University of the Aegean

Towards the Design of Usable Privacy by Design Methodologies

Argyri Pattakou, Aikaterini-Georgia Mavroeidi, Vasiliki Diamantopoulou, Christos Kalloniatis and Stefanos Gritzalis

Privacy Engineering and Social Informatics Lab.
Information and Communication Systems Security Lab.

August 2018
Banff, Canada

Department of Cultural Technology & Communication, University of the Aegean
Department of Information & Communication Systems Engineering, University of the Aegean

Overview

- Considering privacy as a part of a system's development process is widely accepted as an important aspect towards the development of privacy-aware systems
- A number of privacy requirements methodologies have been introduced in order to assist system designers and developers to analyse and elicit privacy requirements for different software systems and architectures
- It is important to ensure that privacy requirements engineering methods have been developed with the appropriate usability aspects in mind, in order to be applied in the intended and proper way
- However, to the best of our knowledge, usability criteria have never been considered as a way for assessing the usability of such methods
- This paper moves into this direction, by presenting well-known requirement engineering methods that deal with privacy and examines their usability against various usability criteria, identified in the respective literature

Usability

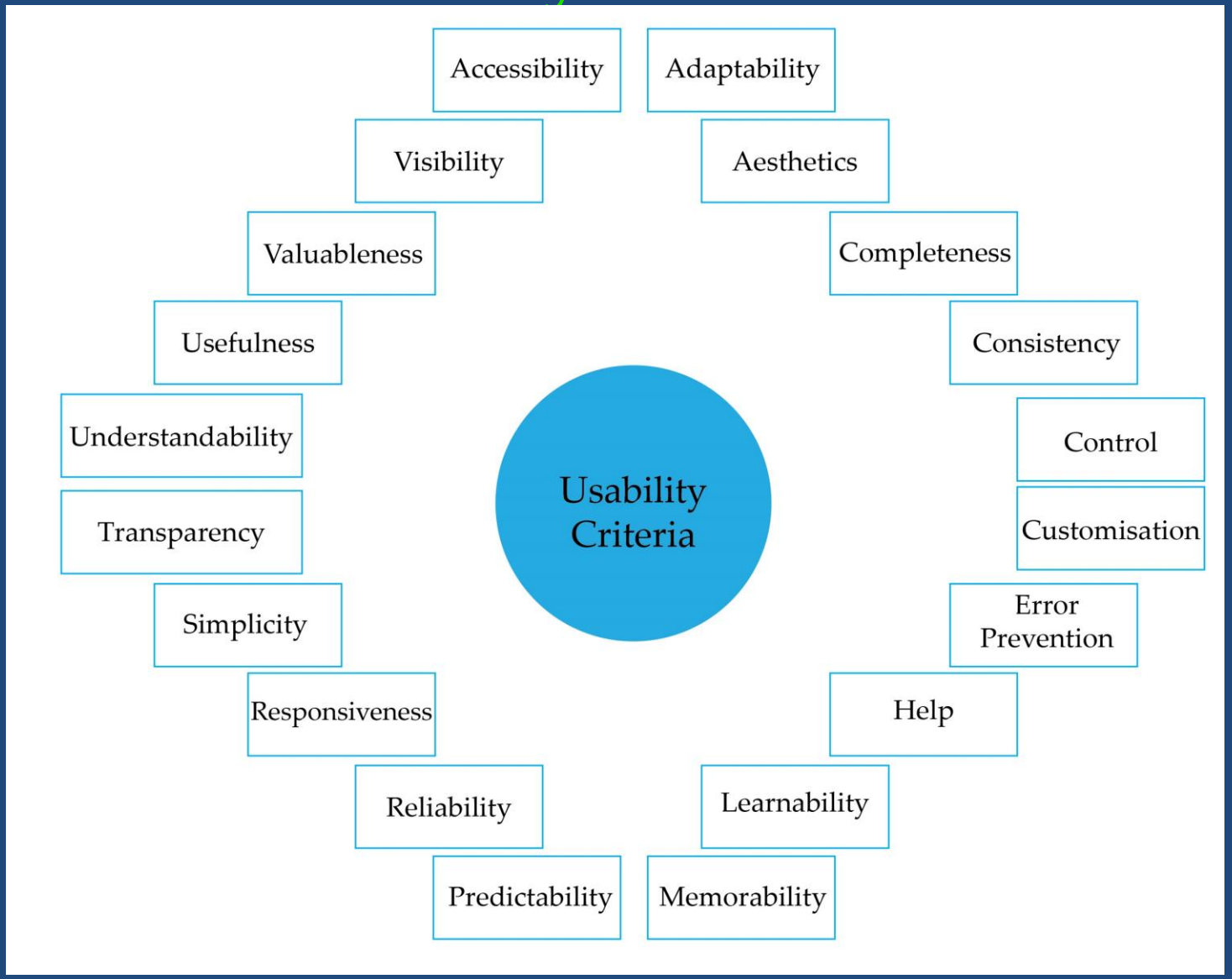
