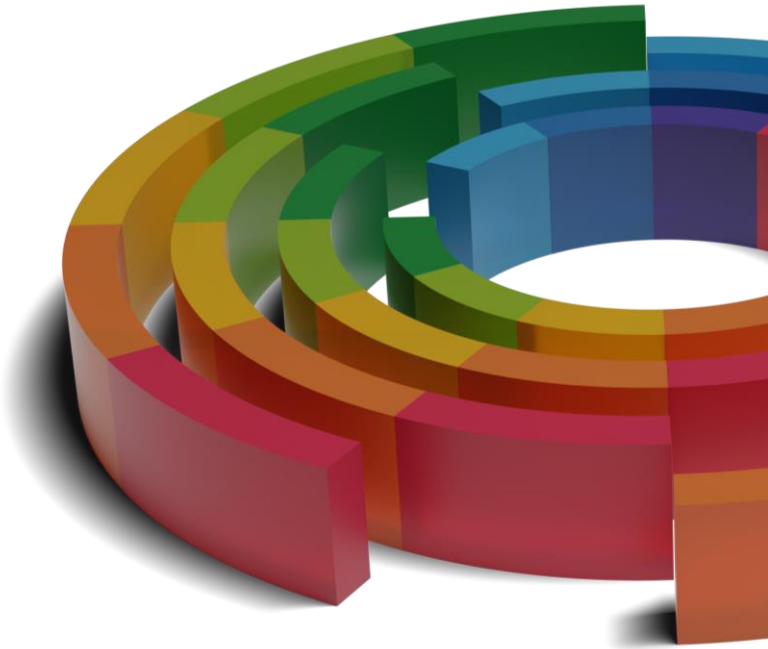
models4LINDDUN

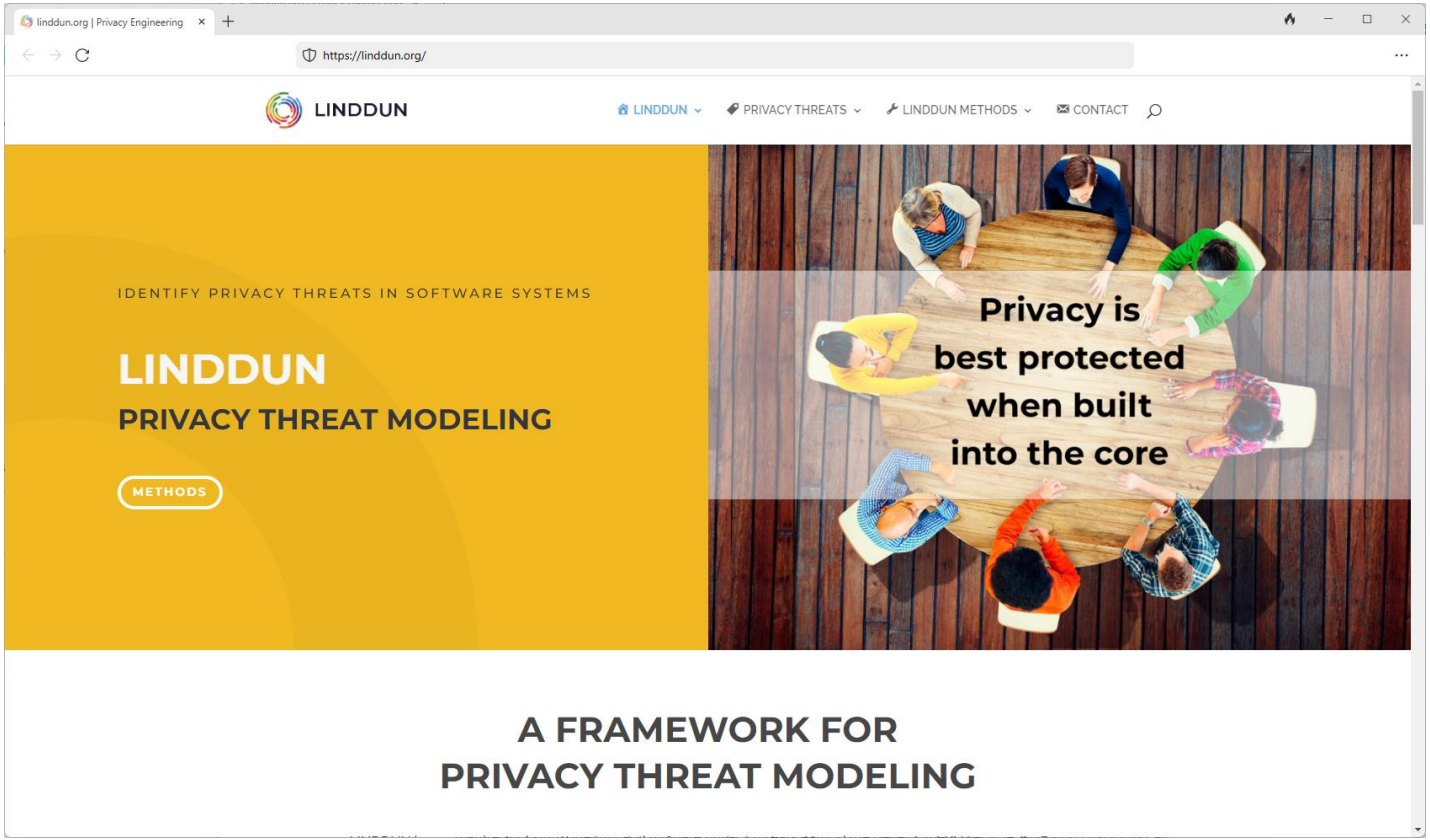
models4privacy



21 November 2023

DistriNet

updated version of LINDDUN



https://linddun.org

10+ years of LINDDUN

Combining, extending, and fine-tuning in privacy threat modeling research

2011

LINDDUN (V1)

Empirical studies

LINDDUN (V2)

