



Universidade
Federal de
Pernambuco

Modeling Language to Support Privacy Requirements

Mariana Peixoto and Carla Silva

{mmp2, ctlls}@cin.ufpe.br

Level: Doctoral

Year of Entry: March/2016

Conclusion Expectation: March/2020

03/2018

Outline

- Problem Characterization
- Background
- Related Works
- Research Goals
- SLR Preliminary Results

Problem Characterization

- Increase in software applications
- Digital data reveal large quantities of personal information [Van Der Syte and Maalej, 2014].
 - People may not be aware of when and for what purpose their personal information has been or will be collected, analyzed or transmitted [Omoronyia et al., 2013].
 - The exposure of such information in an unregulated way can threaten user privacy [Omoronyia et al., 2013].

Problem Characterization

- In the report created by Data Protection Working Party (2017), about data protection and privacy, there is a list of examples:
 - An organization offers fitness monitoring devices to its employees as a general gift.
 - The devices register heartbeats and sleeping patterns over time.

Problem Characterization

- In the report created by Data Protection Working Party (2017), about data protection and privacy, there is a list of examples:
 - A transport company equips all of its vehicles with a video camera inside the cabin which records sound and video.
 - The purpose of processing these data is to improve the driving skills of the employees.

Problem Characterization

- In the report created by Data Protection Working Party (2017), about data protection and privacy, there is a list of examples:
 - An employer deploys a Data Loss Prevention tool to monitor the outgoing e-mails automatically, for the purpose of preventing unauthorized transmission of proprietary data (e.g. customer's personal data), independently from whether such an action is unintentional or not.

Problem Characterization

Mobile Application Security Report 2016 (Hewlett Packard Enterprise, 2016)

- Between May and November 2015
- 36,000 applications in 27 categories: Android AND iOS
- Personal information such as contacts, calendar data and geolocation are widely accessed without need
 - 52,1% geolocation data
 - 11,5% contacts
 - 19,8% financial investments
 - 16,3% calendar data
 - 41,9% games
 - 61,7% tool related to advertising or data analysis

Problem Characterization

- The Hancock Health Hospital located in the United States, paid \$ 55,000 to regain access to medical records of patients [Greenfield, 2018].
 - Hackers blocked 1,400 files
 - The security flaw in the system also led to a break in the privacy of patient records.
- Strava, which records the distance, course and speed of your user during physical activities, has disclosed location information for its users [BBC, 2018].
 - Soldiers of the US in Syria and in Afghanistan
 - Military routine in Brazil

Problem Characterization

- **Privacy and Information Sharing: Scenarios** (*Pew Research Center, 2016)
 - **Office surveillance cameras:** Acceptable (54%); It depends (21%); Not acceptable (24%);
 - **Sharing health information:** Acceptable (52%); It depends (20%); Not acceptable (26%);
 - **Retail loyalty cards:** Acceptable (47%); It depends (20%); Not acceptable (32%);
 - **Smart thermostat:** Acceptable (27%); It depends (17%); Not acceptable (55%).

* <http://www.pewinternet.org/interactives/privacy-scenarios/>

Problem Characterization

- Privacy is a multifaceted concept, as well as it can often be vague and elusive. Comes in many forms, relating to what one wishes to keep private [Kalloniatis et al., 2008; Gharib et al., 2017]. This has resulted in much confusion among designers and stakeholders, and has led in turn to wrong design decisions [Gharib et al., 2017].
- Is necessary address the privacy issues since the early stages of development, ie the Requirements Engineering phase [Kalloniatis et al., 2008; Omoronyia et al., 2012; Tun et al., 2012].
- There is a need for systematic approaches for reasoning, modeling and analyzing privacy from the early stages of the software development [Webster et al., 2005].

Background

- Privacy is the right to determine when, how and what conditions it is permitted to disclose personal information and to transmit such information to third parties [Kalloniatis et al., 2008].
- According to Data Protection Working Party (2013)
 - Location;
 - Contacts;
 - Unique device and customer identifiers (such as IMEI13 and mobile phone number);
 - Identity of the data subject;
 - Credit card and payment data;
 - Phone call logs, SMS or instant messaging;
 - Browsing history;
 - Email;
 - Information society service authentication credentials (especially services with social features).

Background

- Modeling language are commonly used in requirements engineering [Sommerville, 2011]
- According Moody (2010) modeling languages use visual notations:
 - a. Effectively communicate with business stakeholders
 - b. Support design and problem solving by software engineers
- Visual notation:

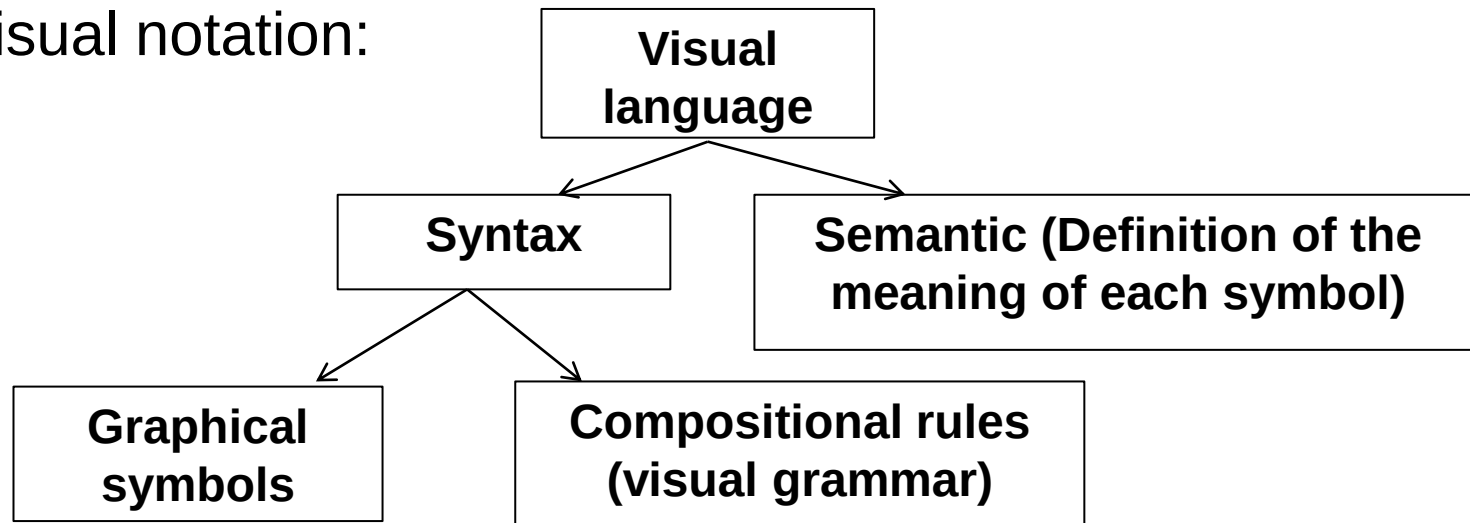


Fig 1. Anatomy of visual notation (Abd El-Ghafar, 2014).

- What makes a good visual notation?
 - Cognitive effectiveness: speed, ease and accuracy with which the human mind processes
 - Physics of Notations (PoN): consists of principles for developing cognitively effective visual notations [Moody, 2009].