- ISO 9241-11

"the extent to which a product can be used by specified users to achieve specified goals with effectiveness, efficiency and satisfaction in a specified context of use"

- Literature records a number of usability criteria in a wide range of IT sectors, such as cloud computing and web services. Usability Criteria are used to examine on time the usability of a system/methodology into consideration

- We summarised the most common identified usability criteria that have been recorded in the literature

Usability Criteria



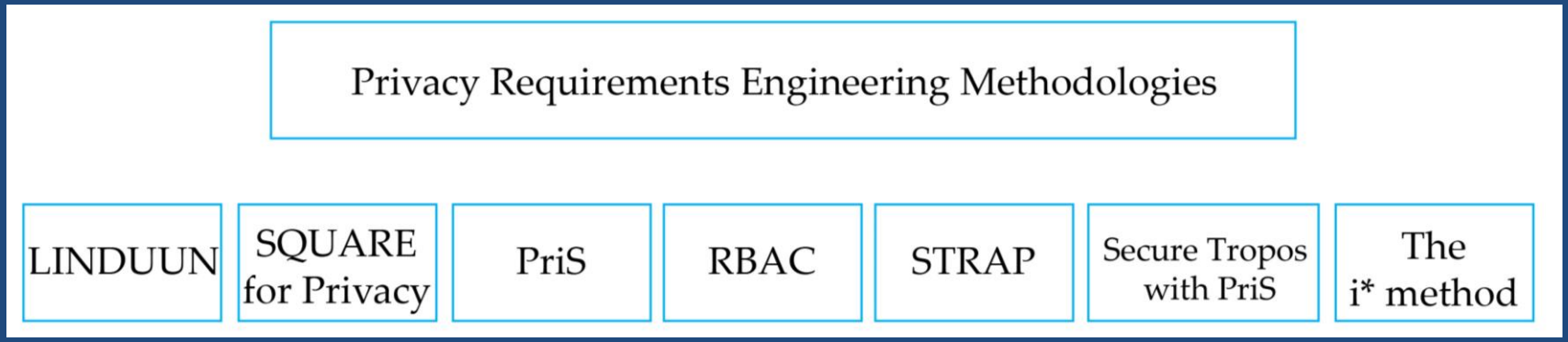
Privacy Requirements Engineering Methodologies

- Possible privacy attacks might cause costly and time-consuming processes
- Many researchers considered the need for examining privacy not as an ad-hoc process during implementation stage but as an integrated process during the system analysis and design level
- Due to a vast amount of privacy incidents and the user awareness about privacy protection, many requirements engineering methods were introduced, in order to support the elicitation and modeling of privacy requirements

Privacy Requirements Methods

- A number of these methods stay on a very abstract level while others include tool support for assisting engineering in accomplishing a holistic approach during system design
- Privacy requirements engineering methods have been built based on different approaches
- For instance: goal-oriented, risk-oriented or threat-oriented approaches, etc.