Updated knowledge and process support

Feedback from the field

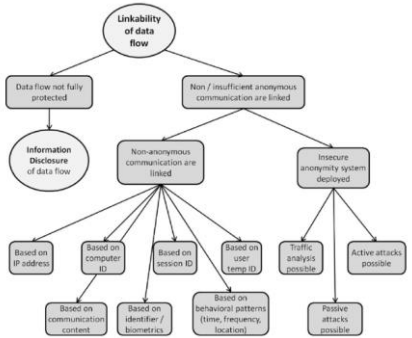
LINDDUN GO

Lean card-based threat elicitation support

Consolidating research expertise

LINDDUN

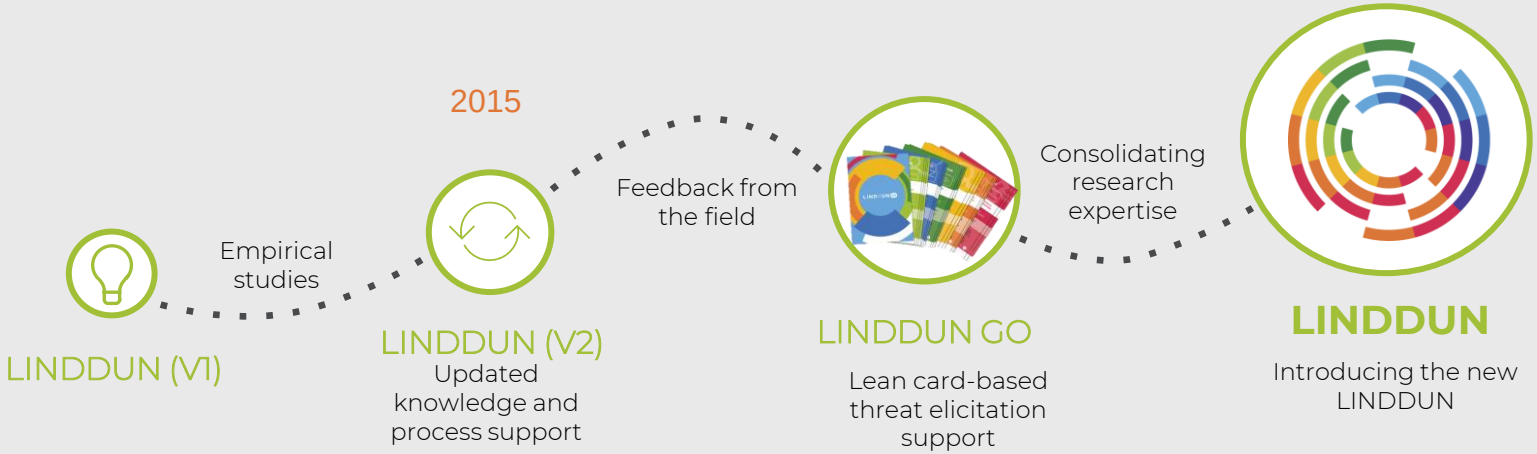
Introducing the new LINDDUN

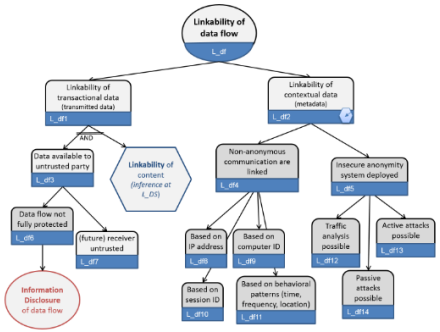


DistriNet

10+ years of LINDDUN

Combining, extending, and fine-tuning in privacy threat modeling research

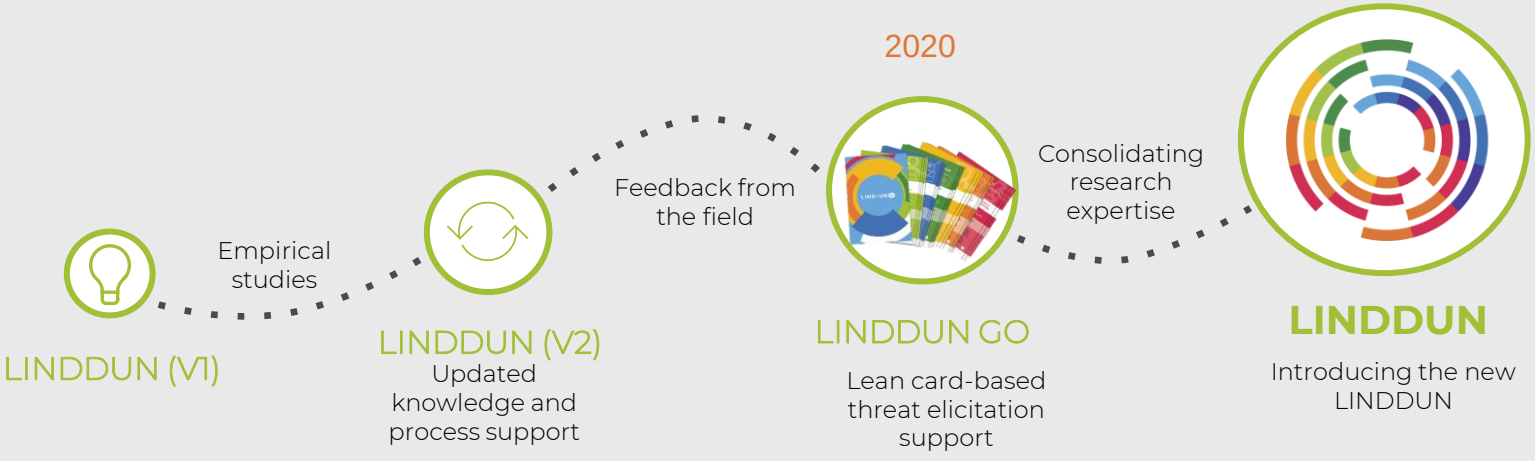


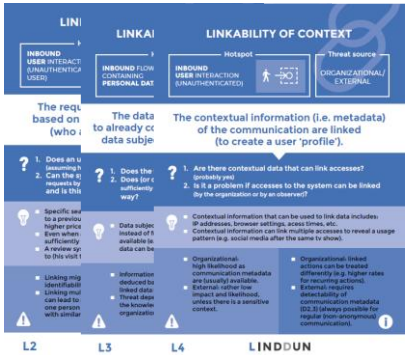


DistriNet

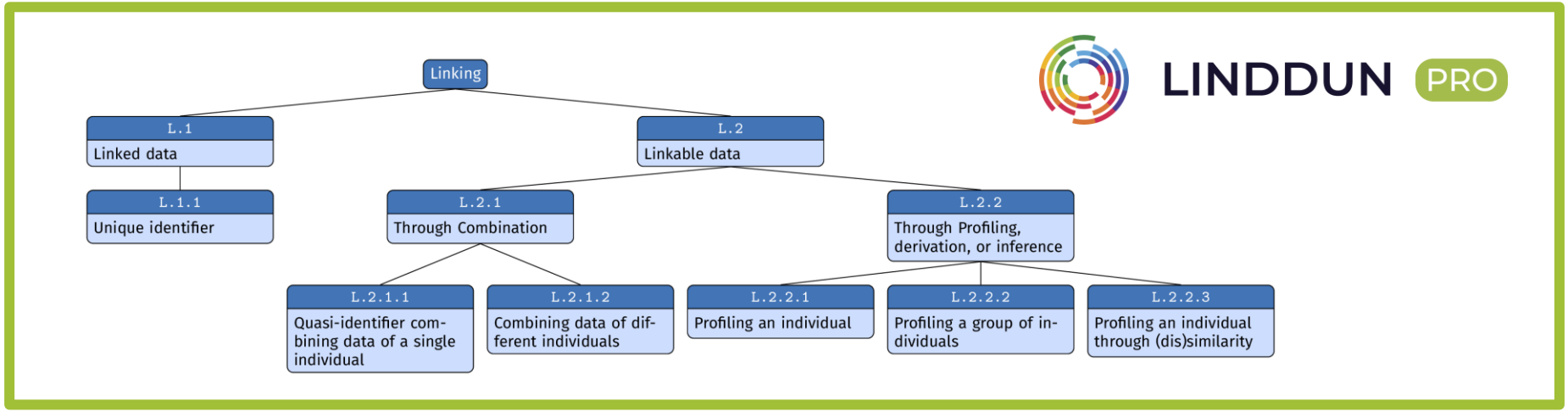
10+ years of LINDDUN