Related Works

- Privacy as part of security [Kalloniatis, 2008].
 - NFR Framework, Tropos , KAOS, i*

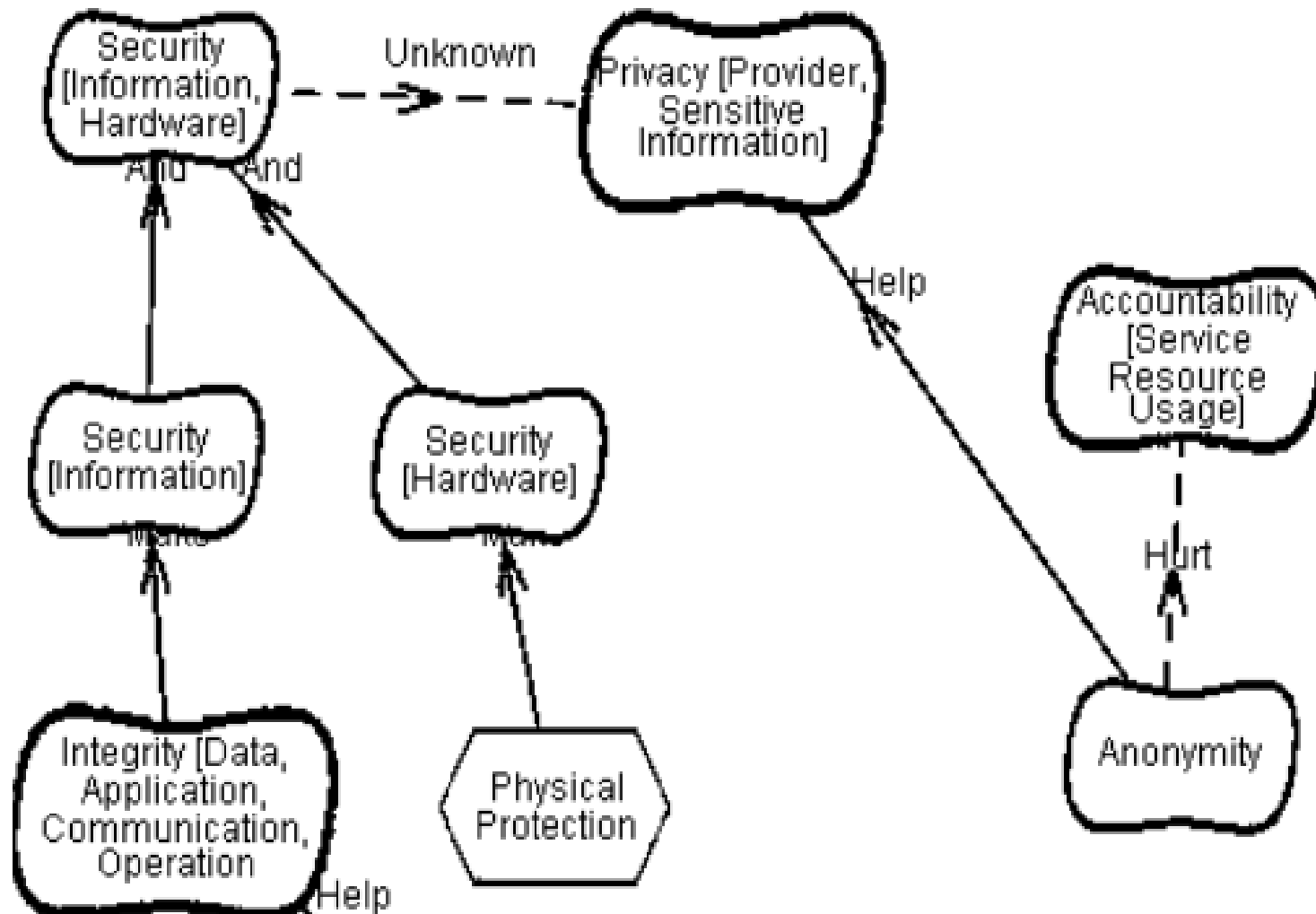


Fig 2. Catalogue of security-related requirements for P2P computing (Liu L, 2002)

Related Works

- Bijwe and Mead (2010) present the Privacy SQUARE method that adapts a security requirements engineering process to identifying privacy requirements
 - **Step 1 – Agree on Definitions** (list of terms)
 - **Step 2 – Identify Privacy Goals** (prioritized privacy goals)
 - **Step 3 – Collect Artifacts** (system architecture diagrams; use case scenarios and diagrams)
 - **Step 4 – Risk Assessment** (vulnerabilities and threats)
 - **Step 5 – Select Elicitation Technique** (structured/unstructured interviews use/misuse cases)
 - **Step 6 – Elicit Security Requirements**
 - **Step 7 – Categorize Requirements** (matrix)
 - **Step 8 – Prioritize Requirements** (Pair-Wise Comparison Method)
 - **Step 9 – Inspect Requirements** (Inspections remove defects and clear ambiguities in the requirements)

Related Works

- Deng et al. (2011) provide the LINDDUN Method (*Linkability, Identifiability, Non-repudiation, Detectability, Disclosure of information, Unawareness, Non-compliance*), which is based on a privacy threat analysis framework to elicit the privacy requirements of software and select privacy-enhancing technologies accordingly.

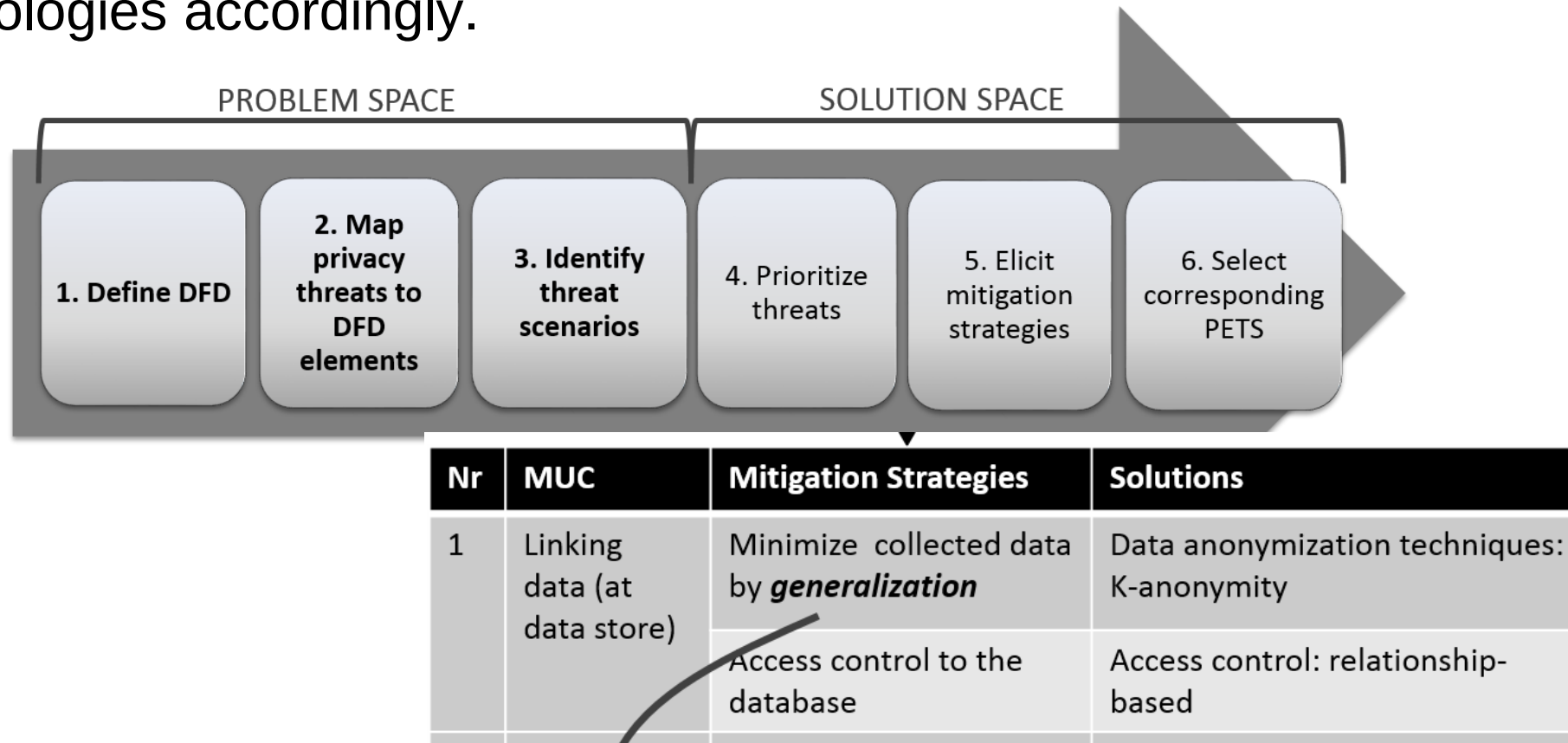


Fig 3. LINDDUN Method

Related Works

- PriS method focuses on bridging the gap between the design and the implementation phases [Kalloniatis, 2008].
 - Elicit privacy-related goals
 - Analyze the impact of privacy goals on organizational processes
 - Model using privacy-process patterns
 - Identify the technique(s) that best support/implement the above processes

