JYVÄSKYLÄN YLIOPISTO
UNIVERSITY OF JYVÄSKYLÄ

“Elderly, with location data, while shopping?”

Spotting Privacy Threats Beyond Software: A Quasi-Experimental Study

Authors: Tuisku Sarrala and Tommi Mikkonen

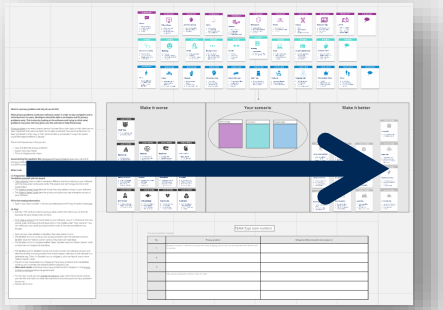
Presenter: Tuisku Sarrala, University of Jyväskylä tuisku.rad.sarrala@jyu.fi

IARIA

Tuisku Sarrala

- Academic
  - Doctoral student (DBA), Information Technology, Jyväskylä University, Finland
  - Master's Degree in Cyber Security, JAMK University of Applied Sciences, Finland, 2021
  - BSc(Hons) Computing & Systems Practice (Open), The Open University, UK, 2014
- Professional
  - Privacy professional with 10+ years of experience, currently Cyber Security & Privacy Manager at Nokia Technologies
  - CIPP/E, CIPT

Broadening developers' view of privacy



Motivation

Problem situation

- Privacy legislation
- Developers' understanding

Approach

- Engineering activity
  - Privacy threat modeling
- Approach
  - Systems thinking
- Implementation
  - Personas technique
  - Scenarios technique
  - Ideation cards

Research Question

- RQ: *How does a method with systems thinking features compare to a method with traditional features in privacy threat discovery in terms of identified threats?*

