TECHNISCHE UNIVERSITÄT DARMSTADT

Privacy and Trust for Mobile Users

INTERDISCIPLINARY SEMINAR ON PRIVACY AND TRUST FOR MOBILE USERS (IPAT SEMINAR)

3 CP, Winter Term 2023/24

Ephraim Zimmer, Simon Althaus

zimmer@privacy-trust.tu-darmstadt.de, althaus@tk.tu-darmstadt.de

TECHNISCHE UNIVERSITÄT DARMSTADT

Privacy and Trust for Mobile Users

TODAY

1 General Information

2 Interdisciplinary Aspects

3 Seminar Topics

GENERAL INFORMATION

TECHNISCHE UNIVERSITÄT DARMSTADT

Privacy and Trust for Mobile Users

Get (first) **insights** into **scientific** research

Improve your **in-depth knowledge** about interesting (mostly) privacy and trust related topics

Improve scientific **reading** and **writing** capabilities

What will you learn?

Topic → Study it

Write a **report** [academic paper style]

Interdisciplinary exchange with others

Present your **final report**

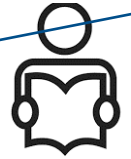
What will you do?

iPAT Seminar

Computer science bachelor and master students

+ joined by other disciplines (more on that later)

For Who?



GENERAL INFORMATION (CONT.)

TECHNISCHE UNIVERSITÄT DARMSTADT

Privacy and Trust for Mobile Users

Participate

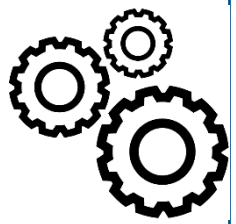
Register in TUCaN (**20-00-1183-se**)

Read/Write German/English
[Advisor]

Scope

You get **3** graded credit points:

- **Written report**:
  10-12 pages IEEE transactions template (team of two)
- **Final presentation**:
  details will be announced later



Schedule (tentative)

17th October (now)
- ✓ Introduction
- ✓ Topic presentation

22nd October
Topic selection deadline

23rd October
Topic assignment notification

30th October
Interdisciplinary Kick-Off
Scientific Publication & Review

11th December
Intermediary session/presentations

16th February
Presentation day

1st March
Final submission of the report

EVALUATION AND GRADING DETAIL

TECHNISCHE UNIVERSITÄT DARMSTADT

Privacy and Trust for Mobile Users

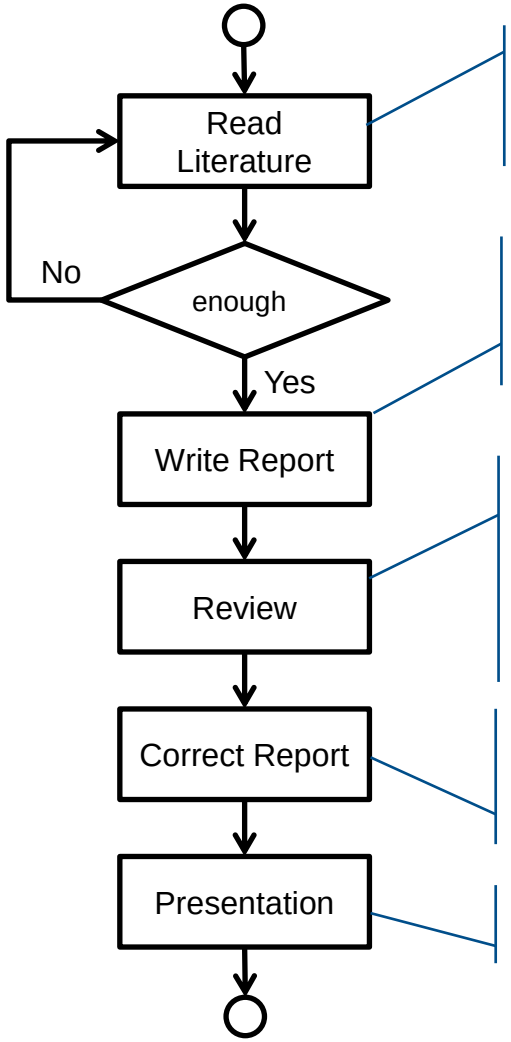
Report	Presentation
Length	Time management
Structure	Content
Content ! ! !	Presentation style
Quality of references	Structure

You need to pass all parts!

5 STEPS TO SUCCESS

TECHNISCHE UNIVERSITÄT DARMSTADT

Privacy and Trust for Mobile Users



Pick a topic, read the provided literature and find more literature

Write an overview/first version of your report

This is more than a simple paper collection!

Review Process

Your report will be reviewed by your advisor

Integrate comments to improve and finalize your report

Present your final work

WHAT TO DO NEXT?