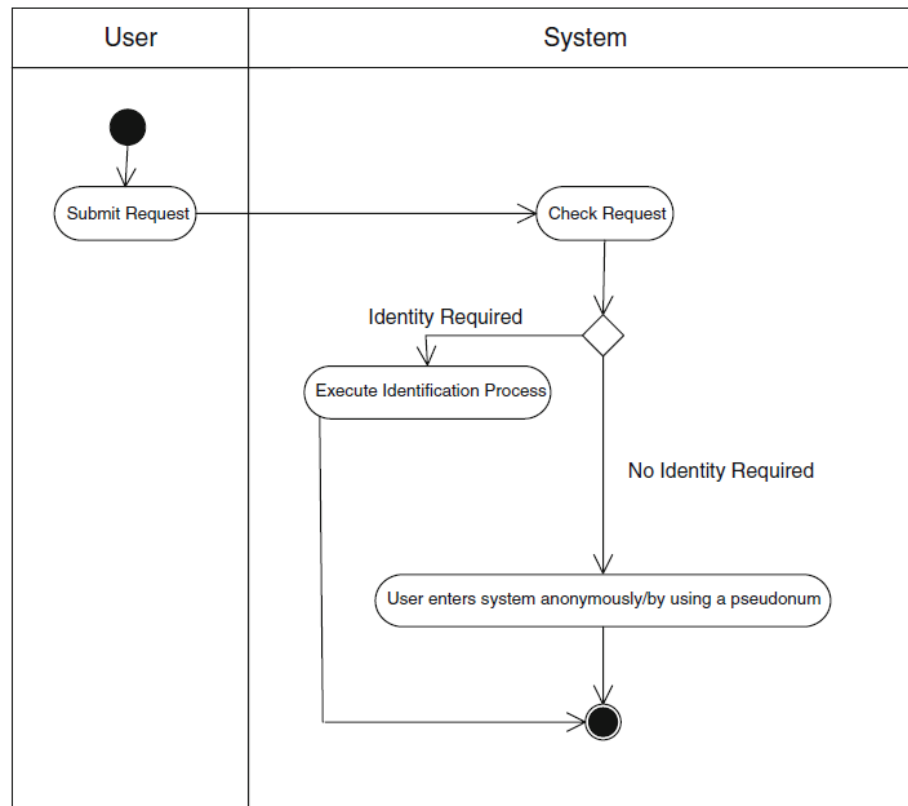


Fig 4. Anonymity and pseudonymity pattern

Related Works

- The STRAP framework [Hong, 2004].
 - In particular, at the beginning STRAP performs a goal-oriented analysis of the system for identifying the relevant actors, goals and major system components. Then a list of vulnerabilities is produced by asking a number of questions.
- Thomas et al. (2014) presents some privacy threats with associated harms
 - **Privacy Threat: Identification.**
 - **Example Harms:** Financial loss
 - **Privacy Threat: Exposure.**
 - **Example Harms:** Relationship breakdown, Discrimination

Related Works - Labda et al. (2014) - Modeling of privacy-aware business processes in bpmn

Privacy Requirement		Icon	Description	BPMN Mapping
Access Control	allow		Specify access control requirements on the resources it is attached to.	Pool, Lane
	Prevent			
	Limited			
Separation of Tasks			Separate the tasks of each role if more than one user is required to successfully complete the process	Lane, Pool, Data Object, and Activity
Binding of Tasks			Same user with different assigned roles needs to execute several tasks of a process	Lane, Pool, Data Object, and Activity
User Consent			Personal information and resources can only be accessed if the user consent is provided	Lane, Pool, Data Object, and Activity, sequence and message flow
Necessity to know	High		A user should only be able to access the information that is strictly necessary for completing a certain task	Lane, Pool, Data Object, Activity, sequence and message
	medium			
	low			

