low applicability due to complexity and costs for normal users.*

Note: Sources can be taken from the seminar paper

TECHNISCHE UNIVERSITÄT DARMSTADT

OUTLOOK

Privacy and Trust for Mobile Users

Attacks	Risk	Protection
▪ Caller ID Spoofing ▪ Voicemail Hacking ▪ Social Engineering, Phishing ▪ Packet sniffing on WiFi-networks ▪ Call Flooding ▪ Network-level attacks, Network Spoofing ▪ VoIP Service Disruption ▪ Trojan, Virus ▪ Physical loss ▪ USB Charging Scams ▪ SIM swapping ▪ Zero-day Exploits	▪ Accessing location information ▪ Accessing personal information, including photos, banking information, communication ▪ Accessibility of information, misinformation and propaganda ▪ Power outage ▪ Legal risks ▪ Physical Threats, caused by unwanted attention or robbery	Security measures by: ▪ App developers ▪ OS developers ▪ Smartphone manufacturers ▪ Manufacturers of connected devices ▪ Government

TECHNISCHE UNIVERSITÄT DARMSTADT

KEY TAKE-AWAYS

Privacy and Trust for Mobile Users

1. **Civilians also have a high risk of being affected by an attack on cellular network. At the same time, there is very little research in this area.**

2. **It is questionable to what extent civilians can protect themselves from these attacks in times of war, as state actors have many resources at their disposal.**

3. **Prevention is already advisable today. Education and sensitization to the topic is particularly important.**

TECHNISCHE UNIVERSITÄT DARMSTADT

SCHEDULE

Privacy and Trust for Mobile Users

iPAT Seminar WiSe23/24 – Final Presentation – Talks Schedule
When: Friday 16.02.2024 @10:00 – 12:30
Where: S202/C110

Start	End	1st Session	Discipline	Topic	Presenter(s)	Adivsor(s)
10:00	10:05			Greetings and Starting Note		(Simon Althaus, Ephraim Zimmer)
10:05	10:30		Psychology	Personalization of Privacy Assistants	Sebastian Gandenberger, Vahan Demirci, Bedirhan Sahin, Till Feldner	Simon Althaus, Sara Hahn, Fransisca Hapsari
10:30	10:50		Sociology	Kritik an Social Media und der Macht von Onlineplattformen	Katharina Worster	Florian Müller, Rebecca Heigl
10:50	11:10			Algorithmic Governance & Nudging	Marvin Fink	Florian Müller, Enno Steinbrink
11:10	11:20			BREAK (Tentative/Optional)		
		2nd Session	**Discipline**	**Topic**	**Presenter(s)**	**Adivsor(s)**
11:20	11:40		Computer Science	Privacy and Utility Perception Compared to Sensor Awareness and Their Actual Privacy Implications	Beliz Balim	Matthias Gazzari, Fransisca Hapsari
11:40	12:00			Attacking Privacy in Electric Vehicle Charging Stations	Joshua Moell	Carsten Schmidt, Sara Hahn
12:00	12:20			Civil Sensor Data During War Time And In Crises	Johanna Jarsch	Enno Steinbrink, Matthias Gazzari
12:20	12:30			Closing Remarks		(Simon Althaus, Ephraim Zimmer)