LINDDUN privacy threat modeling

Kim Wuyts

@wuytski

DistriNet

CIF seminar – september 2020

ABOUT ME

KIM WUYTS

POSTDOCTORAL RESEARCHER
IMEC-DISTRINET, KU LEUVEN, BELGIUM

RESEARCH FOCUS

PRIVACY
THREAT MODELING
SOFTWARE ENGINEERING
DATA PROTECTION
SECURITY

GET IN TOUCH

kim.wuyts@kuleuven.be
@wuytski
https://www.linkedin.com/in/kwuyts/

DistriNet

Today

- Threat modeling in general
- LINDDUN
  - What is LINDDUN?
  - LINDDUN privacy categories
  - Walk-through
  - Security vs. privacy threat modeling
- LINDDUN GO

WHY THREAT MODELING?

Threat modeling

Think about what can go wrong
so you can fix it, before it actually happens

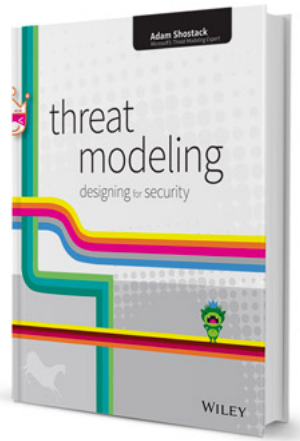
Threat modeling

What are you working on?

What can go wrong?

What are you going to do about it?

Did you do an acceptable job?



LINDDUN

LINDDUN privacy engineering framework

Systematic threat modeling methodology

- Inspired by STRIDE
- Support for elicitation and mitigation of privacy threats in software systems
- Early on in the development lifecycle

Privacy knowledge base


Linkability


Identifiability


Non-repudation


Detectability


Disclosure of information


Unawareness


Non-Compliance

LINDDUN privacy engineering framework

Systematic threat modeling methodology

- Inspired by STRIDE
- Support for elicitation and mitigation of privacy threats in software systems
- Early on in the development lifecycle

Scientific renown

Privacy knowledge base


Linkability


Non-repudation


Unawareness


Identifiability


Detectability


Non-Compliance


Disclosure of information

Industry acceptance
(ISO 27550, EDPS PbD opinion, ENISA PbD)