Fig 5. Privacy Requirements Description and annotations

Related Works - Webster et al. (2005) – Reusable Knowledge for Achieving Privacy

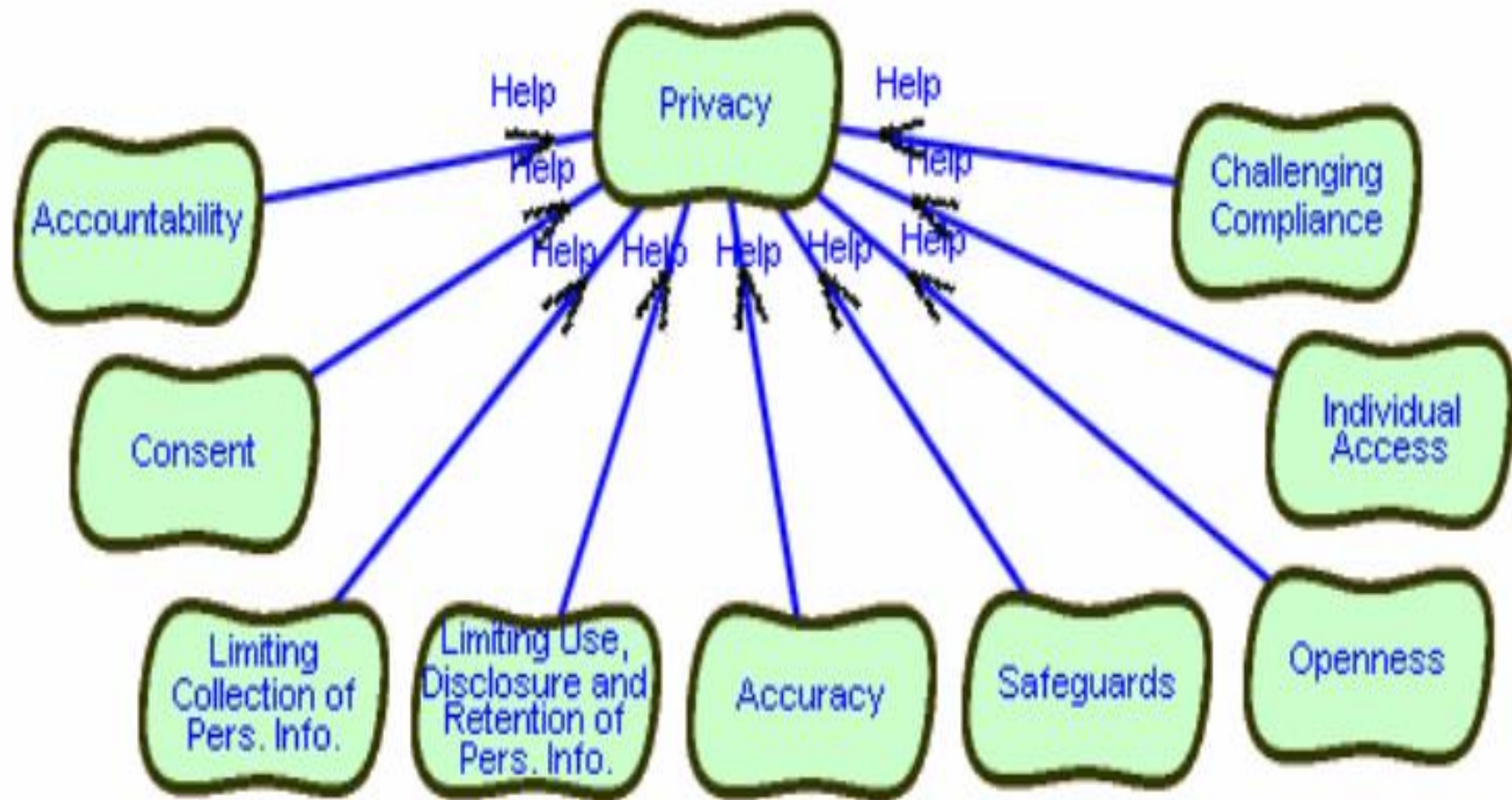


Fig 6: Privacy Catalogue

Related Works - Gharib et al. (2016) – Ontology for Privacy Requirements

Organizational		Agentive																			Intentional																			Informational																			Interaction																																																																																																																																																																																																																																																																																																																																																																																																																																																																							
		actor																			role																			agent																			user																			stakeholder																			person																			is_a																			plays																			goal																			objective																			task																			action																			refinement																			asset																			information																			data																			resource																			personal info																			sensitive info																			part_of																			own																			obj deleg.																			perm. deleg.																			info provision																			monitor																			obj trust																			perm trust																		
		actor																			role																			agent																			user																			stakeholder																			person																			is_a																			plays																			goal																			objective																			task																			action																			refinement																			asset																			information																			data																			resource																			personal info																			sensitive info																			part_of																			own																			obj deleg.																			perm. deleg.																			info provision																			monitor																			obj trust																			perm trust																		
		actor																			role																			agent																			user																			stakeholder																			person																			is_a																			plays																			goal																			objective																			task																			action																			refinement																			asset																			information																			data																			resource																			personal info																			sensitive info																			part_of																			own																			obj deleg.																			perm. deleg.																			info provision																			monitor																			obj trust																			perm trust																		
Risk		risk																			threat																			inten. threat																			casual threat																			vulnerability																			attack																			attacker																			attack method																			impact																			threaten																			exploit																																																																																																																																																																																																																																																																																																																																		
		risk																			threat																			inten. threat																			casual threat																			vulnerability																			attack																			attacker																			attack method																			impact																			threaten																			exploit																																																																																																																																																																																																																																																																																																																																		
		risk																			threat																			inten. threat																			casual threat																			vulnerability																			attack																			attacker																			attack method																			impact																			threaten																			exploit																																																																																																																																																																																																																																																																																																																																		
		risk																			threat																			inten. threat																			casual threat																			vulnerability																			attack																			attacker																			attack method																			impact																			threaten																			exploit																																																																																																																																																																																																																																																																																																																																		
Privacy		countermeasure																			mitigate																			control																			treatment																			s/p goal																			s/p constraint																			s/p policy																			s/p mechanism																			sec/priv req.																			confidentiality																			integrity																			availability																			non-repudiation																			notice																			anonymity																			transparency																			accountability																																																																																																																																																																																																																
		countermeasure																			mitigate																			control																			treatment																			s/p goal																			s/p constraint																			s/p policy																			s/p mechanism																			sec/priv req.																			confidentiality																			integrity																			availability																			non-repudiation																			notice																			anonymity																			transparency																			accountability																																																																																																																																																																																																																
		countermeasure																			mitigate																			control																			treatment																			s/p goal																			s/p constraint																			s/p policy																			s/p mechanism																			sec/priv req.																			confidentiality																			integrity																			availability																			non-repudiation																			notice																			anonymity																			transparency																			accountability																																																																																																																																																																																																																
		countermeasure																			mitigate																			control																			treatment																			s/p goal																			s/p constraint																			s/p policy																			s/p mechanism																			sec/priv req.																			confidentiality																			integrity																			availability																			non-repudiation																			notice																			anonymity																			transparency																			accountability																																																																																																																																																																																																																

Fig 7. Summary of the privacy related concepts and relations

Research Goals

Define modeling language for privacy requirements, with support for requirements analysis and adherence to PoN.

- Present the current state of the art of Requirements Engineering in relation to the modeling languages of privacy requirements;
- Present a modeling language for privacy requirements and their respective metamodel;
 - Present the analysis method
- Present the results of applying the language in scenarios that need privacy;
- Present the evaluation results of the modeling language by experts, and through a controlled experiment.

SLR Preliminary Results

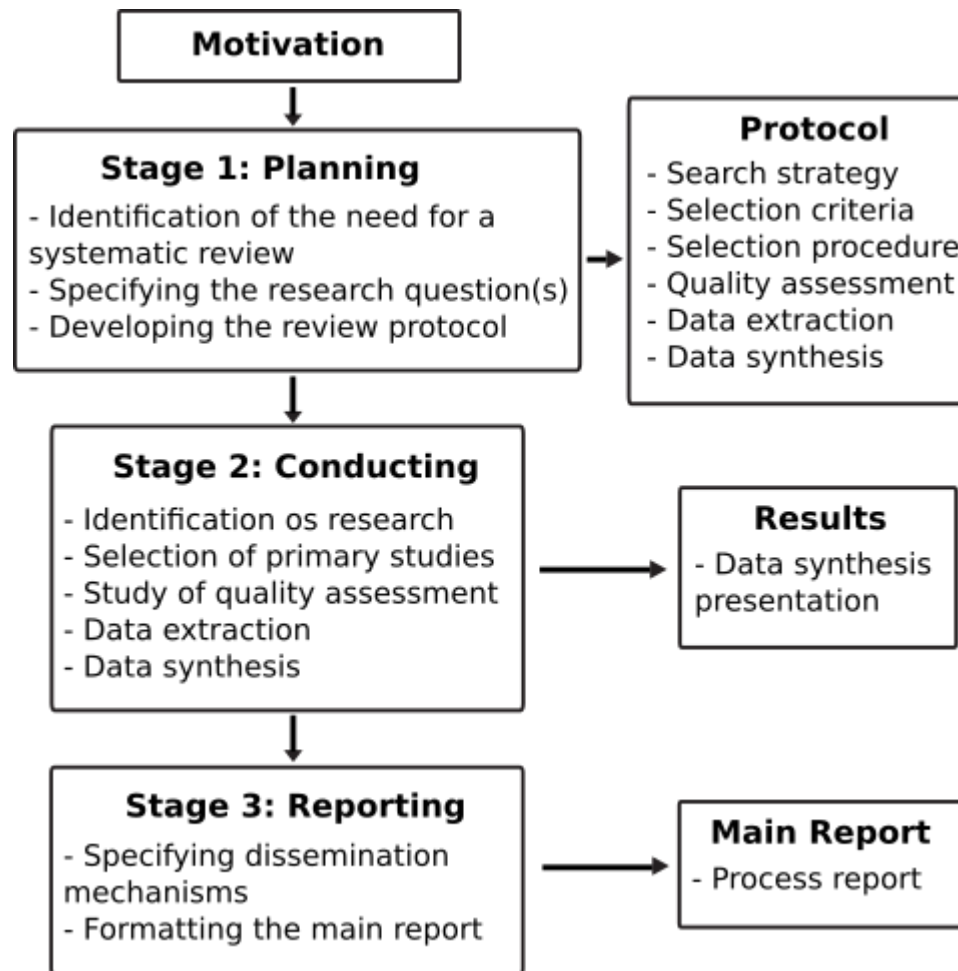


Fig 8. SLR Process adapted from Kitchenham and Charters (2007).

SLR Preliminary Results

- ***What are the modeling languages used to modeling and analysis of privacy requirements?***
 - SRQ1 - What modeling languages capture privacy concepts? Is it an extension of existing language? The language has tool support?
 - SRQ2 - What are the benefits and limitations reported in the use of the modeling languages?
 - SRQ3 - What are the privacy concepts captured by modeling languages?
 - SRQ4 - What are the modeling elements used to capture privacy concepts and their relationships?
 - SRQ5 – Do these languages support requirements analysis? What are the methods of analysis used?
 - SRQ6 - Are the modeling languages concerned with cognitive understanding aspects?

SLR Preliminary Results

Search Strategy: automatic search and snowball method

- Search String: (“privacy”) AND (“requirements engineering”) AND (“modeling” OR “modelling” OR “model” OR “language” OR “notation”)
- Search Engines:
 - IEEExplore
 - ACM Digital Library
 - Science Direct
 - Scopus
 - COMPENDEX

SLR Preliminary Results

Table 1. Selection Criteria.

