TECHNISCHE UNIVERSITÄT DARMSTADT

Privacy and Trust for Mobile Users

IPAT SEMINAR – INTERMEDIARY PRESENTATIONS

TECHNISCHE UNIVERSITÄT DARMSTADT

Privacy and Trust for Mobile Users

AGENDA

1 Organizational Remarks

2 Sociology: Katharina Worster

3 Psychology: Demirci, Sahin, Gandenberger, Feldner

4 Computer Science: Johanna Jarsch

5 Computer Science: Joshua Moell

6 Computer Science: Beliz Balim

7 Discussion

TECHNISCHE UNIVERSITÄT DARMSTADT

Privacy and Trust for Mobile Users

INTERMEDIARY PRESENTATIONS

- Format
  - ~5 minutes per seminar topic
  - Followed by short Q&A session per topic
- Content
  - General description, introduction of the research problem, main challenges, etc.
  - Current status of the work, keywords, search results, etc.

TECHNISCHE UNIVERSITÄT DARMSTADT

Privacy and Trust for Mobile Users

KRITIK AN SOCIAL MEDIA UND DER MACHT VON ONLINEPLATTFORMEN

Katharina Worster

Soziologie

Uni Kassel

TECHNISCHE UNIVERSITÄT DARMSTADT

Privacy and Trust for Mobile Users

ALGORITHMEN ALS PROBLEMATIK

- Algorithmen können durch Nutzer manipuliert werden -> missbräuchliche Absichten, wie bspw. Belästigung oder Schädigung anderer
- Können eine Gefahr für die Öffentlichkeit darstellen, bspw. Durch die Verbreitung von Hassreden und Fehlinformationen
- Filterblasen und Echokammern sorgen für eine verzerrte Wahrnehmung der tatsächlichen Realität
- Diskriminierung und Marginalisierung von bestimmten Gruppen und Minderheiten

TECHNISCHE UNIVERSITÄT DARMSTADT

Privacy and Trust for Mobile Users

GEFAHR DURCH SOCIAL MEDIA

- Online Hassreden -> betroffen sind bestimmte Gruppen, die sich Eigenschaften, wie z.B. Religion, Ethnizität oder Geschlecht teilen
- Motiviert durch Ideologien
- Negativer Einfluss auf die mentale Gesundheit und das Wohlbefinden von Kindern und Jugendlichen
- Stress, Depressionen, suizidale Gedanken und Abhängigkeit

TECHNISCHE UNIVERSITÄT DARMSTADT

Privacy and Trust for Mobile Users

INDIVIDUALISIERUNGSMÖGLICHKEITEN PRIVACY BUDDY

Demirci, Sahin, Gandenberger, Feldner

Fachbereich 3 (Humanwissenschaften)

TU Darmstadt

TECHNISCHE UNIVERSITÄT DARMSTADT

ZIELSETZUNG

Privacy and Trust for Mobile Users

Ausgangslage:

Der Privacy Buddy soll Personen in Privatsphäre Themen aufklären und unterstützen.

Aber:

Vorherige Arbeiten haben gezeigt, dass Personen unterschiedliche Bedürfnisse an ein Privacy Support Tool haben. (Anonymous Author(s), 2024; Schmidt, 2020)

Zielsetzung:

Empirisch erhobene Empfehlungen für Individualisierungsmöglichkeiten des Privacy Buddy ableiten

TECHNISCHE UNIVERSITÄT DARMSTADT

Privacy and Trust for Mobile Users

VORGEHEN UND AKTUELLER STAND

1. Zusammentragen von Literatur bezüglich Privatsphäre und Privacy Support Tools (Nutzergruppen, Bedürfnisse, Motivationen)
2. Abwägen von methodischen Möglichkeiten (z.B. Qualitativ oder Quantitativ)
   → *Entscheidung*: Fragebogen, da bereits explorative Vorarbeiten bestehen und wir die Meinung möglichst vieler Personen erfassen wollen
3. Ausarbeiten eines 2-geteilten Fragebogens:
   a. Integration bestehender Fragebögen bezüglich Bedürfnisse an ein Privacy Support Tool (Validität der Tests bereits bestätigt)
   b. Ausarbeitung eigener Items mit spezifischen Individualisierungsvorschlägen (z.B. wie oft möchtest du benachrichtigt werden, wenn eine andere App Daten abführt → 0 – gar nicht; 5 – jedes Mal)