Combining, extending, and fine-tuning in privacy threat modeling research

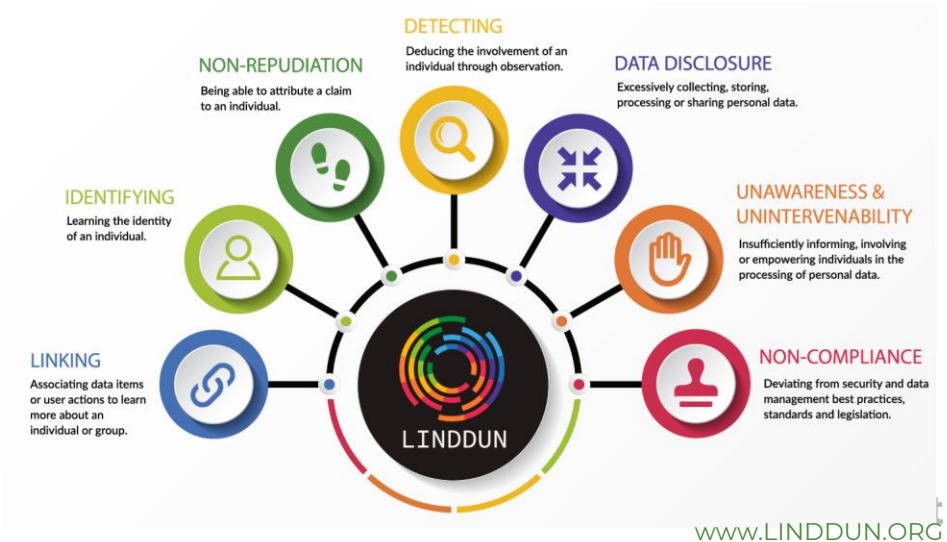




DistriNet

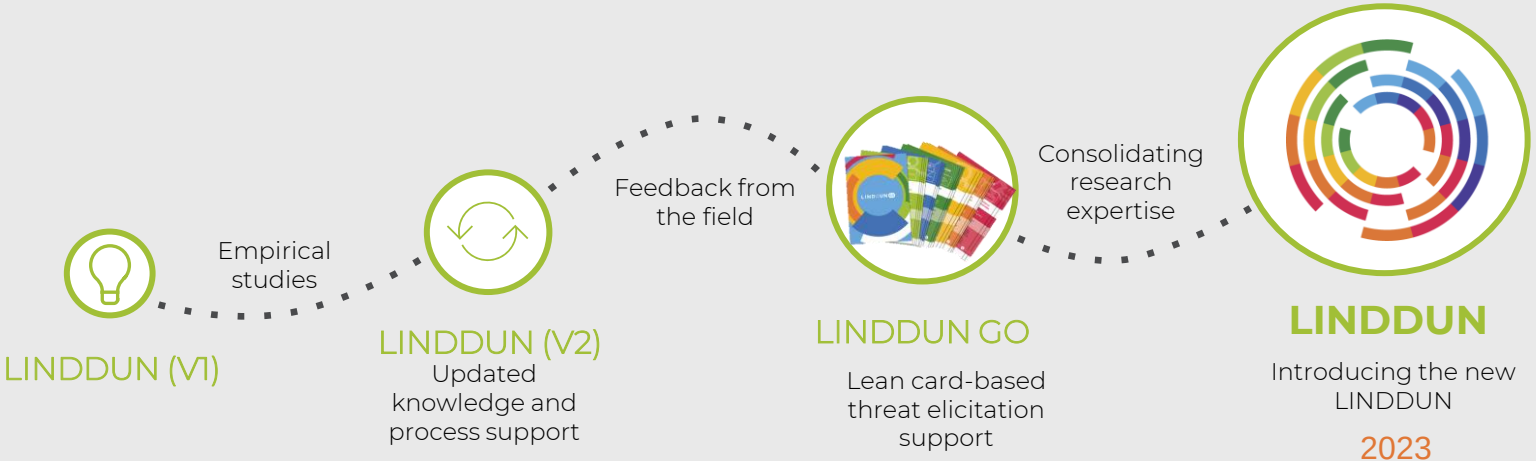

Linking
L.1
Linked data
L.1.1
Unique identifier
L.2
Linkable data
L.2.1
Through Combination
L.2.2
Through Profiling, derivation, or inference
L.2.1.1
Quasi-identifier combining data of a single individual
L.2.1.2
Combining data of different individuals
L.2.2.1
Profiling an individual
L.2.2.2
Profiling a group of individuals
L.2.2.3
Profiling an individual through (dis)similarity
LINDDUN PRO