Inclusion Criteria		Exclusion Criteria	
I1	Primary Studies	E1	Studies that are not focused on Requirements Engineering
I2	Peer-reviewed studies	E2	Duplicate studies (only one copy of each study was included)
I3	Studies that present some visual language	E3	Incomplete studies (short papers (≤ 3 pages))
I4	Available studies	E4	Presentations, reports, dissertations, theses, secondary studies, tertiary and meta-analysis).
I5	Original studies in languages: English, Portuguese or Spanish	E5	Studies that do not capture privacy concepts

SLR Preliminary Results

Selection Procedure

- Step 1: reading titles, abstracts and keywords; considering the inclusion and exclusion criteria.
- Step 2: reading introduction and conclusion; considering the inclusion and exclusion criteria.
- Step 3: the studies included are fully read; excluding irrelevant papers for the research questions.

SLR Preliminary Results

Table 2. Data Extraction.

#	Data	Description
1	Identifier (ID)	Unique identifier for each paper
2	Year, Affiliations, List of Authors, Title, Abstract and Keywords	
3	Source	IEEE, ACM, Scopus, Science Direct, Ei COMPENDEX
4	Application context	Industrial, academic, both
5	Study Type	Journal, conference, symposium, workshop, book chapter
6	Research Type (based on Wieringa et al., 2006)	Evaluation research, validation research, solution proposal, philosophical papers, experience papers, opinion papers
7	Evaluation Method (based on Easterbrook et al., 2008)	Controlled experiment, case study, survey, ethnography, action research, illustrative scenario, not applicable
8	Application Domain	Any domain. For example, Health Care
7	Research Questions	Answer to each research question

SLR Preliminary Results

Quality Assessment

- To verify the quality, the studies were classified according to Wieringa (2005):
 - Validation Research
 - Evaluation Research
 - Experience Papers
 - Opinion Papers
 - Philosophical Papers
 - Solution Proposal

Table 3. Quality Assessment

Quality Assessment						
Question	Eva	Val	Sol	Phi	Exp	Opi
QA1- Are the proposed concepts/relations clearly defined? (Gharib et al., 2017).	x	x	x	x	x	x
QA2- Does the work propose sufficient concepts/relations to deal with privacy aspects? (Gharib et al., 2017).	x	x	x	x	x	x
QA3- Is the problem clearly stated? (Wieringa, 2006).	x	x	x			
QA4- Is the research method clearly stated? (Wieringa, 2006).	x	x				
QA5- Is there an adequate description of the context? (Dyba and Dingsoyr, 2008).	x	x				
QA6- Was the data collected in a way that addressed the research issue? (Dyba and Dingsoyr, 2008).	x	x				
QA7- Was the data analysis sufficiently rigorous? (Dyba and Dingsoyr, 2008).	x	x				
QA8- Is there a clear statement of findings? (Dyba and Dingsoyr, 2008).	x	x				
QA9- Was there a control group with which to compare treatments? (Dyba and Dingsoyr, 2008).		x				
QA10- Is the technique novel, or is the application of the techniques to this kind of problem novel? (Wieringa, 2006).			x			
QA11- Is the technique argued? (Wieringa, 2006).			x			
QA12- Is the broader relevance of this novel technique argued? (Wieringa, 2006).			x			
QA13- Is there sufficient discussion of related work? (Wieringa, 2006).			x			
QA14- Is the conceptual framework original? (Wieringa, 2006).				x		
QA15- Is it argued? (Wieringa, 2006).				x		
QA16- Is the experience original? (Wieringa, 2006).					x	
QA17- Is the report about it sound? (Wieringa, 2006).					x	
QA18- Is the report relevant for practitioners? (Wieringa, 2006).					x	
QA19- Is the stated position argued? (Wieringa, 2006).						x
QA20- Is the opinion Innovating? (Wieringa, 2006).						x
QA21- Is it likely to provoke discussion? (Wieringa, 2006).						x

SLR Preliminary Results

Threats to validity

- This review was conducted by only one researcher and one advisor. To reduce the bias in this case, a structured data extraction approach was used, as indicated by Cruzes and Dyba (2011).
- The search string used for the automatic search may not include all the existing synonyms for the terms present in the expression "Modeling languages that support privacy requirements" and thus be insufficient to capture all area studies. To reduce this bias the snowball search was performed.

SLR Preliminary Results

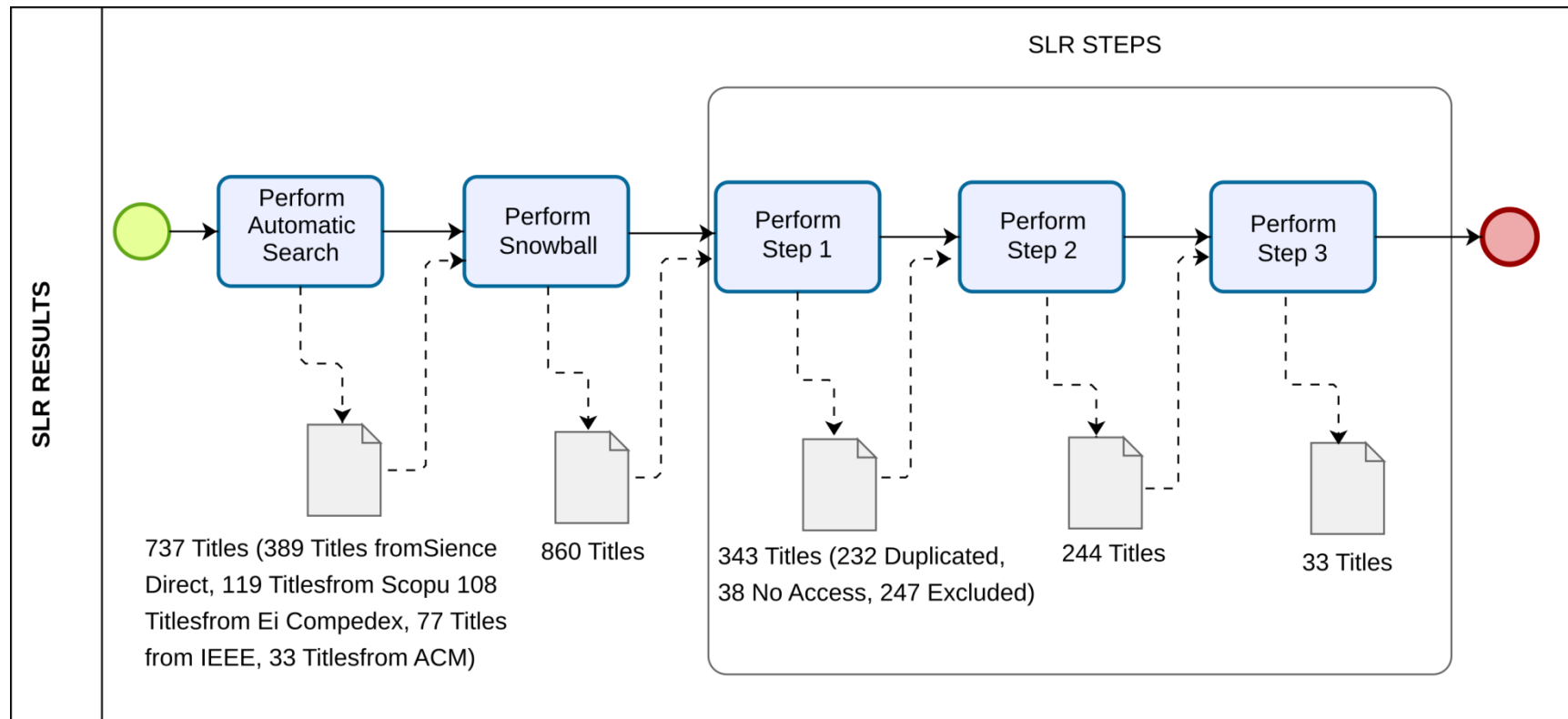


Fig 9. SLR Results.