TECHNISCHE UNIVERSITÄT DARMSTADT

Privacy and Trust for Mobile Users

VORGEHEN UND AKTUELLER STAND

1. Zusammentragen von Literatur bezüglich Privatsphäre und Privacy Support Tools (Nutzergruppen, Bedürfnisse, Motivationen)
2. Abwägen von methodischen Möglichkeiten (z.B. Qualitativ oder Quantitativ)
   → *Entscheidung*: Fragebogen, da bereits explorative Vorarbeiten bestehen und wir die Meinung möglichst vieler Personen erfassen wollen
3. Ausarbeiten eines 2-geteilten Fragebogens:
   a. Integration bestehender Fragebögen bezüglich Bedürfnisse an ein Privacy Support Tool (Validität der Tests bereits bestätigt)
   b. Ausarbeitung eigener Items mit spezifischen Individualisierungsvorschlägen (z.B. wie oft möchtest du benachrichtigt werden, wenn eine andere App Daten abführt → 0 – gar nicht; 5 – jedes Mal)

TECHNISCHE UNIVERSITÄT DARMSTADT

Privacy and Trust for Mobile Users

VORGEHEN UND AKTUELLER STAND

1. Zusammentragen von Literatur bezüglich Privatsphäre und Privacy Support Tools (Nutzergruppen, Bedürfnisse, Motivationen)
2. Abwägen von methodischen Möglichkeiten (z.B. Qualitativ oder Quantitativ)
   → *Entscheidung*: Fragebogen, da bereits explorative Vorarbeiten bestehen und wir die Meinung möglichst vieler Personen erfassen wollen
3. Ausarbeiten eines 2-geteilten Fragebogens:
4. Umfrage mit möglichst vielen Versuchspersonen
5. Auswertung mittels verschiedener Clusteranalyseverfahren

Gewünschtes Ergebnis:

Gruppe X legt bei Feature X einen großen Wert auf X. Im Gegensatz dazu ist für Gruppe Y Feature Y von besonderer Bedeutung.

TECHNISCHE UNIVERSITÄT DARMSTADT

QUELLEN

Privacy and Trust for Mobile Users

Anonymous Author(s). 2024. 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, NY, USA, 36 pages.

Schmidt, J. (2020). *„Privacy Paradox": An analysis of different factors to categorize internet users* (unveröffentlichte Masterarbeit). Technische Universität Darmstadt, Darmstadt.