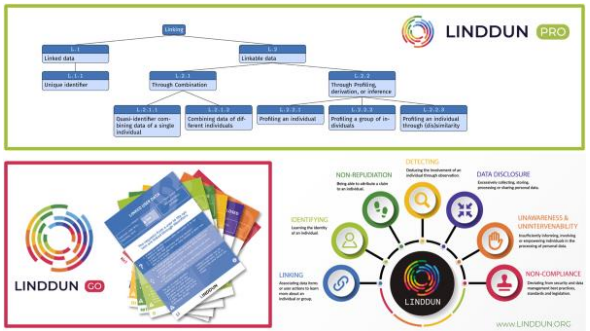

LINDDUN GO
LINKED USER DATA
LINDDUN


DETECTING
Deducing the involvement of an individual through observation.
NON-REPUDIATION
Being able to attribute a claim to an individual.
DATA DISCLOSURE
Excessively collecting, storing, processing or sharing personal data.
IDENTIFYING
Learning the identity of an individual.
UNAWARENESS & UNINTERVENABILITY
Insufficiently informing, involving or empowering individuals in the processing of personal data.
LINKING
Associating data items or user actions to learn more about an individual or group.
NON-COMPLIANCE
Deviating from security and data management best practices, standards and legislation.
LINDDUN