- Common Goal: support the fulfillment of privacy requirements in software-based systems



Parts of a Privacy Requirements Engineering Methodology

- Modelling Language (Graphical/Textual)
- Processes
- Tool

Table 1. Privacy Requirements Engineering Methodologies

Method	Methodology's part				
	Language		Processes	Tool	
	Graphical	Textual		Supported by tool	Formal Tool
LINDDUN	√		√		
SQUARE for Privacy			√	√	PRET
PriS		√	√	√	PriS Case tool
RBAC		√	√		
STRAP			√		
Secure Tropos with PriS	√		√		
i*	√		√	√	OME

USABILITY CRITERIA IN PRIVACY REQUIREMENTS METHODOLOGIES

Steps of our research 1/3

Step 1

Based on the definitions and the concept of the Usability Criteria, we identified which of them can be examined to each part of a privacy requirements engineering method

Table 2. Usability Criteria in the parts of a methodology

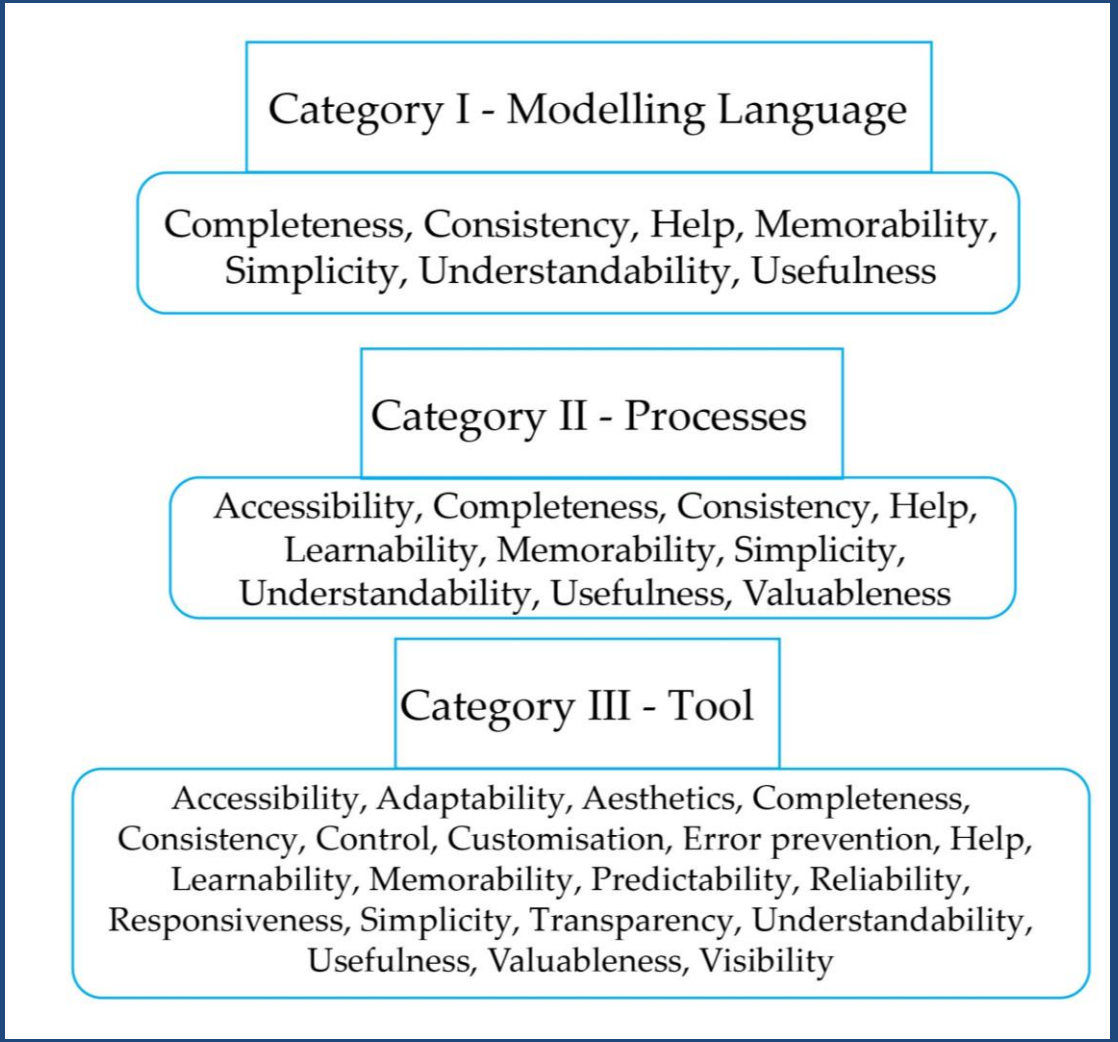
Usability Criteria	Parts of a methodology			
	Modelling Language		Processes	Tool
	Graphical	Textual		
Accessibility			X	X
Adaptability				X
Aesthetics				X
Completeness	X	X	X	X
Consistency	X	X	X	X
Control				X
Customisation				X
Error prevention				X
Help	X	X	X	X
Learnability			X	X
Memorability	X	X	X	X
Predictability				X
Reliability				X
Responsiveness				X
Simplicity	X	X	X	X
Transparency				X
Understandability	X	X	X	X
Usefulness	X	X	X	X
Valuableness			X	X
Visibility				X