SLR Preliminary Results

Table 4. Selected Papers

Id	Title	Authors
ACM7	Distilling Privacy Requirements for Mobile Applications	Thomas, K; Bandara, A. K.; Price, B.A.; Nuseibeh, B. (2014)
ACM8	Elaborating Security Requirements by Construction of Intentional Anti-Models	Lamsweerde, A.V. (2004)
ACM17	Legal Goal-oriented Requirement Language (Legal GRL) for Modeling Regulations	Ghanavati, S.; Amyot, D.; Rifaut, A. (2014)
COMPEDEX9	Designing privacy-aware personal health record systems	Samavi, R.; Topaloglou, T. (2008)
IEEE18	Compliance Analysis Based on a Goal-oriented Requirement Language Evaluation Methodology	Ghanavati, S.; Amyot D., Peyton, L. (2009)
IEEE30	Goal-oriented compliance with multiple regulations	Ghanavati, S.; Rifaut, A.; Dubois, E.; Amyot, D. (2014)
IEEE48	Requirements engineering patterns for the modeling of Online Social Networks features	Bouraga, S.; Jureta, I.; Faulkner, S. (2014)
...	...	...

SLR Preliminary Results

■ Overview Results

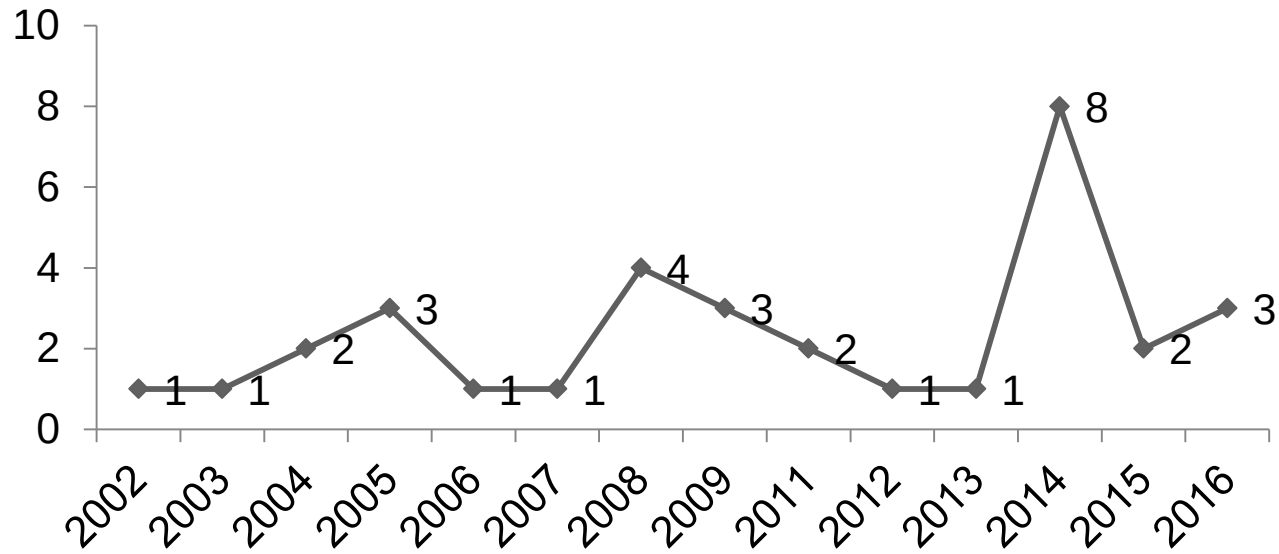


Fig. 10 Publication year.

SLR Preliminary Results

■ Overview Results

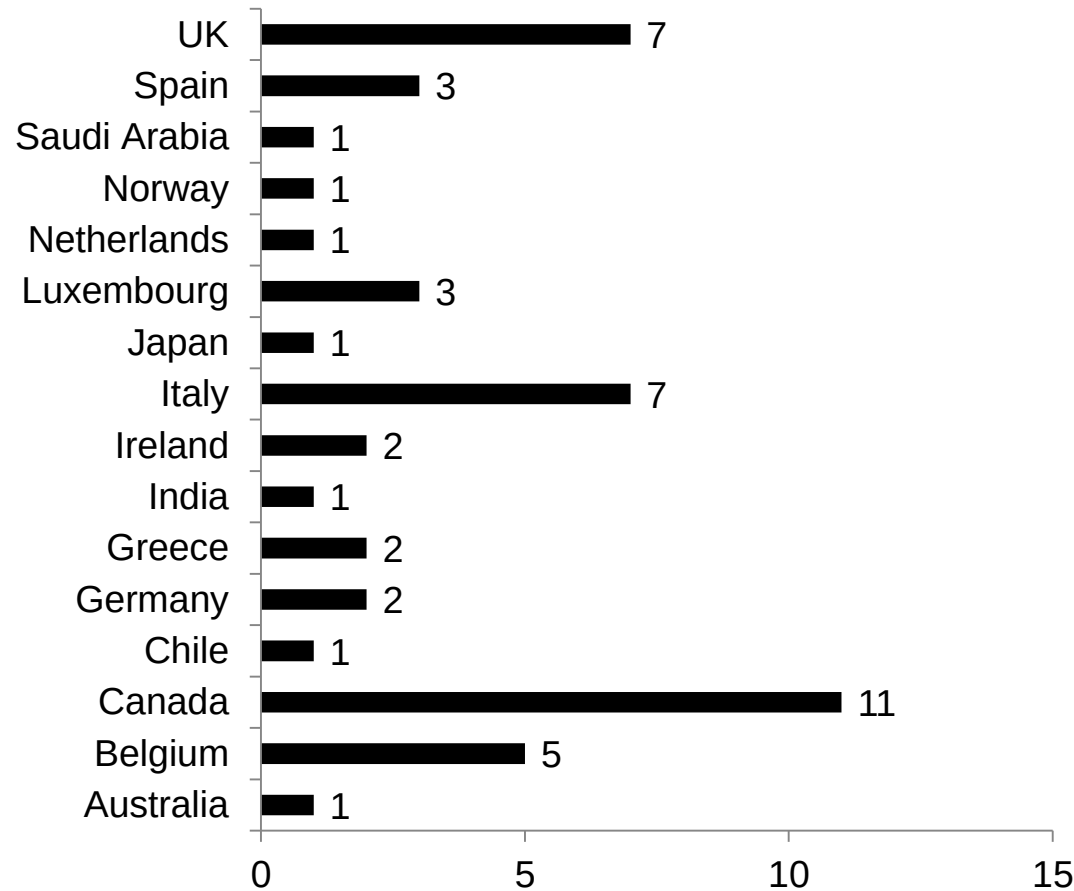


Fig. 11 Authors nationalities.

SLR Preliminary Results

■ Overview Results

Table 5. Paper type x context.

	Application Context		
Study Type	Academic	Academic/ Industrial	Total
Conference	13	0	13
Journal	7	2	9
Symposium	2	0	2
Workshop	9	0	9
Total	31 (93.9%)	2 (6.0%)	33 (100%)

SLR Preliminary Results

■ Overview Results

Table 6. Research type.

Research Type	f	%
Solution Proposal	29	87.9
Evaluation Research	3	9.1
Validation Research	1	3.0
Total	33	100.0

SLR Preliminary Results

■ Overview Results

Table 7. Evaluation method

Evaluation Method	Frequency	Percentage
Case study	6	18.2%
Controlled Experiment	1	3.0%
Illustrative Scenario	20	60.6%
Not Applicable	5	15.2%
Survey	1	3.0%
Total	33	100.0%

SLR Preliminary Results

■ Overview Results

Table 8 Application Domain

Application Domain	Frequency	Percentage
Cloud Computing Systems	2	6.1%
General	17	51.5%
Health Care	5	15.2%
Legal Regulations	5	15.2%
Mobile Applications	2	6.1%
Online Social Networks	1	3.0%
Socio-Technical Systems	1	3.0%
Total	33	100.0%

SLR Preliminary Results

What modeling languages capture privacy concepts? Is it an extension of existing language? The language has tool support?

Table 9. Languages used for privacy.

