



Elderly

- Physical
- Varied comp
- auto

TECHNOLOGY



Location

- Static or dynamic
- Public or private
- Whose location?
- Location

FUNCTION



Shopping

- Payment data
- Sensitive purchases
- Personal preferences



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@ju.fi





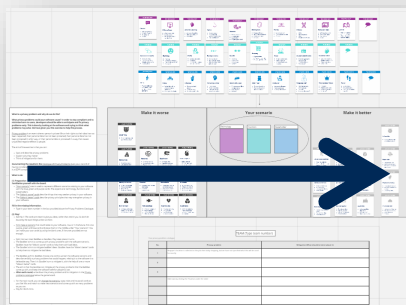
Tuisku Sarrala

- 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

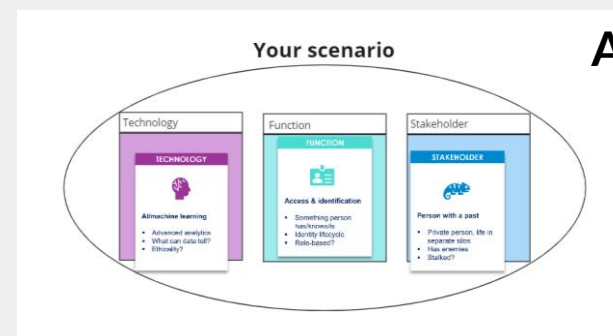
65





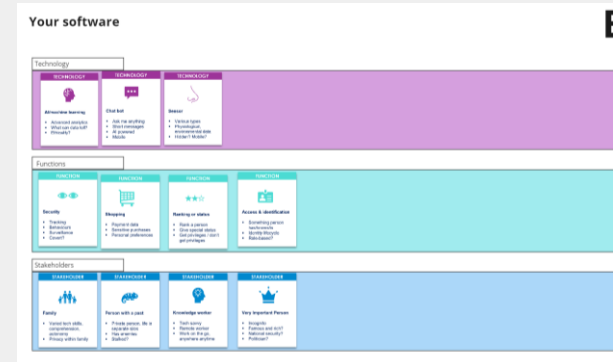
Experimental

A



Control

B



What is a privacy problem and why do we do this?

What privacy problems could your software cause? In order to stay compliant and to minimize harm to users, developers should be able to anticipate and fix privacy problems early. This is done by looking at the software and trying to think what problems may arise. We have given you this exercise to help this process.

Privacy problem is an event where a person's private life or their rights to their data has not been respected, their personal data has not been processed, their personal data has not been processed in a fair way, or their personal data is processed in a way that causes unjustified negative effects to people.

The aim of the exercise is that you can:

- Spot and describe privacy problems
- Explain why they matter
- Think of mitigations for them

Documenting the results in the Catalogue of Privacy Problems gives you a record of having considered and mitigated privacy problems in your software. Being able to prove it is a GDPR compliance requirement.

What to do:

(1) Preparation
Familiarize yourself with the board.

- The **Privacy Problem** area is used to represent different scenarios relating to your software with the blue, green and purple cards. The purple cards are technology, functions and stakeholders.
- The **Make it worse** cards describe things that may weaken privacy in your software.
- The **Make it better** cards describe privacy principles that may strengthen privacy in your software.

(2) In the middle information.

- Type in your team number in the box provided above the Privacy Problems Catalogue.

(3) Play!

- Roll No. 1: The cards are meant to give you ideas, rather than restrict you. So don't be bound by the exact things written on them.
- Roll No. 2: The cards are meant to give you ideas, rather than restrict you. So don't be bound by the exact things written on them.
- Roll No. 3: The cards are meant to give you ideas, rather than restrict you. So don't be bound by the exact things written on them.

Make it worse

Your scenario

Make it better

TEAM (Type team number)

No.	Privacy problems	Mitigation (What should be done about it?)
1	Person's location is collected as they do their daily shopping, but we have not specified what this will be used for exactly.	
2		
3		
	Add notes by clicking the + button under the table	



Results

Similarities

- 43 threats
- Timings
- Threats per group

Experimental

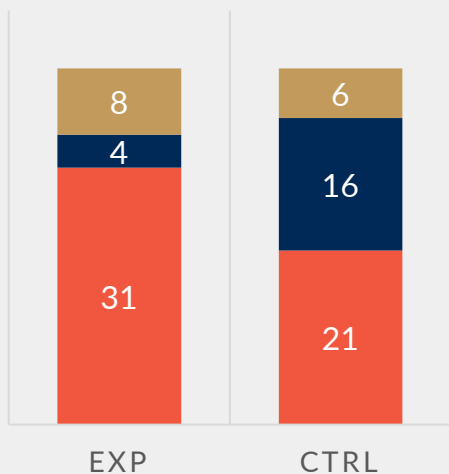
- Broader scope
- Social scope
- Context-based
- Personal harmed party