Steps of our research 2/3

Step 2

Categorisation of the Usability Criteria, depending on the parts of a methodology.

This categorisation results from the Step 1



Steps of our research 3/3

Step 3

Depending on the parts that includes each PRM and the relevant categorisation of the usability criteria (Step 2), we identified the usability criteria that can be considered in each part of each PRM

M1=LINDDUN
M2=SQUARE for privacy
M3=PriS
M4=RBAC
M5=STRAP
M6=Secure Tropos + PriS
M7=i*
GL= Graphical Language
TL= Textual Language
P= Processes
T= Tool

Table 3. Matching Usability Criteria with Privacy Requirements Methodologies

Criterion	Privacy Requirements Methodologies						
	M1	M2	M3	M4	M5	M6	M7
Accessibility (II,III)	P	P, T	P, T	P	P	P	P, T
Adaptability (III)		T	T				T
Aesthetics (III)		T	T				T
Completeness (I, II, III)	GL, P	P, T	TL, P, T	TL, P	P	GL, P	GL, P, T
Consistency (I, II, III)	GL, P	P, T	TL, P, T	TL, P	P	GL, P	GL, P, T
Control (III)		T	T				T
Customisation (III)		T	T				T
Error prevention (III)		T	T				T
Help (I, II, III)	GL, P	P, T	TL, P, T	TL, P	P	GL, P	GL, P, T
Learnability (II, III)	P	P, T	P, T	P	P	P	P, T
Memorability (I, II, III)	GL, P	P, T	TL, P, T	P	P	GL, P	GL, P, T
Predictability (III)		T	T				T
Reliability (III)		T	T				T
Responsiveness (III)		T	T				T
Simplicity (I, II, III)	GL, P	P, T	TL, P, T	TL, P	P	GL, P	GL, P, T
Transparency (III)		T	T				T
Understandability (I, II, III)	GL, P	P, T	TL, P, T	TL, P	P	GL, P	GL, P, T
Usefulness (I, II, III)	GL, P	P, T	TL, P, T	TL, P	P	GL, P	GL, P, T
Valuableness (II, III)	P	P, T	P, T	P	P	P	P, T
Visibility (III)		T	T				T

Conclusions 1/2

- A number of privacy requirements methodologies have been introduced in order to support the development of privacy-aware systems
- It should be ensured that the PRM cover the appropriate usability aspects, as any methodology must be usable by software engineers in order to be applied successfully and to achieve its goals
- However, we observed that literature does not record any efforts to consider the usability of privacy requirements engineering methods

Conclusions 2/2

- The contribution of our work was to cover partly this gap by examining how usability can be combined with privacy requirements methods

- Namely, we identified which usability criteria can be examined in each part of the existing privacy requirements methodologies

Future Work

- This approach could be a pattern for a future evaluation of these privacy requirements methods regarding usability

- In addition, as security and privacy are two different concepts that should be examined in parallel during designing information systems in order to prevent possible privacy and security incidents, we believe that this work could be a first step not only for assessing usability in privacy requirements engineering methods but security requirements engineering methods as well

Contact Info

- Pattakou Argyri

a.pattakou@aegean.gr
http://privasi.aegean.gr

- Diamantopoulou Vasiliki

vdiamant@aegean.gr
http://www.icsd.aegean.gr

- Gritzalis Stefanos

sgritz@aegean.gr
http://www.icsd.aegean.gr

- Mavroeidi Katerina

kmav@aegean.gr
http://privasi.aegean.gr

- Kalloniatis Christos

chkallon@aegean.gr,
privasi@aegean.gr
https://kalloniatis.aegean.gr
http://privasi.aegean.gr

THANK YOU!