LINDDUN threat categories

Privacy threat categories

Linkability

Identifiability

Non-repudiation

Detectability

Disclosure of information

Unawareness

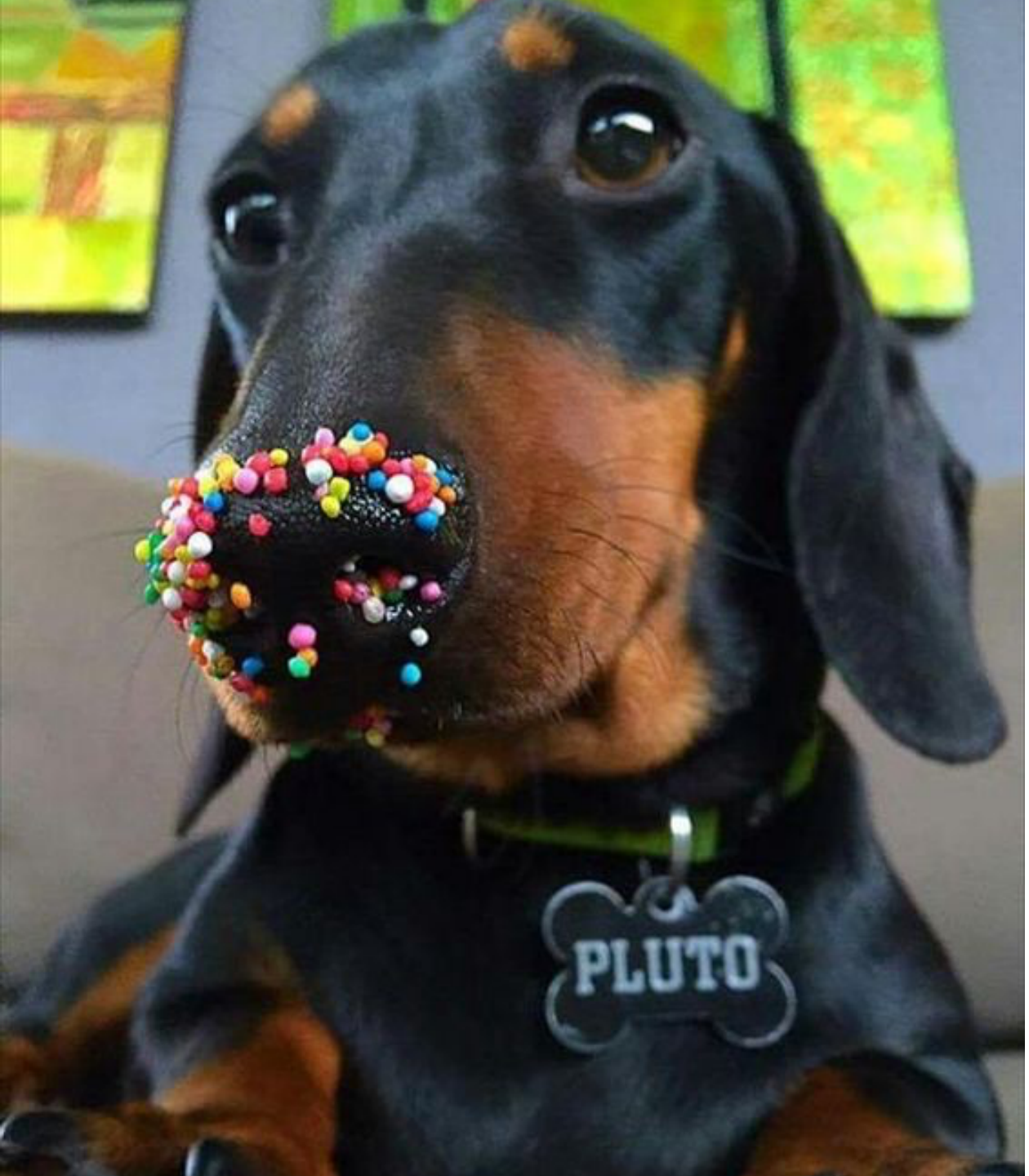
Non-compliance

Identifiability

Linkability

LINDDUN

Linkability



Non-repudiation

Detectability

LINDDUN

Disclosure of information

Unawareness

Non-compliance

LINDDUN

GDPR: Key concepts

Data subject rights

- Right to information
- Right to object
- Right of access
- Right to rectification
- Right to be forgotten
- Right to data portability
- Right to object to profiling

Unawareness

Processing principles

- Lawfulness fairness transparency
- Storage limitation
- Purpose limitation
- Accuracy
- Data minimization (proportionality)
- Integrity & confidentiality
- Accountability

Non-compliance

LINDDUN GO

DistriNet

Alternative privacy taxonomies

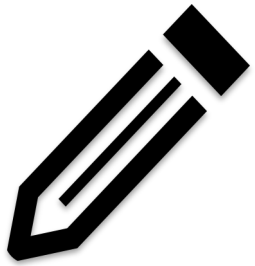
Similar to *security's* **CIA**

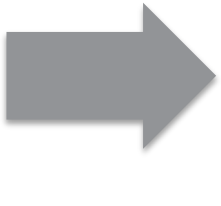
- Unlinkability - Intervenability – Transparency
  - Hansen, Jensen & Rost, 2015. *protection goals for privacy engineering*
- Predictability – Manageability – Dissassociability
  - NIST, 2017, *NISTIR 8062 – An introduction to privacy engineering and risk management in federal systems*

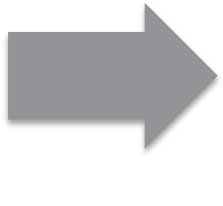
- Solove, D.J., 2006. *A taxonomy of privacy*
- Hoepman, J.-H., 2012. *Privacy Design Strategies*
- Gurses, S., 2010. *Multilateral Privacy Requirements Analysis in Online Social Networks*