Control

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

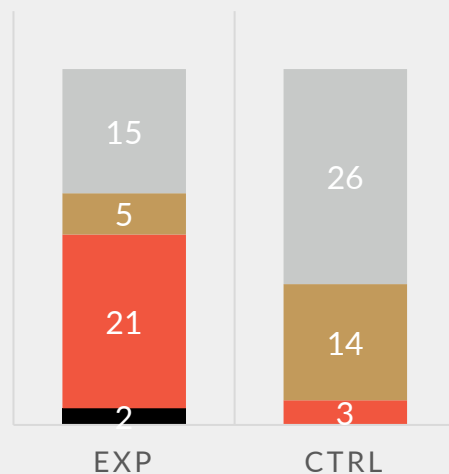
TYPE OF THREATS

Privacy Security Other



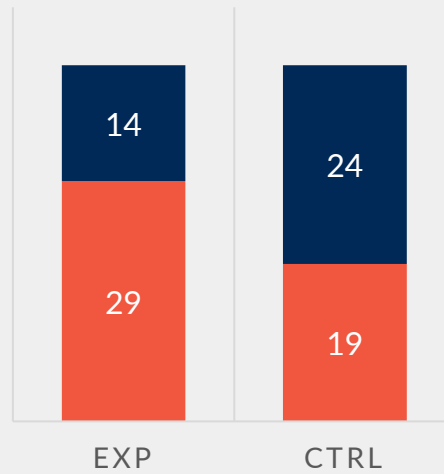
SCOPE OF THREATS

Society Social
Malicious Software



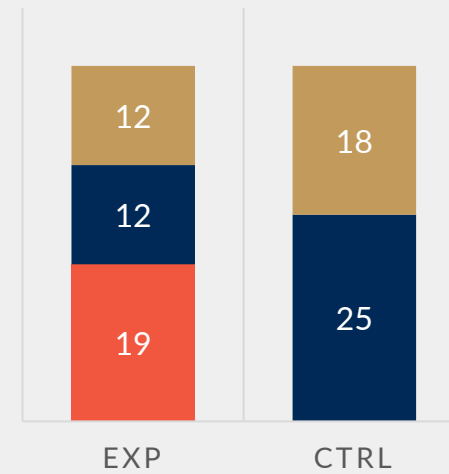
CONTEXT-BASED?

Pre-definable
Context-based



HARMED PARTY

Persona Neutral None





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



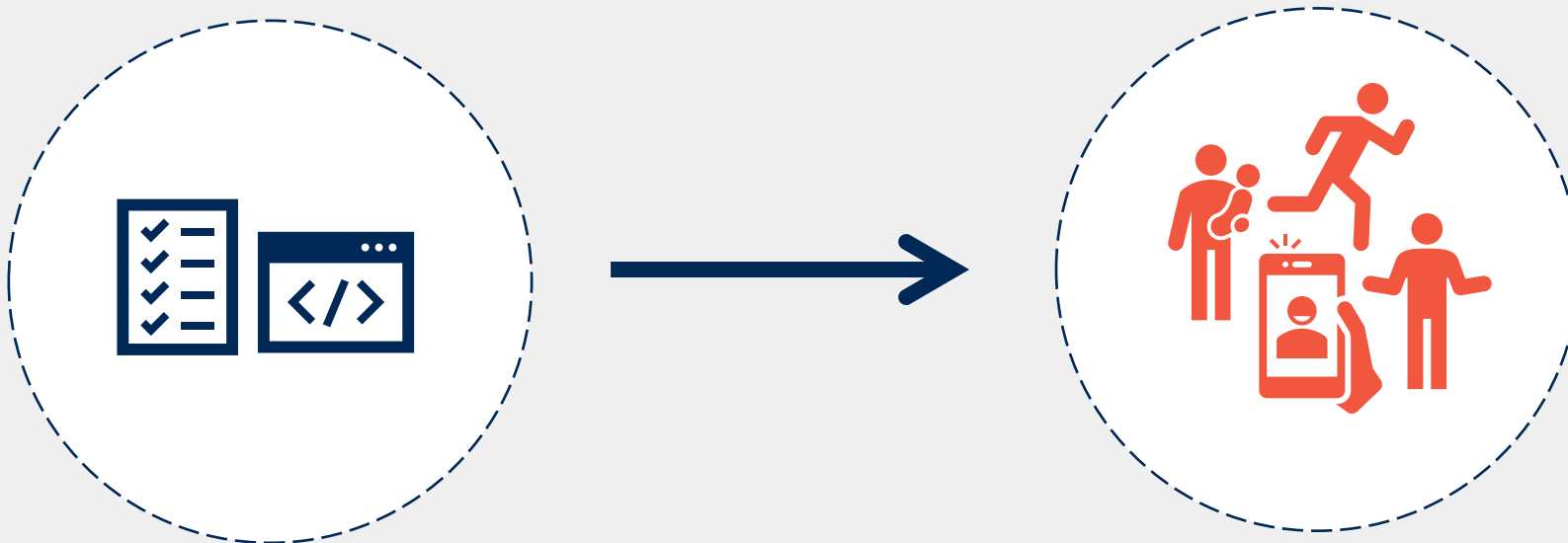
Validity

- 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





Thank you

TECHNOLOGY	FUNCTION	STAKEHOLDER	MAKE IT WORSE	MAKE IT BETTER
				
Location <ul style="list-style-type: none">▪ Static or dynamic▪ Public or private▪ Whose location?▪ Location history	Ranking or status <ul style="list-style-type: none">▪ Rank a person▪ Give special status▪ Get privileges / don't get privileges	Family <ul style="list-style-type: none">▪ Varied tech skills, comprehension, autonomy▪ Privacy within family	Inaccuracy <ul style="list-style-type: none">▪ Poor input quality▪ No accuracy check▪ Manual entry▪ Indirect data source	Let them steer <ul style="list-style-type: none">▪ People can choose what data is used / when / for what purpose



Privacy, security and ethics in software development

Tuisku Sarrala, University of Jyväskylä

tuisku.rad.sarrala@jyu.fi