Language	Frequency	Percentage
UML4PF	1	2.4%
BPMN	1	2.4%
Data Flow Diagrams	1	2.4%
Goal Modeling	2	4.9%
GRL	2	4.9%
i-Star	7	17.1%
KAOS	1	2.4%
Legal GRL	2	4.9%
Misuse Cases	3	7.3%
NFR Framework	3	7.3%
Problem Frames	1	2.4%
Secure Tropos	5	12.2%
SI* modelling	1	2.4%
STS-ml (Socio-Technical Security modelling language)	2	4.9%
Threat Model	1	2.4%
Threat Tree	1	2.4%
Tropos	3	7.3%
UML	2	4.9%
Use Case Maps	2	4.9%
Total	41	100,0%

SLR Preliminary Results

What modeling languages capture privacy concepts? Is it an extension of existing language? The language has tool support?

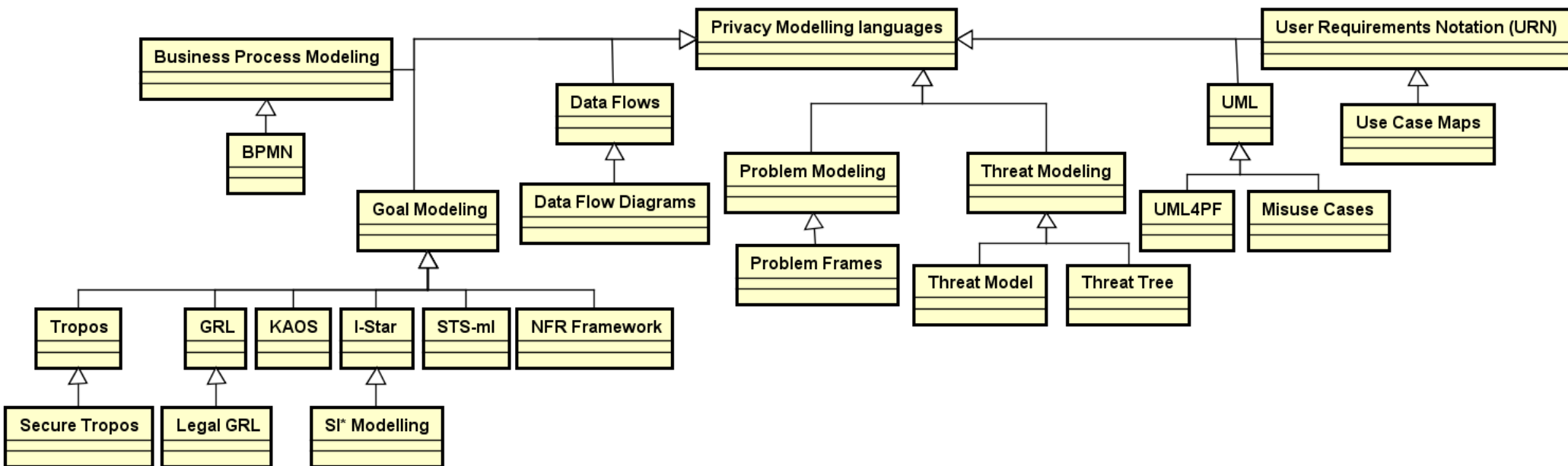


Fig 12. Taxonomy of privacy modeling languages.

SLR Preliminary Results

What modeling languages capture privacy concepts? Is it an extension of existing language? The language has tool support?

- 24 (72.7%) studies used an existing language;
- 9 (27.3%) studies proposed an extension of an existing language;
- It was not possible to observe the proposal of no new language.

SLR Preliminary Results

What modeling languages capture privacy concepts? Is it an extension of existing language? The language has tool support?

- UML4PF is an extension of UML to support Personal Information.
- BPMN is used to support Personal Information, Consent and Autonomy.
- GRL is used to support Personal Information, Consent, Collect, Disclosure, Use and Assurance.
- UML is used to support Personal Information, Awareness, Consent, Obligation, Non Repudiation, Disclosure, Access Control, Confidentiality, Integrity, Anonymity, Authorization and Harms.

SLR Preliminary Results

What modeling languages capture privacy concepts? Is it an extension of existing language? The language has tool support?

Table 10. Paper Whose has Tool Support.

ID	Tool Name
ACM7	OpenArgue
ACM17/ IEEE18/ IEEE30/ SCOPUS6	jUCMNav
IEEE58	UML profile
SCOPUS20	CREE-tool
SCIENCE27	Tool developed using the Open Models Initiative Platform
SNOW22	Pris-Tool
SNOW114/ SNOW122	STS-Tool
SNOW116	Oryx-editor BPMN tool

SLR Preliminary Results

What are the privacy concepts captured by modeling languages?

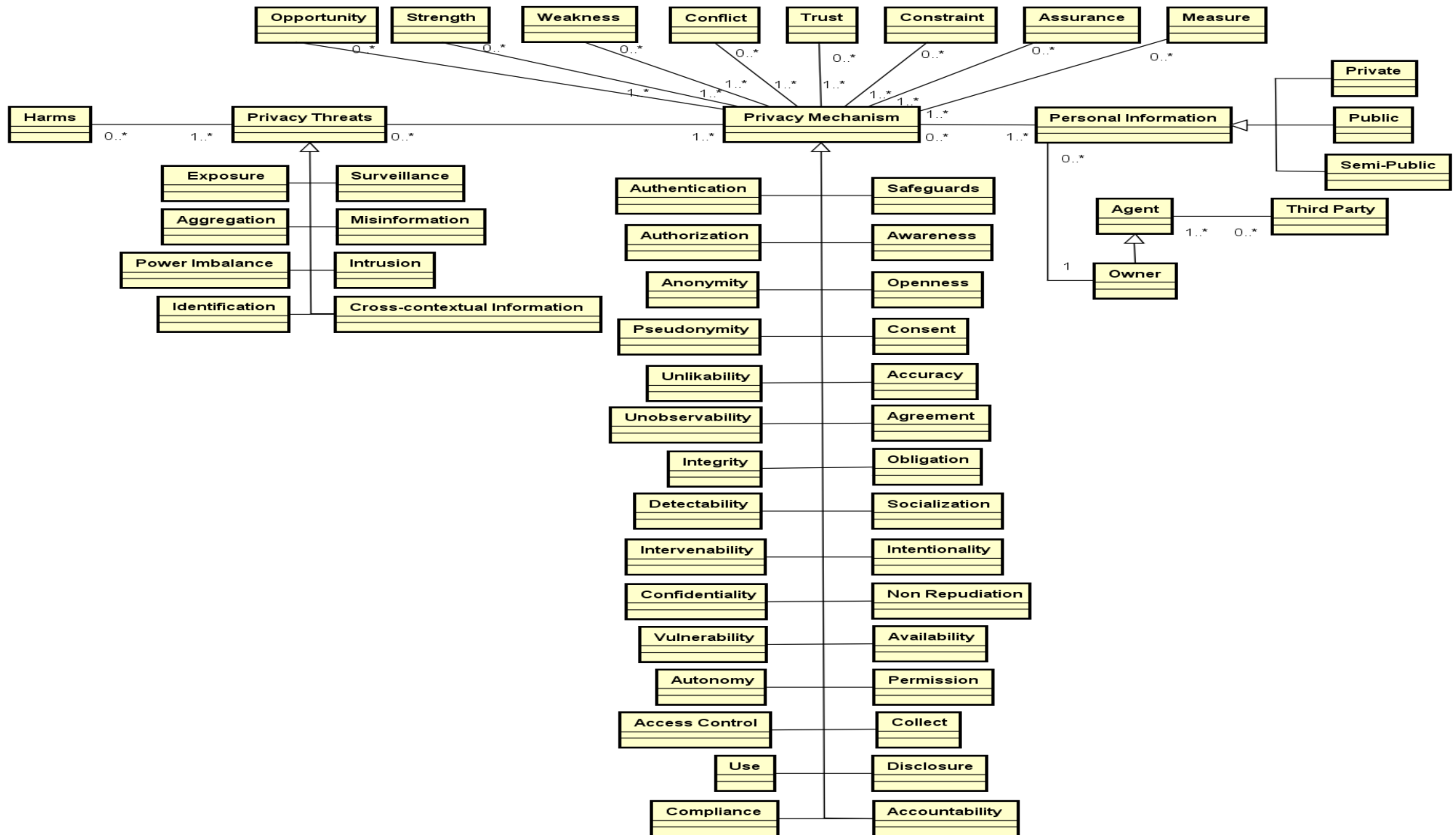


Fig 13. Privacy conceptual model.