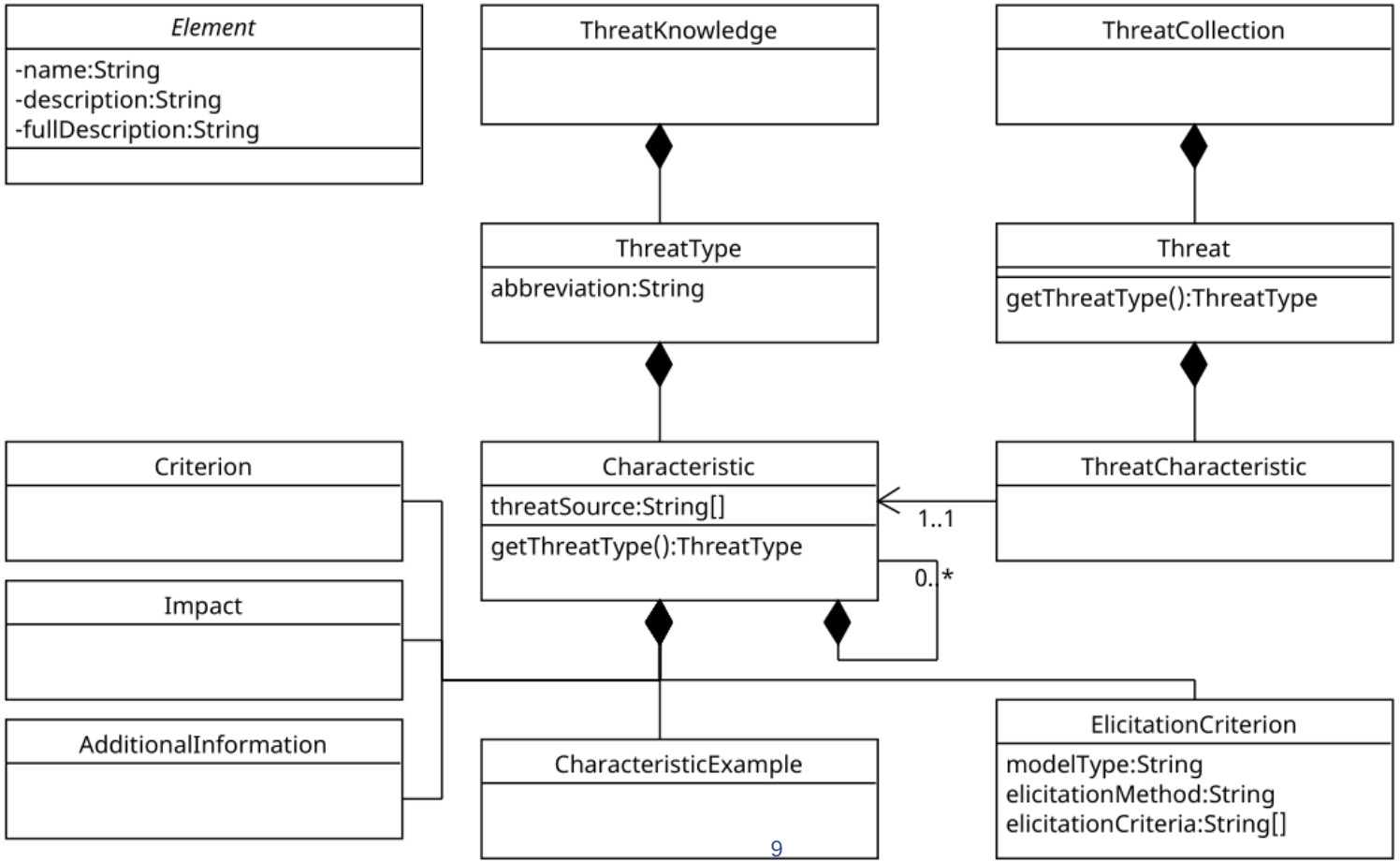
10+ years of LINDDUN

Combining, extending, and fine-tuning in privacy threat modeling research





Meta-model for threat knowledge



Linking

Identifying

Non-repudiation

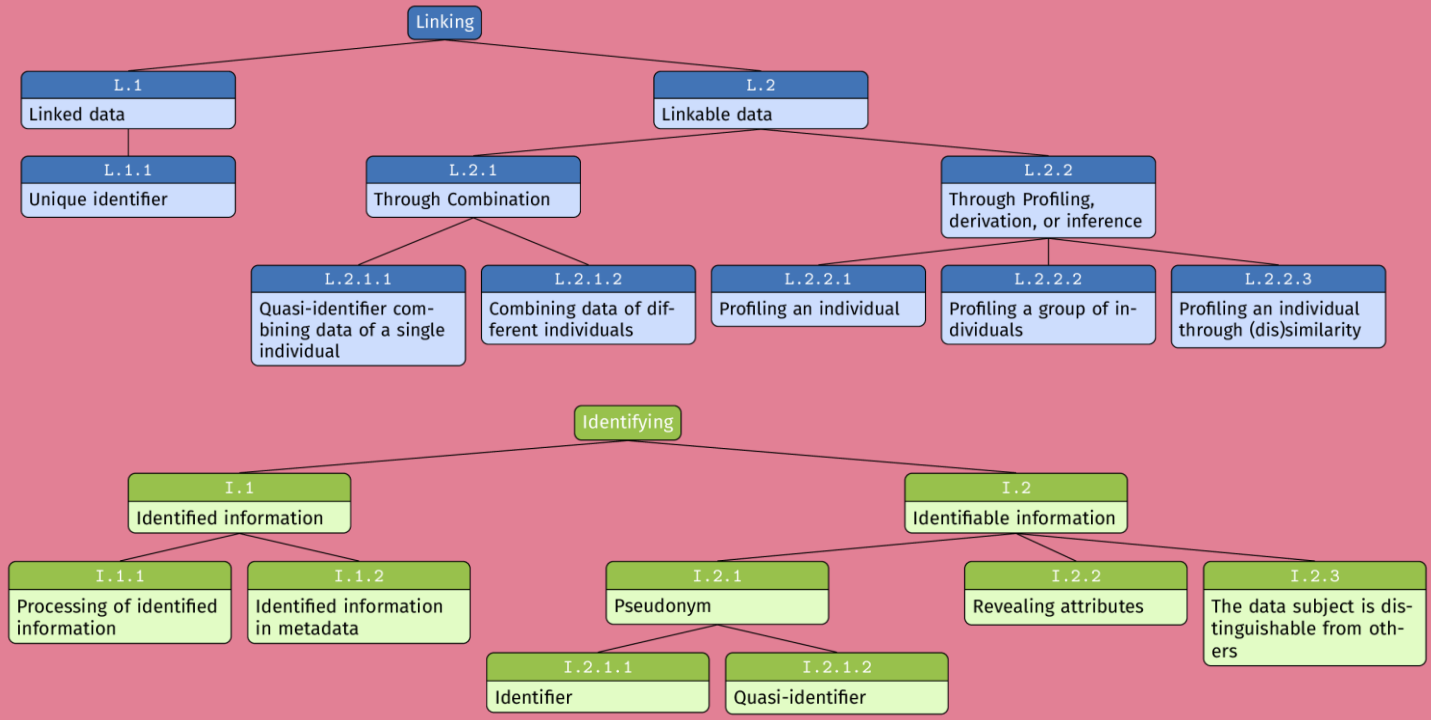
Detecting

Data Disclosure

Unawareness & Unintervenability

Non-compliance


LINKED USER DATA
Threat Source
ORGANIZATIONAL
EXTERNAL
INBOUND USER WITH PERSONAL DATA
Hotspot
The requests from a user to the system are linked through identifiers.
1. Is there an identifier (unique within the system or for the session) or dataset?
2. Is there other data associated with that identifier?
3. Is there previous data with the same identifier to which new data can be linked?
An email address as ID can be used to link al activity to the same user even across multiple services where that email address is used.
IP address can be used to link multiple visits to the same user.
All product views in a web shop are linked to the same because they are logged in.
Linking is especially easy for authenticated users, as all requests in the same session are linked.
The use of unique identifiers enables the linking of new data items to a user profile to gather increasing amounts of personal data linked to this profile. This can later lead to identifying threats.
LINDDUN
L1
Nc1
D1
Nr1
I1


Linking
L.1
Linked data
L.1.1
Unique identifier
L.2
Linkable data
L.2.1
Through Combination
L.2.1.1
Quasi-identifier combining data of a single individual
L.2.1.2
Combining data of different individuals
L.2.2
Through Profiling, derivation, or inference
L.2.2.1
Profiling an individual
L.2.2.2
Profiling a group of individuals
L.2.2.3
Profiling an individual through (dis)similarity
Identifying
I.1
Identified information
I.1.1
Processing of identified information
I.1.2
Identified information in metadata
I.2
Identifiable information
I.2.1
Pseudonym
I.2.1.1
Identifier
I.2.1.2
Quasi-identifier
I.2.2
Revealing attributes
I.2.3
The data subject is distinguishable from others