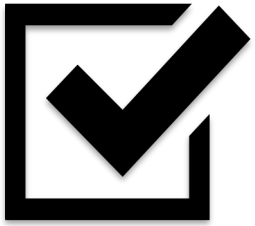
LINDDUN step-by-step

LINDDUN privacy engineering framework









Model the system

- create a data flow diagram
- describe all data

Elicit threats

- map threats to DFD elements
- identify threats using threat trees

Knowledge support

- mapping table
- LINDDUN threat taxonomy

Manage threats

- prioritize in dialog with the DPO
- mitigate using a taxonomy of PETs

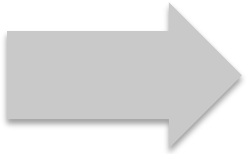
Knowledge support

- Taxonomy of mitigation strategies
- Classification of privacy solutions

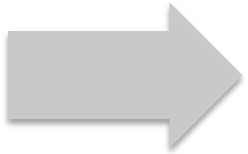
LINDDUN privacy engineering framework

LINDDUN privacy engineering framework - Step 1

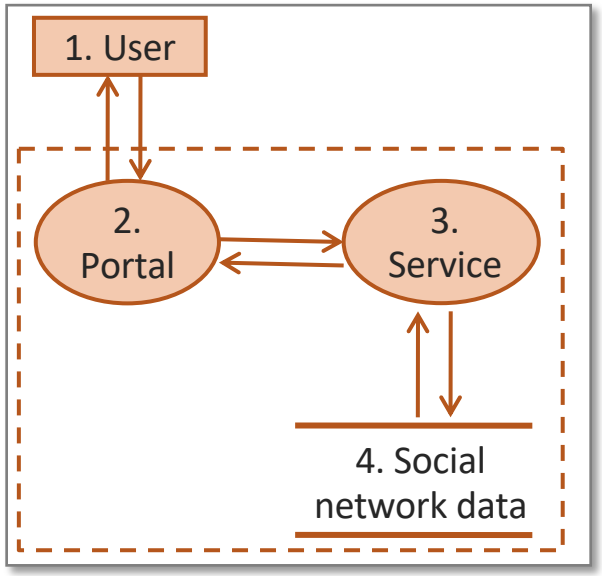
Model the system



Elicit threats



Manage threats



Entity

Data store

Process

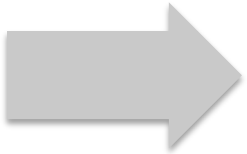
Data flow

LINDDUN

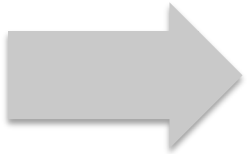
DistriNet

LINDDUN privacy engineering framework – Step 2

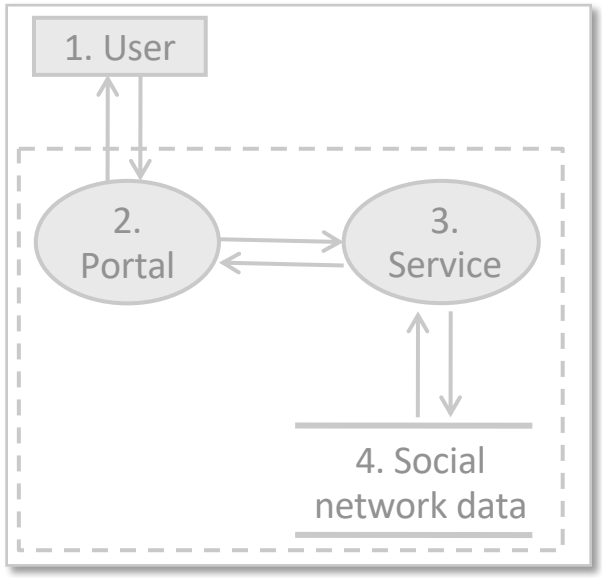
Model the system



Elicit threats



Manage threats



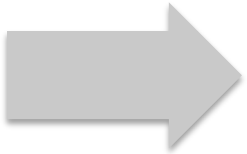
	Threat target	L	I	N	D	D	U	N
Data store	Social network db	X	X	x	x	X		X*
Data flow	User-portal data stream	X	X			X		X
	...	...						X