TECHNISCHE UNIVERSITÄT DARMSTADT

Privacy and Trust for Mobile Users

Submit your topic preferences until the end of this week (22nd October)!

→ After successful topic assignment, contact your designated topic advisor until 27th October

All announcement, materials, and further information can be found on our website: https://www.informatik.tu-darmstadt.de/telekooperation/teaching_tk/winter_term_2023___24/interdiscipliniary_seminar_in_privacy_and_trust_/tk_pin_1.en.jsp

Be **proactive**!

Ask your advisor!

Start as **Early** as Possible!

INTERDISCIPLINARY ASPECTS

TECHNISCHE UNIVERSITÄT DARMSTADT

Privacy and Trust for Mobile Users

- Your seminar topics will have a focus on computer science topics
- Your topic can comprise interdisciplinary aspects from the fields of psychology, information systems, laws, and sociology.
- Goal: Bringing different disciplines together and exchanging knowledge
- In the remaining seminar sessions, you will be joined by students from
  - Computer Science (TU Darmstadt)
  - Psychology (TU Darmstadt)
  - Sociology (University of Kassel)

TECHNISCHE UNIVERSITÄT DARMSTADT

Privacy and Trust for Mobile Users

IPAT SEMINAR TOPICS

Winter Term 2023/24

TECHNISCHE UNIVERSITÄT DARMSTADT

Privacy and Trust for Mobile Users

TOPIC SELECTION

- Each topic will be assigned to a group of two students.
- You (each student) can select 3 topics that you like and 3 that you would not want to be assigned, by sending an email to althaus@tk.tu-darmstadt.de (Simon Althaus) specifying the following information in the email:

  ****
  Subject of the email: [iPAT Seminar WS 2023/24] – Topic Selection
  Body of the email:
  Student: <Your Name>, <Your Surname>
  Topic I would like to be assigned:
  Preference 1: <Topic Id>
  Preference 2: <Topic Id>
  Preference 3: <Topic Id>
  Topic that I would NOT want to be assigned:
  Preference 1: <Topic Id>
  Preference 2: <Topic Id>
  Preference 3: <Topic Id>
  ****

- Please notice that the final evaluation and grades will be done on the report (even though a topic will be assigned to a group of two students).
- Mind the deadline for the topic selection announced here
- After the deadline, and based on your preferences, you will be assigned to a group bearing the name of the topic. Then, you should take the initiative and contact the specific topic supervisor (e.g. via email) for initial material and guidance throughout the seminar (you can find the names and emails of our nice colleagues who provided topics for this semester on the title slide of each topic).

TECHNISCHE UNIVERSITÄT DARMSTADT

Privacy and Trust for Mobile Users

TOPIC 1: PRIVACY AND UTILITY PERCEPTION COMPARED TO SENSOR AWARENESS AND THEIR ACTUAL PRIVACY IMPLICATIONS

Matthias Gazzari (mgazzari@seemoo.tu-darmstadt.de)

Fransisca Hapsari (fransisca.hapsari@tu-darmstadt.de)

Computer Science & Psychology

TOPIC 1: PRIVACY AND UTILITY PERCEPTION COMPARED TO SENSOR AWARENESS AND THEIR ACTUAL PRIVACY IMPLICATIONS

TECHNISCHE UNIVERSITÄT DARMSTADT

Privacy and Trust for Mobile Users

- **Overview**
  - Sensors in smart homes or as part of wearables provide many utilities like automating your household, tracking your health, or supporting learning. However, these sensors also provide many ways to violate the privacy of users and bystanders alike. What are meaningful and appropriate ways to use these sensors?
- **Research questions**
  - Does the perceived privacy threat and expected utility match the actual risks and benefits of sensors?
  - How much is the perception dependent on sensor awareness and how can we positively influence it?
- **Tasks**
  - Summarize the state of the art on privacy and utility perception of sensors in the light of actual sensor awareness.
  - Compare perceived privacy risks with actual privacy implications.
  - Summarize appropriate coping strategies and awareness measures to support users and bystanders in using sensors.
- **References** (initial reading material to get you started)

  - Velykoivanenko, Lev, Kavous Salehzadeh Niksirat, Noé Zufferey, Mathias Humbert, Kévin Huguenin, and Mauro Cherubini. 2022. “Are Those Steps Worth Your Privacy? Fitness-Tracker Users’ Perceptions of Privacy and Utility.” Proceedings of the ACM on Interactive, Mobile, Wearable and Ubiquitous Technologies 5 (4): 181:1-181:41. https://doi.org/10.1145/3494960
  - Windl, Maximiliane, and Sven Mayer. 2022. “The Skewed Privacy Concerns of Bystanders in Smart Environments.” Proceedings of the ACM on Human-Computer Interaction 6 (MHCI): 184:1-184:21. https://doi.org/10.1145/3546719
  - Wang, Qiaosi & Jing, Shan & Joyner, David & Wilcox, Lauren & Li, Hong & Ploetz, Thomas & Disalvo, Betsy. (2020). Sensing Affect to Empower Students: Learner Perspectives on Affect-Sensitive Technology in Large Educational Contexts. 63-76. https://doi.org/10.1145/3386527.3405917