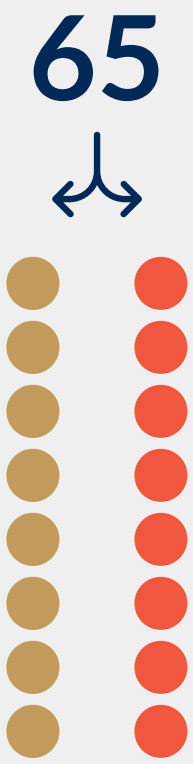
Experiment setting

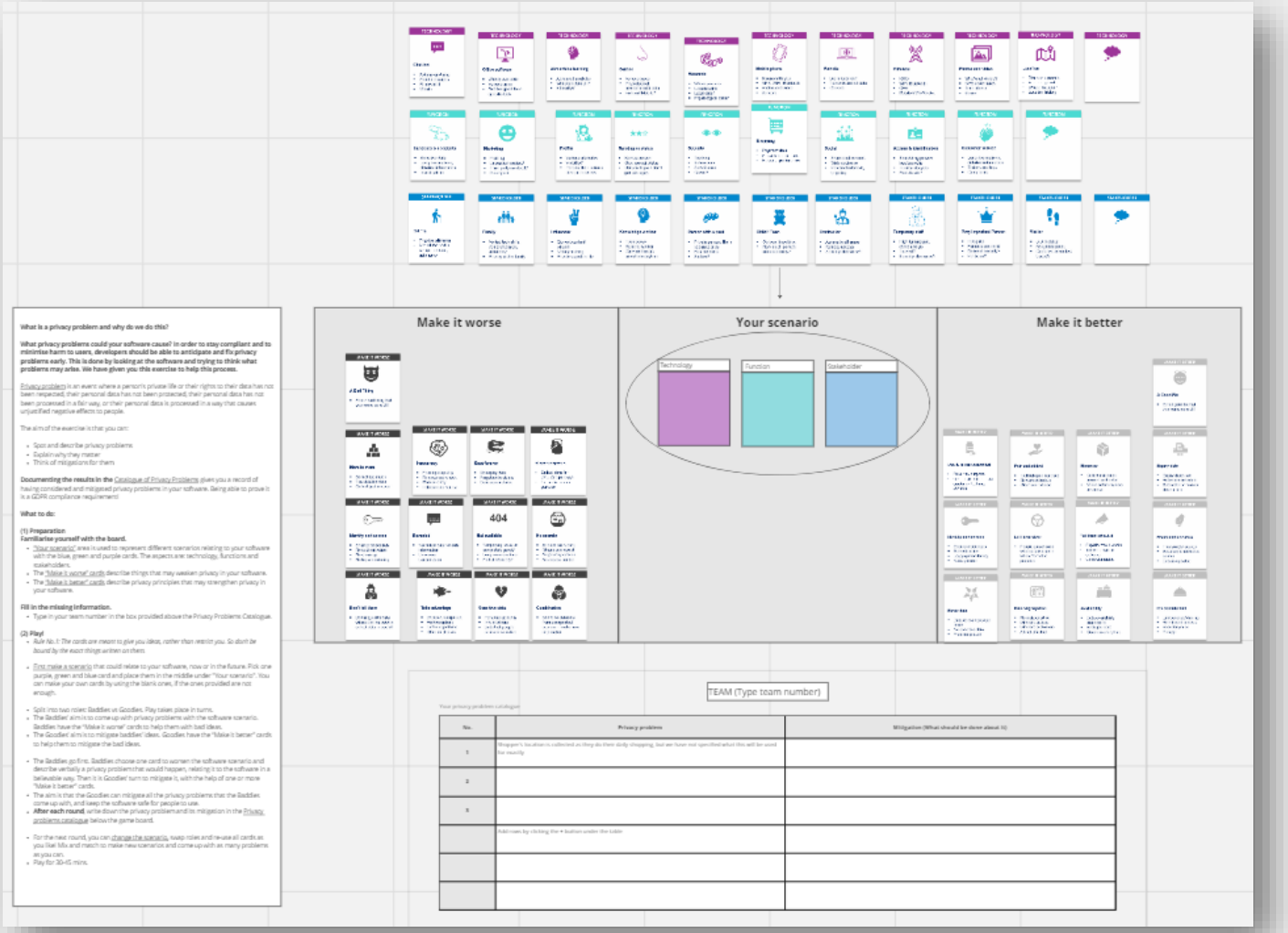
Course

- 5-week remote course
- 65 participants
- Varied programming confidence 0-10
- Varied relevant work experience 0-10+ yrs

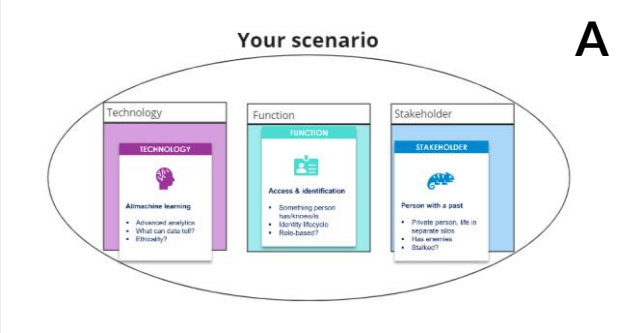
For the experiment

- 8 + 8 teams (3-5 participants each)
- Based on programming confidence, then work experience

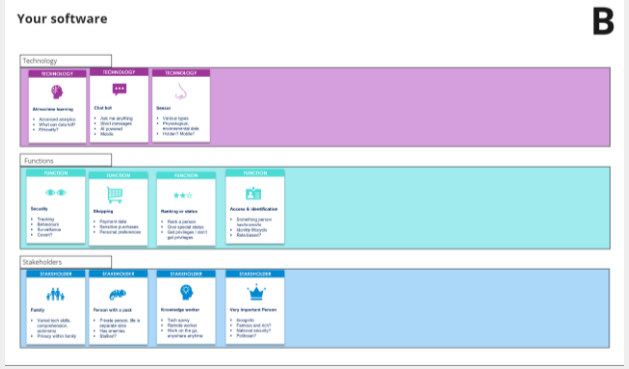




Experimental



Control



Results

Similarities

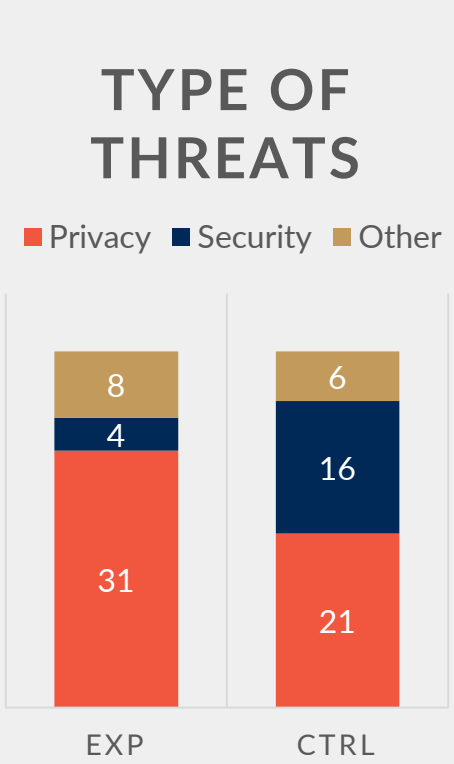
- 43 threats
- Timings
- Threats per group