LINDDUN Web Catalog

Linking / Linked data / Unique identifie

- **LINKING** (2)
  - Linked data (1)
    - Unique identifier
  - Linkable data (2)
- **IDENTIFYING** (2)
- **NON-REPUDIATION** (2)
- **DETECTING** (3)
- **DATA DISCLOSURE** (4)
- **UNAWARENESS AND UNINTERVENABILITY** (2)
- **NON-COMPLIANCE** (3)

Unique identifier

Description

Linking based on an identifier that is u

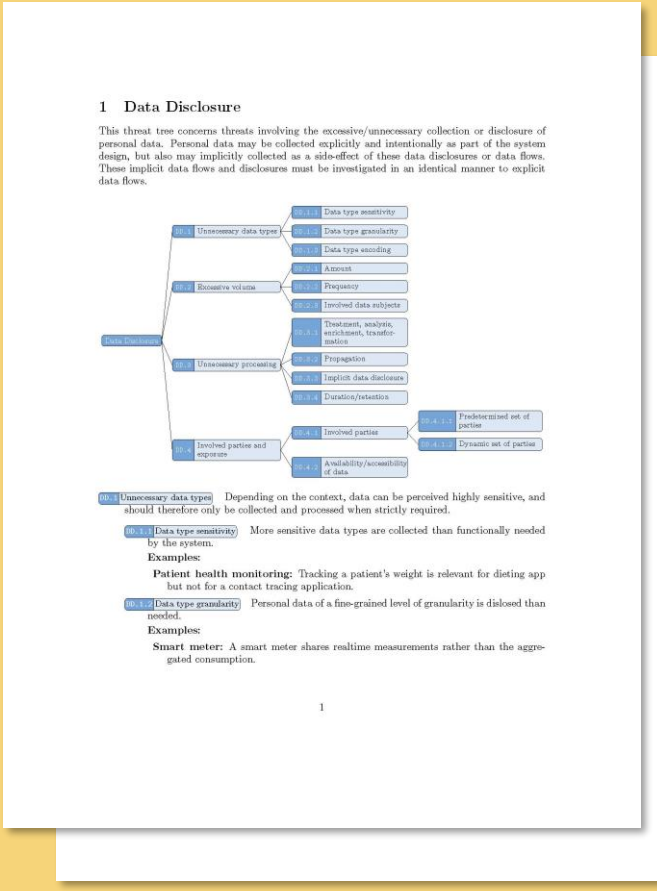
Unique identifiers make it trivial to link
interactions with a system) as belongi

Examples

- **Email address as ID**

  An email address as ID can be used t
  address is used.

  Many services frequently rely on emai
  different services on which they use t



1 Data Disclosure

This threat tree concerns threats involving the excessive/unnecessary collection or disclosure of personal data. Personal data may be collected explicitly and intentionally as part of the system design, but also may implicitly collected as a side-effect of these data disclosures or data flows. These implicit data flows and disclosures must be investigated in an identical manner to explicit data flows.

DD.1 Unnecessary data types Depending on the context, data can be perceived highly sensitive, and should therefore only be collected and processed when strictly required.

DD.1.1 Data type sensitivity More sensitive data types are collected than functionally needed by the system.

Examples:

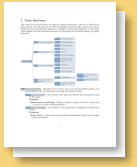
Patient health monitoring: Tracking a patient's weight is relevant for dieting app but not for a contact tracing application.

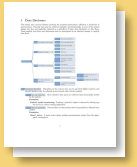
DD.1.2 Data type granularity Personal data of a fine-grained level of granularity is disclosed than needed.

Examples:

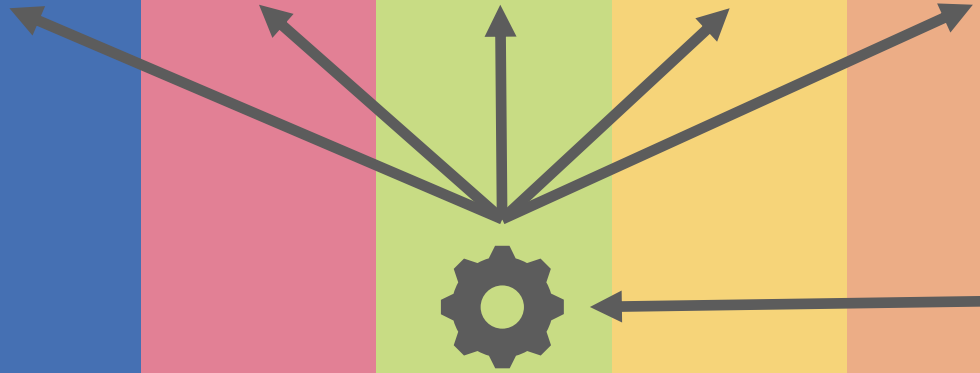
Smart meter: A smart meter shares realtime measurements rather than the aggregated consumption.