TECHNISCHE UNIVERSITÄT DARMSTADT

Privacy and Trust for Mobile Users

TOPIC 2: PRIVACY AND REGULATORY CONSIDERATIONS IN REAL-WORLD APPLICATIONS OF SECURE MULTI-PARTY COMPUTATION

Andreas Brüggemann (brueggemann@encrypto.cs.tu-darmstadt.de)

Loïc Reissner (reissner@jur.uni-frankfurt.de)

Computer Science & Law

TECHNISCHE UNIVERSITÄT DARMSTADT

Privacy and Trust for Mobile Users

TOPIC 2: PRIVACY AND REGULATORY CONSIDERATIONS IN REAL-WORLD APPLICATIONS OF SECURE MULTI-PARTY COMPUTATION

- **Motivation**
  - Secure Multi-Party Computation (MPC) provides cryptographic primitives that enable multiple parties to process their joined data without any party disclosing its data to others. It relies on certain theoretical considerations on how strong an adversary/attacker may be.
  - Privacy and regulatory concerns of users or companies, and legal requirements such as the GDPR pose challenges when exchanging and processing data.
- **Objective**
  - Given a real-world application, which theoretical adversary matches the real-world risks connected to the application?
  - Which (legal) considerations were made for existing MPC applications, and why?
- **Task**
  - Summarize the existing types of theoretical adversaries.
  - Then, for at least 2 real-world MPC applications, analyze what adversary they consider, how they assess given (legal) privacy risks, and how the choice of the adversary is justified given the specific risks.
- **References** (These are directions, you may choose any other MPC application)
  - D. W. Archer, D. Bogdanov, Y. Lindell, L. Kamm, K. Nielsen, J. Illeborg Pagter, N. P. Smart, and R. N. Wright. “From Keys to Databases—Real-World Applications of Secure Multi-Party Computation.” In The Computer Journal 61(12), 2018. https://doi.org/10.1093/comjnl/bxy090
  - J. Lindell. “Secure Multiparty Computation (MPC).” In CACM 64(1), 2021. https://doi.org/10.1145/3387108
  - United Nations, Department of Economic and Social Affairs, Statistics Division. “The PET Guide: The United Nations Guide on Privacy-Enhancing Technologies for Official Statistics.” 2023. https://unstats.un.org/bigdata/task-teams/privacy/guide/index.cshtml

TECHNISCHE UNIVERSITÄT DARMSTADT

Privacy and Trust for Mobile Users

TOPIC 3: AUTOMATED ANDROID APPLICATION INSPECTION AND MANIPULATION

Simon Althaus (althaus@tk.tu-darmstadt.de)

Loïc Reissner (reissner@jur.uni-frankfurt.de)

Computer Science & Law

TOPIC 3: AUTOMATED ANDROID APPLICATION INSPECTION AND MANIPULATION

TECHNISCHE UNIVERSITÄT DARMSTADT

Privacy and Trust for Mobile Users

- **Motivation**
  - Collection of personal user data and habits by mobile apps, oftentimes without the user being aware of it or the extend
  - → Investigation of privacy-leaking behavior of Android applications necessary
- **Objective**
  - How can we determine which part of an Android application's source code is responsible for given observable Android application behavior?
  - How can we automatically manipulate Android application code (i.e. injecting privacy harming behavior)?
  - Are we allowed to do so from a legal perspective? (decompilation vs. open source apps)
- **Task**
  - Provide a literature review of scientific papers about the objectives mentioned above.
  - Conduct hands on testing, configuration, and extraction of potential solutions.
- **References** (initial reading material to get you started)
  - Samhi, Jordan, Tegawendé F. Bissyandé, and Jacques Klein. "TriggerZoo: A Dataset of Android Applications Automatically Infected with Logic Bombs." Proceedings of the 19th International Conference on Mining Software Repositories. 2022. https://doi.org/10.1145/3524842.3528020
  - Schütte, Julian, Rafael Fedler, and Dennis Titze. "Condroid: Targeted dynamic analysis of android applications." 2015 IEEE 29th International Conference on Advanced Information Networking and Applications. IEEE, 2015. https://doi.org/10.1109/AINA.2015.238

TECHNISCHE UNIVERSITÄT DARMSTADT

Privacy and Trust for Mobile Users

TOPIC 4: ATTACKING PRIVACY IN ELECTRIC VEHICLE CHARGING STATIONS

Carsten Schmidt (carsten.schmidt@sit.tu-darmstadt.de)

