Privacy Engineering:

Towards a definition

Gap between research and practice

Privacy (research)

- Theories
- Paradigms
- Frameworks
- Threats and risks
- Technologies

Privacy by Design

(Software) engineering

- Development process
- Business domain
- System type

Privacy Engineering

Privacy Engineering

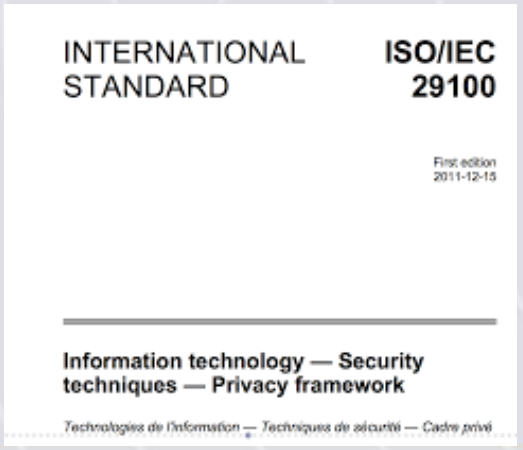
Field of research and practice
that designs, implements, adapts, and evaluates
theories, methods, techniques, and tools
to systematically capture and address privacy issues
when developing information systems

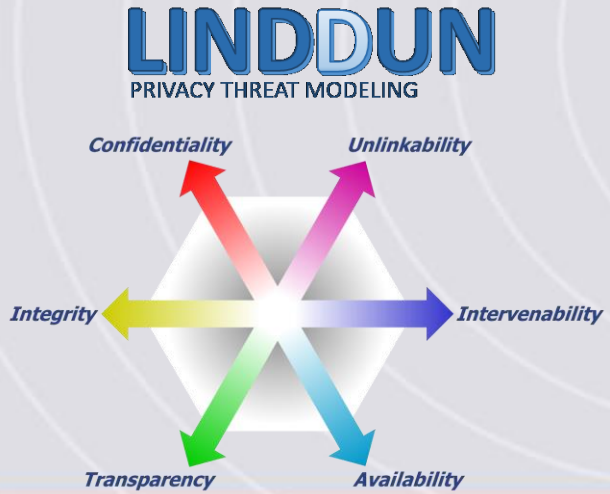
Seda Gürses & Jose M. del Alamo
Privacy Engineering: Shaping an Emerging Field of Research and Practice
IEEE Security and Privacy 14:2, pp. 40-46, 2016.

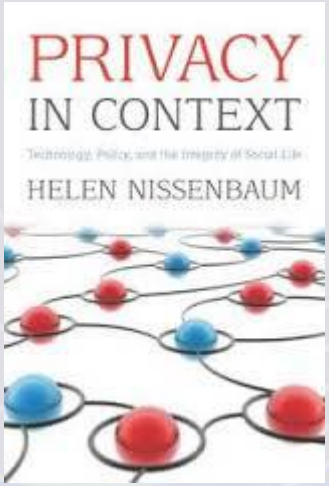
Privacy Engineering

Field of research and practice
that designs, implements, adapts, and evaluates
theories, methods, techniques, and tools
to systematically capture and address privacy issues
when developing information systems

Theory: Privacy conceptualization



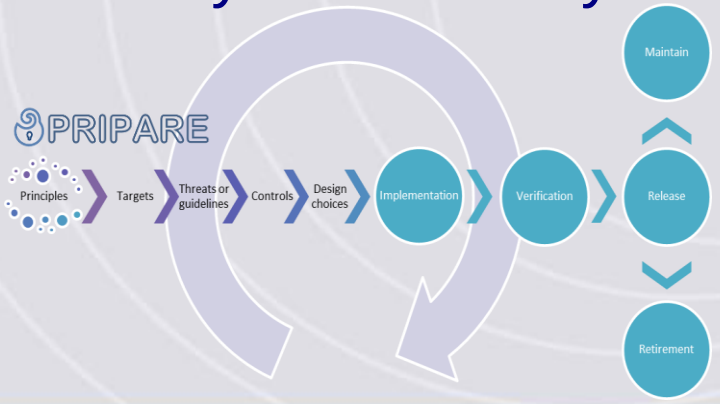




Privacy Engineering

Field of research and practice
that designs, implements, adapts, and evaluates
theories, methods, techniques, and tools
to systematically capture and address privacy issues
when developing information systems