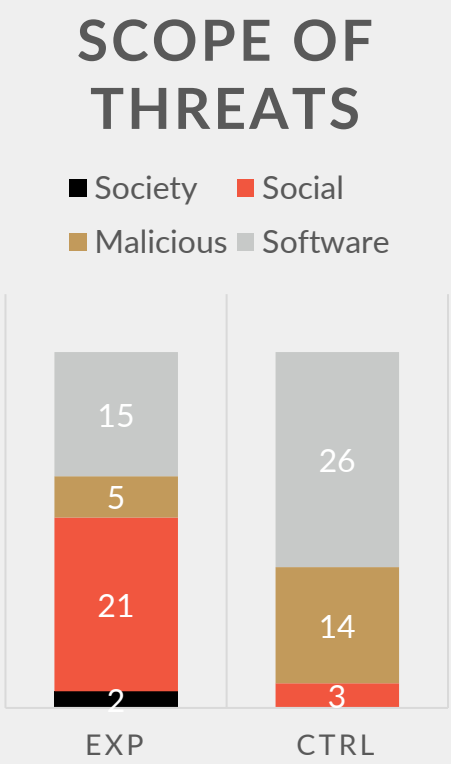
Experimental

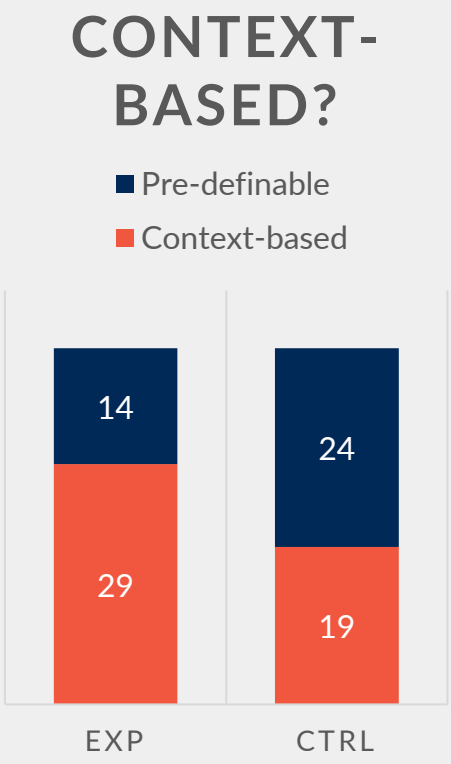
- Broader scope
- Social scope
- Context-based
- Personal harmed party

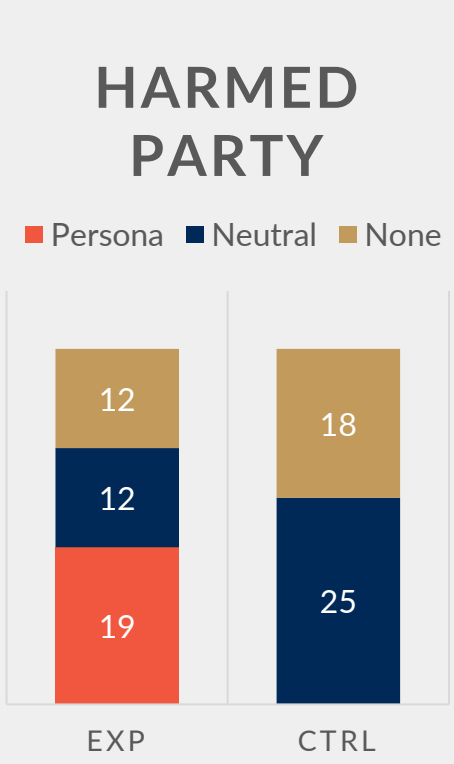
Control

- In line with existing research
- Security-focused
- Software artifact and malicious actors
- Non-personal harmed party









Same cards, but different results?