TECHNISCHE UNIVERSITÄT DARMSTADT

Privacy and Trust for Mobile Users

CIVIL SENSOR DATA DURING WAR TIME AND IN CRISES

Johanna Jarsch

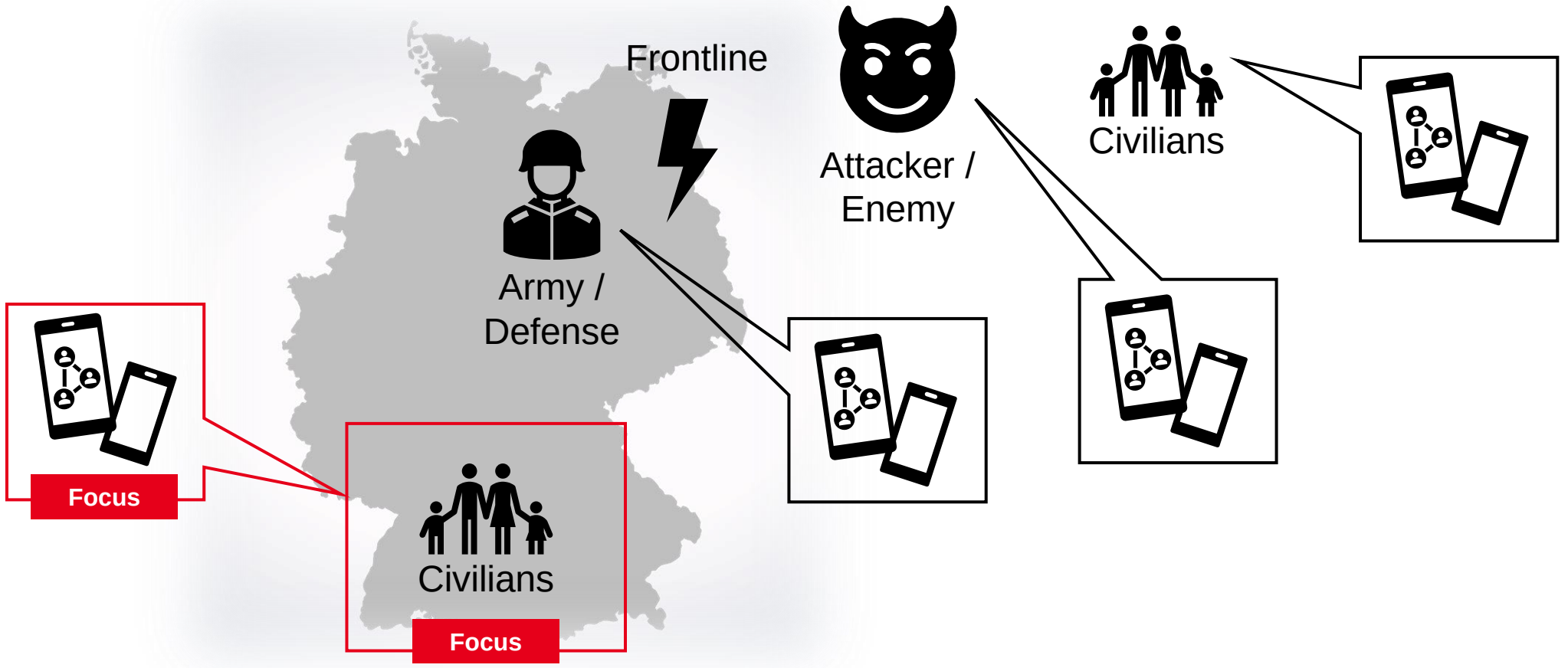
Business Informatics

TU Darmstadt

TECHNISCHE UNIVERSITÄT DARMSTADT

FICTIONAL SCENARIO

Privacy and Trust for Mobile Users



TECHNISCHE UNIVERSITÄT DARMSTADT

SECURITY RISKS FOR CIVILIANS

Privacy and Trust for Mobile Users

Accessing to location information	*E. g. localisation by light, mobile radio or GPS possible*
Accessing personal information	*E. g. through malware, loss or usage of unsecured devices*
Attack on communication	*E. g. when communicating via mobile phones, social networks or WIFI*
Accessability of information	*E. g. this can be made more difficult by fake news, internet restrictions, sabotage or censorship*
Power outage	*E. g. smartphone battery does not long that last, channels such as WIFI and mobile network fail*
Legal risks	*E. g. civilians who report observations and document them*

Note: Sources can be taken from the seminar paper

TECHNISCHE UNIVERSITÄT DARMSTADT

CHALLENGES

Privacy and Trust for Mobile Users

Note: AI generated pictures

TECHNISCHE UNIVERSITÄT DARMSTADT

Privacy and Trust for Mobile Users

ATTACKING PRIVACY IN ELECTRIC VEHICLE CHARGING STATIONS

Joshua Moell

Computer Science

TU Darmstadt

TECHNISCHE UNIVERSITÄT DARMSTADT

OBJECTIVES

Privacy and Trust for Mobile Users

- Overview
- Compare to attacker models in IT Security
- Information Sheet

TECHNISCHE UNIVERSITÄT DARMSTADT

OVERVIEW

Privacy and Trust for Mobile Users

- Main Components
  - Electric Vehicle (EV)
  - Charging Point (CP)
  - Network
  - Backend
- Attacker Models (sorted by Components)
  - EV Compromised
  - CP Compromised
  - Network compromised
  - Backend Data Leaked
- Consequences of a Successful Attack
  - Financial damage
  - Power Grid stability issues
  - Interruption of the Charging process / Denial of Service
  - Location Tracking / Movement profile
  - Identity Theft / personal data theft
  - Network Attacker could charge a vehicle at the cost of somebody else

TECHNISCHE UNIVERSITÄT DARMSTADT

Privacy and Trust for Mobile Users

NEXT STEPS

- Gather More Information for the Overview
- Compare to attacker models in IT Security
- Information Sheet