MAPPING TEMPLATE

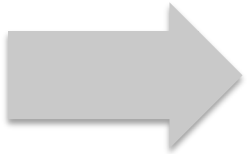
LINDDUN	L	I	N	D	D	U	N
Data store	X	X	X	X	X		X
Data flow	X	X	X	X	X		X
Process	X	X	X	X	X		X
Entity	X	X				X	

LINDDUN privacy engineering framework – step 2

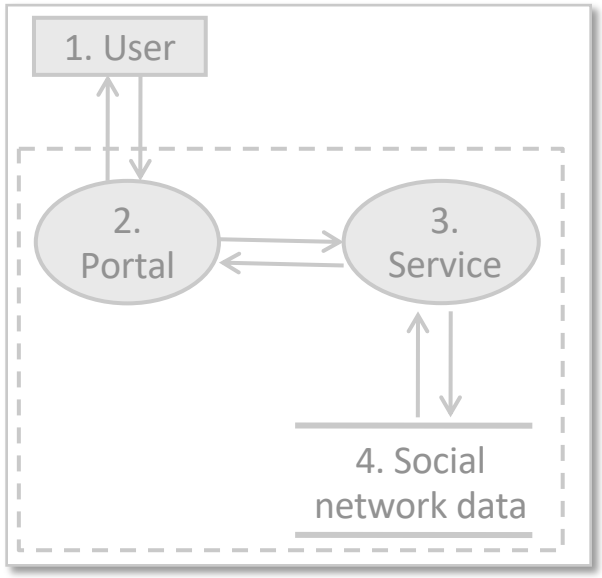
Model the system



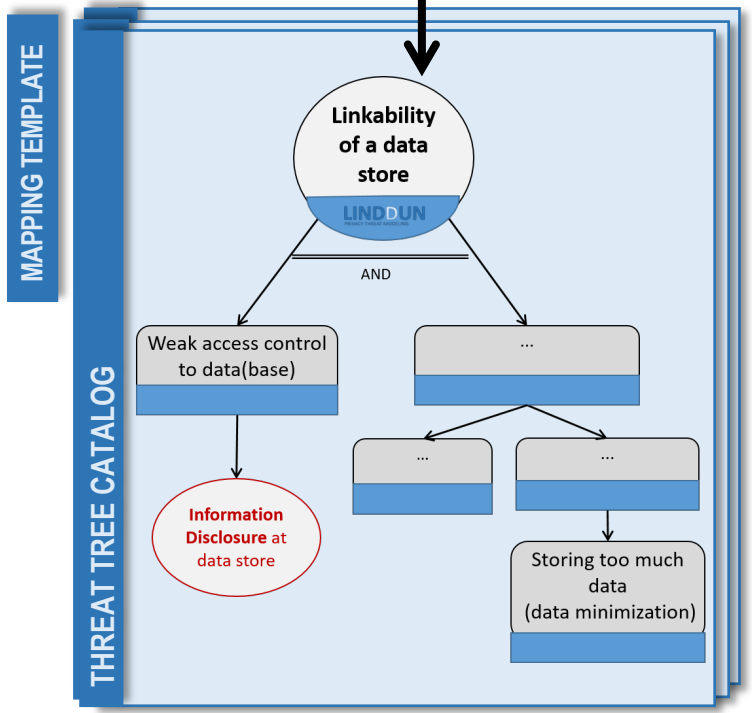
Elicit threats



Manage threats



	Threat target	L	I	N	D	D	U	N
Data store	Social network db	X	X	x	x	X		X*
Data flow	User-portal data stream	X	X			X		X
	...	...						X