Sara Hahn (sara.hahn@tu-darmstadt.de)

Computer Science & Psychology

TECHNISCHE UNIVERSITÄT DARMSTADT

Privacy and Trust for Mobile Users

TOPIC 4: ATTACKING PRIVACY IN ELECTRIC VEHICLE CHARGING STATIONS

- **Motivation**
  - In theory, charging station providers can track their users location within their network.
  - Furthermore, the charging process can be compromised by several other parties.
- **Objectives**
  - Get an overview of several methods how the users privacy could be harmed while the user is charging their Electric Vehicle.
  - Discuss these attacker models and compare them to attacker models in IT security
  - Design an information sheet how the users could be made aware of these attacks
- **Method**
  - Literature Review
  - “Product design”: Information sheet
- **References**
  - ISO 15118
  - More initial reading material to get you started will be provided later

TECHNISCHE UNIVERSITÄT DARMSTADT

Privacy and Trust for Mobile Users

TOPIC 5: CIVIL SENSOR DATA DURING WAR TIME AND IN CRISES

Enno Steinbrink (steinbrink@peasec.tu-darmstadt.de)

Matthias Gazzari (mgazzari@seemoo.tu-darmstadt.de)

Computer Science & Psychology

TOPIC 5: CIVIL SENSOR DATA DURING WAR TIME AND IN CRISES

- **Motivation**
  - Civil internet and communication technology or IoT devices generate a lot of data
  - This data can be used for localization, targeting and crowdsensing in military contexts as well as for crisis management, which can be either dangerous or beneficial for the user
- **Objective**
  - Consider a specific scenario. What are possible attack vectors in this specific scenario?
  - Which examples are/were practically used?
- **Task** (open for discussion)
  - Conduct a literature research of scientific papers
  - Come up with a realistic, detailed scenario
  - Classify different attacks and risks associated (e.g. for civilians) with a thread model (backed by literature)
  - Be creative
- **References**
  - Horbyk, R. “The war phone”: mobile communication on the frontline in Eastern Ukraine. Digi War 3, 9–24 (2022). https://doi.org/10.1057/s42984-022-00049-2 (especially the section “Soft targets: targeting and spotting”)
  - N. Suri et al., "Analyzing the applicability of Internet of Things to the battlefield environment," 2016 International Conference on Military Communications and Information Systems (ICMCIS), Brussels, Belgium, 2016, pp. 1-8, doi: 10.1109/ICMCIS.2016.7496574.
  - B. Lashkari, J. Rezazadeh, R. Farahbakhsh and K. Sandrasegaran, "Crowdsourcing and Sensing for Indoor Localization in IoT: A Review," in IEEE Sensors Journal, vol. 19, no. 7, pp. 2408-2434, 1 April1, 2019, doi: 10.1109/JSEN.2018.2880180. (especially the section on crowd sourcing vs sensing)

TECHNISCHE UNIVERSITÄT DARMSTADT

Privacy and Trust for Mobile Users

TOPIC 6: DEEP PRIVACY ADHERENCE MONITORING FOR SYSGRAPHING

Ephraim Zimmer (zimmer@privacy-trust.tu-darmstadt.de)

Andreas Brüggemann (brueggemann@encrypto.cs.tu-darmstadt.de)

Computer Science (Systems Security & Cryptography)

TECHNISCHE UNIVERSITÄT DARMSTADT

Privacy and Trust for Mobile Users

TOPIC 6: DEEP *PRIVACY ADHERENCE* MONITORING FOR SYSGRAPHING

- **Motivation**
  - Operating systems, applications, and protocols implementations promise to adhere to modern privacy standards (purpose limitation, confidentiality, etc.)
  - Users' trust in those promises is granted based on reputation or selective/assumed auditing (or privacy indifference ;-p)
- **Objective**
  - Find low-level ways of dynamically monitoring the adherence to privacy promises/standards
  - Acquire as much information as needed for SysGraphing this privacy adherence
- **Task** (open for discussion)
  - Focus on System Call Monitoring (OS auditing) mechanisms, which can be utilized for SysGraphing
  - Consider the two scenarios of (1) purpose limitation in sensor utilization as well as (2) confidentiality in cryptographic protocols
  - Conduct a literature research of scientific papers, system documentations, and developer guides
  - Be creative
- **References**
  - Zimmer, E. "Insider Threat Protection via SysGraph Signatures." In Privacy-friendly Detection and Prevention of Insider Threats. PhD Thesis. Staats- und Universitätsbibliothek Hamburg Carl von Ossietzky. Available at: https://ediss.sub.uni-hamburg.de/handle/ediss/8860 (German).
  - Lindell, J. "Secure Multiparty Computation (MPC)." In CACM 64(1), 2021. https://doi.org/10.1145/3387108