SLR Preliminary Results

What are the modeling elements used to capture privacy concepts and their relationships?

Table 11. Modeling elements and relationships.

Concept	<Element; Relationships (ID)>
Private	<Resource; Dependency (IEEE48)>
Public	<Resource; Dependency (IEEE48)>
Semi-Public	<Resource; Dependency (IEEE48)>
Owner	Owner; Dependency (SNOW122)
Third Party	<Goal; Decomposition link (ACM17)>
Personal Information	<Resource; Dependency (COMPEDEX9/IEEE48/SNOW123), part of (SCOPUS31), Trust relation, Owner relation, Permission relation (SCOPUS30)>, <Goal; Contribution Link (IEEE18/SNOW7), Goal decomposition (SNOW46), Dependency (SCIENCE323/SCIENCE332)>, <Softgoal; Decomposition Link (IEEE30), Strategic Dependencies (IEEE53), Association (SCIENCE40)>, < Stereotype; Extension (IEEE58)>, <Document; Contribution link SNOW122)>

SLR Preliminary Results

What are the modeling elements used to capture privacy concepts and their relationships?

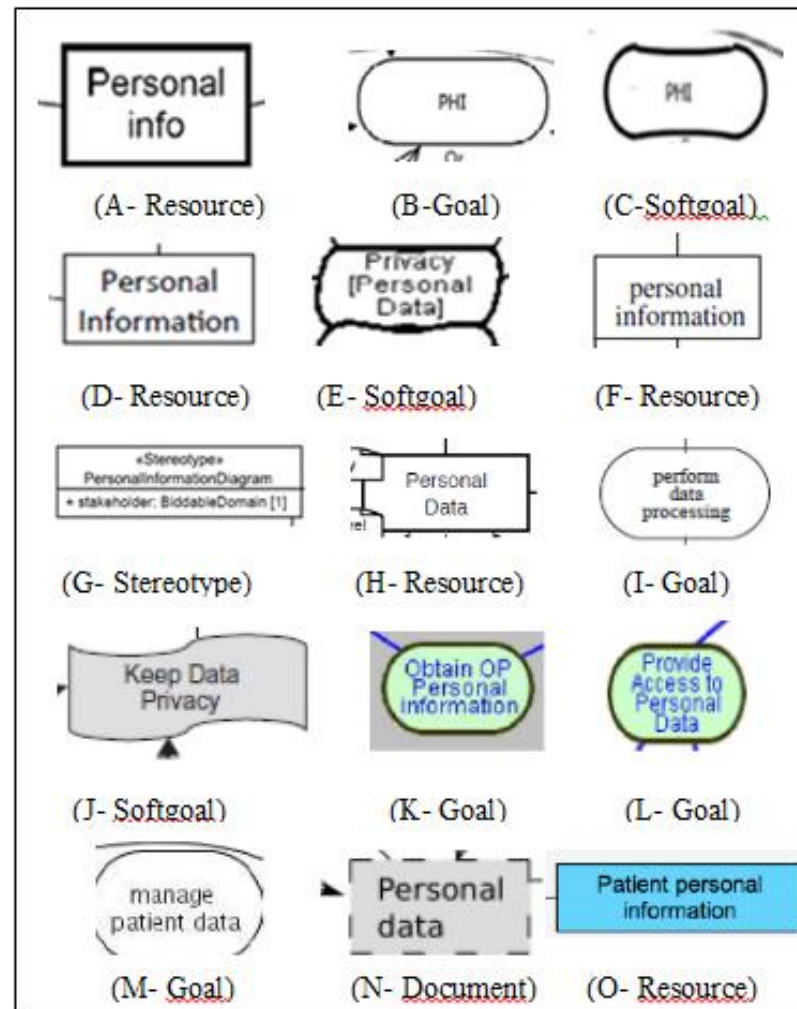


Fig 14. Modeling Elements .

SLR Preliminary Results

Do these languages support requirements analysis? What are the methods of analysis used?

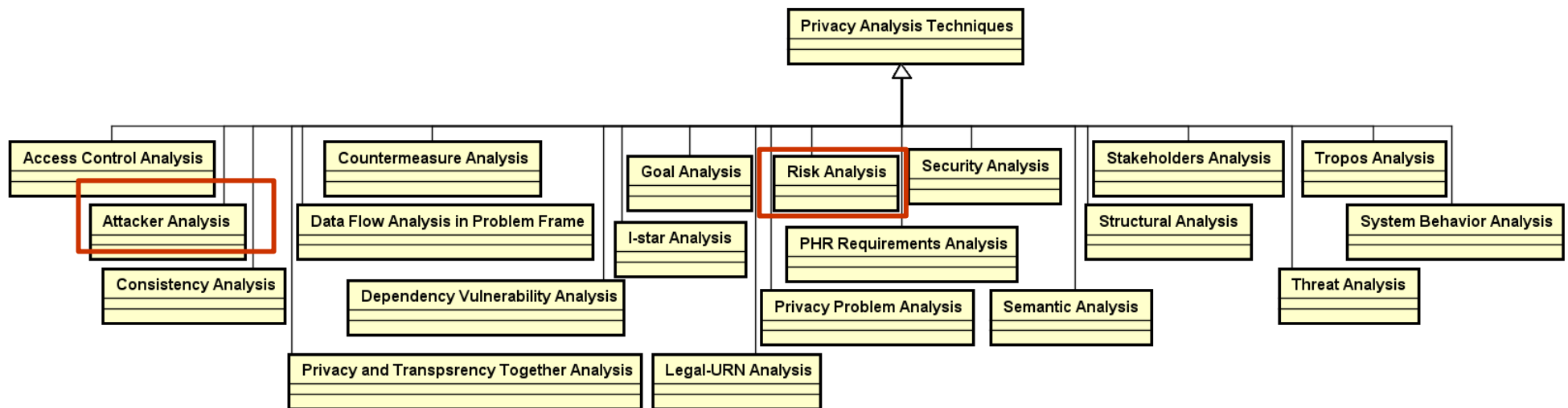


Fig 15. Requirements Analysis Methods.

SLR Preliminary Results

Do these languages support requirements analysis? What are the methods of analysis used?

Table 12. Requirements Analysis Techniques X Suported Concept

ID	Requirements Analysis Techniques	Suported Concept
SNOW115	Privacy and Transparency Together Analysis: Aims to analyze how privacy would impact Transparency and vice versa.	Third Party, Personal Information, Privacy Mechanism, Awareness, Socialization, Collect, Use, Anonymity and Trust
IEEE53/ SNOW123	Attacker Analysis: Aims to identify potential system abusers and their malicious intents	Personal Information, Privacy Mechanism, Awareness, Consent, Collect, Disclosure, Access Control, Confidentiality, Authorization, Authentication, Trust, Constraint, Assurance and Privacy Threats
SNOW122	Consistency Analysis: Aims to verify whether the diagram built by the designer is consistent and valid.	Owner, Personal Information, Availability, Confidentiality, Integrity, Authorization and Privacy Threats
IEEE53	Countermeasure Analysis: System designers make decisions on how to protect security and privacy from potential attackers and vulnerabilities	Personal Information, Awareness, Disclosure, Access Control, Confidentiality, Authorization, Trust and Privacy Threats
IEEE58	Data Flow Analysis in Problem Frames: Aims to analyze how the identified personal data of each stakeholder is propagated through the system.	Personal Information

SLR Preliminary Results

Are the modeling languages concerned with cognitive understanding aspects?

- no study

SLR Preliminary Results - Quality Assessment

- Evaluation research: 3 papers (80, 40 and 60 quality) from a maximum of 80;
- Validation research: 1 paper (75 quality) from a maximum of 90;
- Solution proposal: 29 papers just one received maximum score, quality 70.



Universidade
Federal de
Pernambuco

Modeling Language to Support Privacy Requirements

Mariana Peixoto and Carla Silva

{mmp2, ctlls}@cin.ufpe.br

Level: Doctoral

Year of Entry: March/2016

Conclusion Expectation: March/2020

03/2018