PRIVACY AND UTILITY PERCEPTION COMPARED TO SENSOR AWARENESS AND THEIR ACTUAL PRIVACY IMPLICATIONS

Beliz Balim

Computer Science

TU Darmstadt

INTRODUCTION

TECHNISCHE UNIVERSITÄT DARMSTADT

Privacy and Trust for Mobile Users

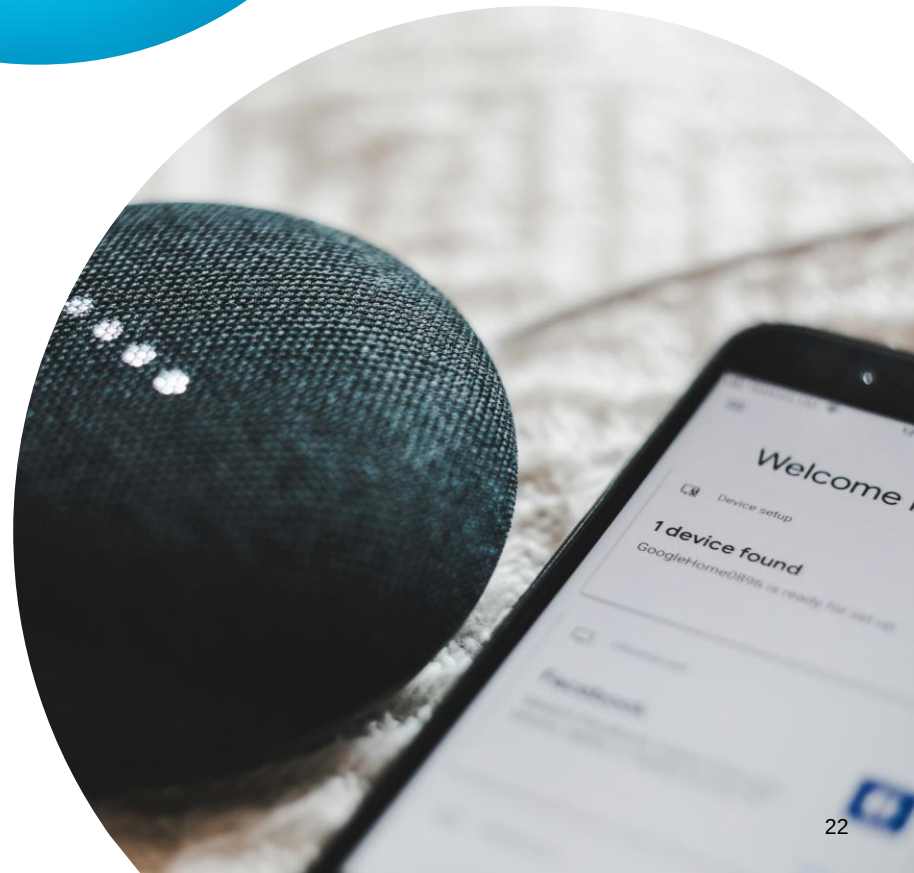
Widespread integration of sensors in our lives, e.g.

- Smart homes & smart workplace
- Fitness trackers
- Mobile phones

Benefits such as supporting in daily tasks, monitoring health metrics, and facilitating personalized learning experiences, ...

Potential violation of user and bystander privacy

The balance between the benefits of sensor technologies and the need to protect individual privacy necessitates an examination



TECHNISCHE UNIVERSITÄT DARMSTADT

Privacy and Trust for Mobile Users

RESEARCH QUESTIONS

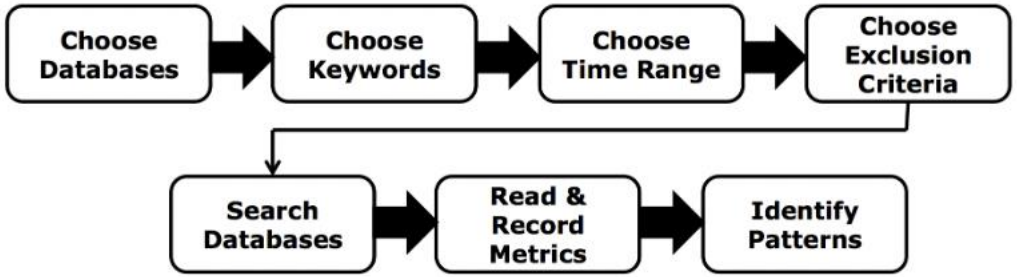
- R1: Does the perceived privacy threat and expected utility match the actual risks and benefits of sensors?
- R2: How much is the perception dependent on sensor awareness and how can we positively influence it?

TECHNISCHE UNIVERSITÄT DARMSTADT

RESEARCH APPROACH

Privacy and Trust for Mobile Users

- Systematic literature review described by Pickering and Byrne (2014)
- Current status:
  - Ca. 25 studies identified as eligible
  - Kew words
    - IOT, wearables, smart home, smart buildings, smart environments, sensor awareness, privacy risks, privacy threats, privacy concern, sensor utility, perceived benefits, privacy preserving measures
  - Identification of patterns in progress



TECHNISCHE UNIVERSITÄT DARMSTADT

STORYLINE OF THE PAPER

Privacy and Trust for Mobile Users

- R1: Does the perceived privacy threat and expected utility match the actual risks and benefits of sensors?
  - Which areas of daily life do individuals perceive utility from sensor-enabled technologies?
  - What are the factors impacting the individuals' privacy concerns?
  - What are the actual privacy implications?
  - Evaluation of the match between percived utility, risks and actual implications
- R2: How much is the perception dependent on sensor awareness and how can we positively influence it?
  - What does sensor awareness mean?
  - To what extent ist privacy and utility perception dependent on sensor awareness?
  - What are measures addressing privacy concerns and increasing sensor awareness?

TECHNISCHE UNIVERSITÄT DARMSTADT

Privacy and Trust for Mobile Users

DISCUSSION