- Mixing and matching → wider scope, contextuality
- More material to consider → wider scope, contextuality but same quantity
- Scenarios before privacy principles → threats not pre-defined
- Personas → person's story, rather than privacy concepts

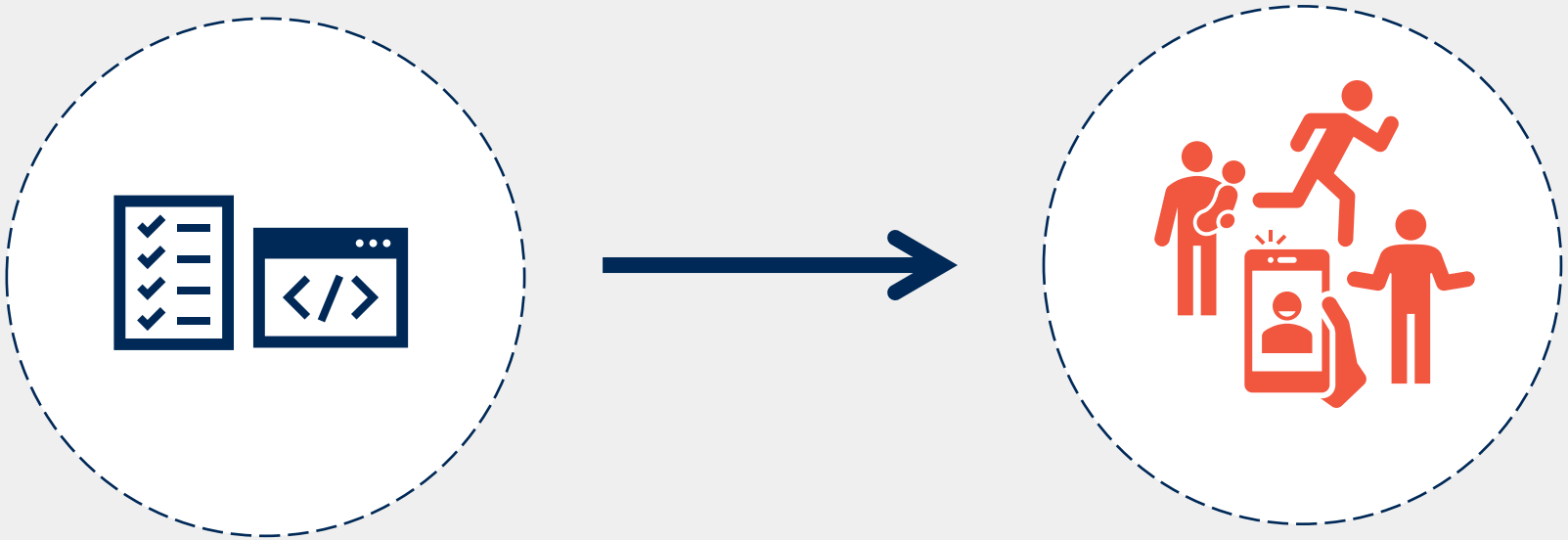
Validity

- Time and available threats
- Persona use challenges
- Participants and participation

- Presence of complexity and systems thinking?
- Control method realistic?
- Plausible threats?
- Generalised to industry?

Conclusion

- Attributing the results to a shift of focus
  - Artifact and privacy principles → **human interaction scenarios** with software
- **Systems thinking features** may improve the situation; a promising direction of research
- Applications: Inform the design of privacy threat modeling and privacy impact assessment methods for developers as well as privacy education



Future work

- Analysis of recordings
- Refining cards
- Refining user guidance
- Validation in the industry

TECHNOLOGY	FUNCTION	STAKEHOLDER	MAKE IT WORSE	MAKE IT BETTER
Location	**Ranking or status**	**Family**	**Inaccuracy**	**Let them steer**
▪ Static or dynamic ▪ Public or private ▪ Whose location? ▪ Location history	▪ Rank a person ▪ Give special status ▪ Get privileges / don't get privileges	▪ Varied tech skills, comprehension, autonomy ▪ Privacy within family	▪ Poor input quality ▪ No accuracy check ▪ Manual entry ▪ Indirect data source	▪ People can choose what data is used / when / for what purpose

Thank you

Privacy, security and ethics in software development

Tuisku Sarrala, University of Jyväskylä

tuisku.rad.sarrala@jyu.fi