LINDDUN Web Catalog
Unique identifier
Description
Examples
Email address as ID



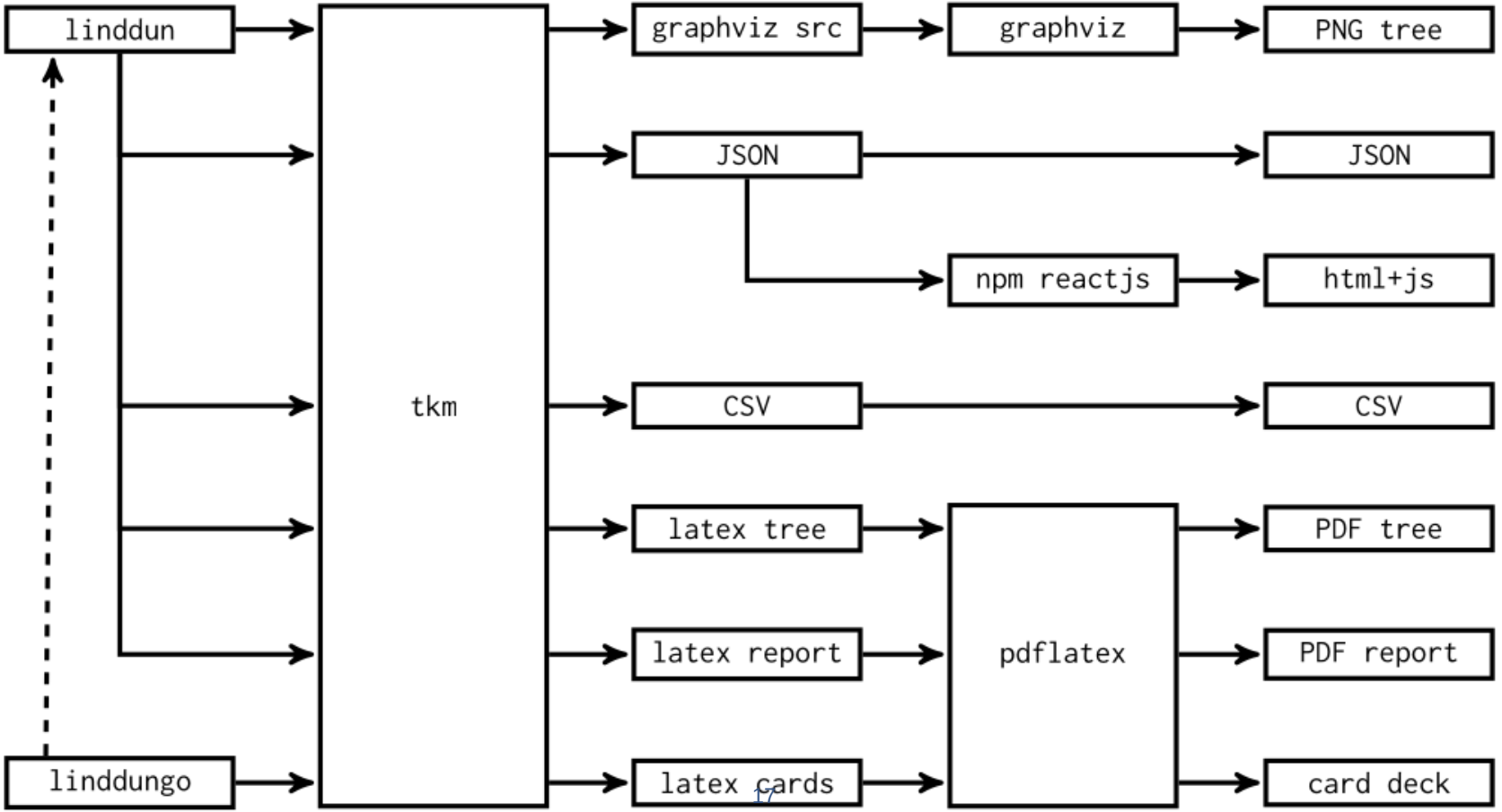


LINDDUN



DistriNet

Under the hood: models, model transformations and automated pipelines



Privacy threat knowledge repository that co-evolves

- Support for change & evolution
  - Privacy threats **evolve**
- Not a one-man/-team job:
  - **Stability** in threat types and characteristics
  - Openness in **characteristic refinement and examples**
- Adapt to domain and organization

looking ahead

- 1st **LINDDUN user group** meeting in Q2 2024
  - Practitioners & researchers
- Application cases!
- Catalog of mitigations, PETs, countermeasures!
- Tools!
- LINDDUN "Maestro"

https://www.linddun.org
linddun@cs.kuleuven.be