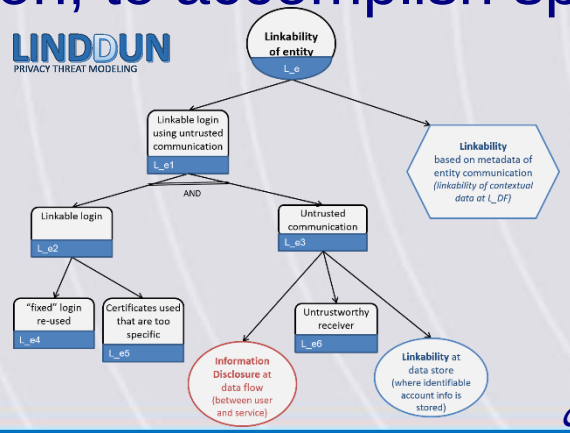
Method: Process description providing directions and rules and helping to set privacy goals, structured in a systematic way in tasks and stages

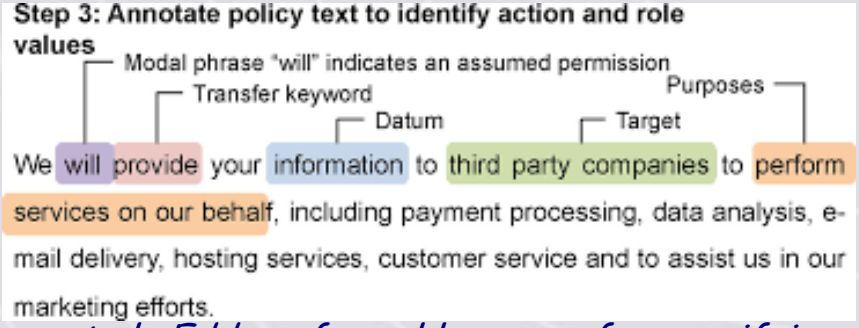


Privacy Engineering

Field of research and practice
that designs, implements, adapts, and evaluates
theories, methods, techniques, and tools
to systematically capture and address privacy issues
when developing information systems

Technique: Procedures, possibly with a prescribed language or notation, to accomplish specific privacy-engineering tasks





T. Breaux et al., Eddy, a formal language for specifying and analyzing data flow specifications for conflicting privacy requirements

Privacy Engineering

Field of research and practice
that designs, implements, adapts, and evaluates
theories, methods, techniques, and tools
to systematically capture and address privacy issues
when developing information systems

Tools: Means (automated or not) that support privacy engineers to carry out their responsibilities within a privacy-engineering method

Privacy Engineering

Field of research and practice
that designs, implements, adapts, and evaluates
theories, methods, techniques, and tools
to systematically capture and address privacy issues
when developing information systems

Method engineering: Engineering discipline to design, construct and adapt methods, techniques and tools for the development of information systems

Sjaak Brinkkemper, Method engineering: engineering of information systems development methods and tools, Information and Software Technology 38:4, pp. 275-280, 1996.

Situational method engineering: Design new methods tuned to the project at hand departing from existing method parts or elements

Next steps

Identify method chunks for privacy engineering

- PRIPARE
- International Workshop on Privacy Engineering
- Privacy Engineering Community

Contribute to ISO/IEC NP 21876: Privacy Engineering

Contact

THANK YOU!!

José M. del Álamo
jm.delalamo@upm.es

3rd IEEE International Workshop on Privacy Engineering
http://ieee-security.org/TC/SPW2017/IWPE
iwpe17@easychair.org