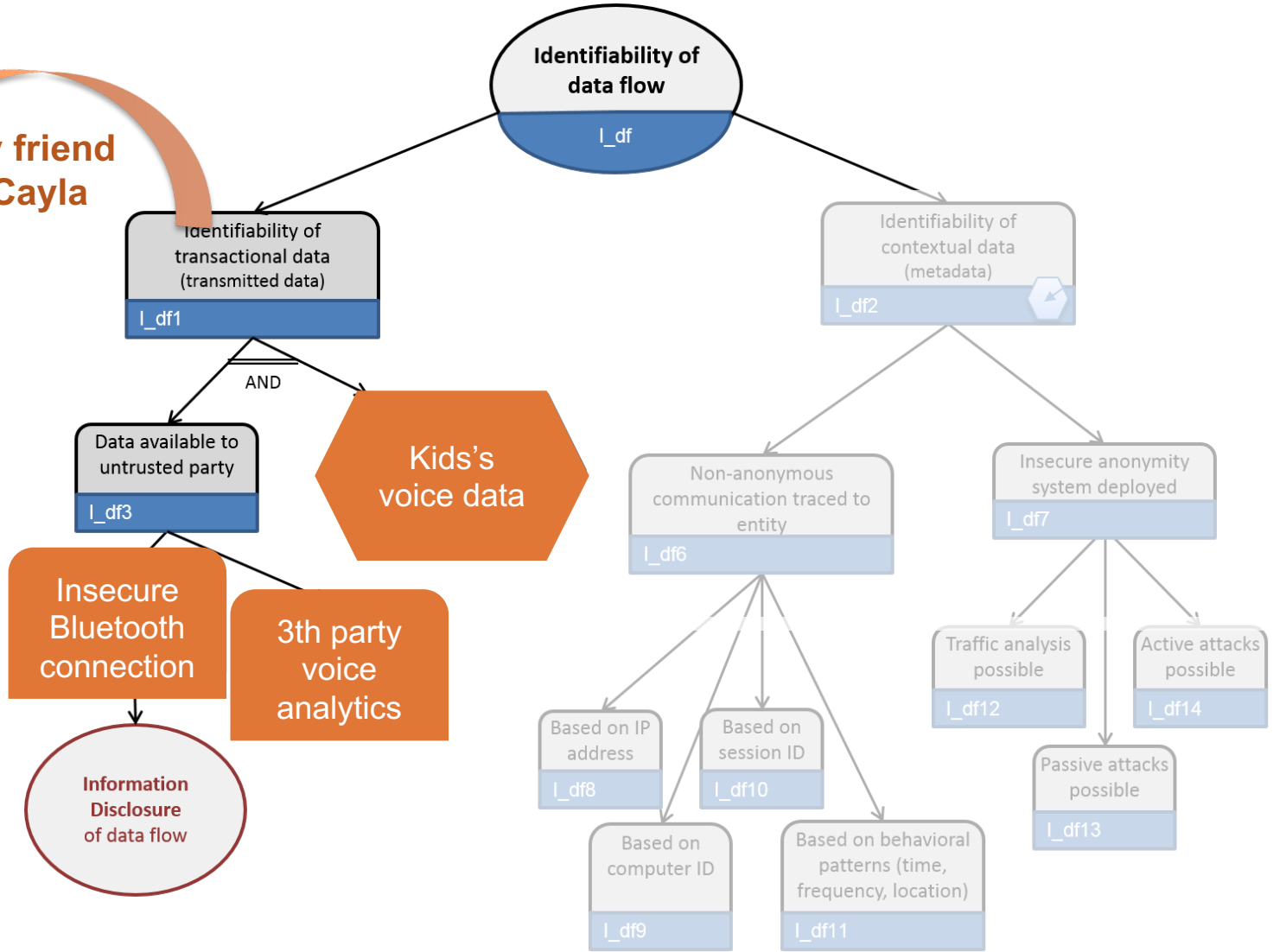


LINDDUN

DistriNet

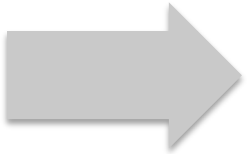
Step 2: Identify threat using threat tree catalog

My friend Cayla

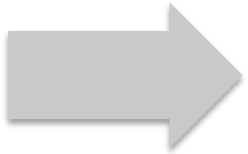


LINDDUN privacy engineering framework – step 2

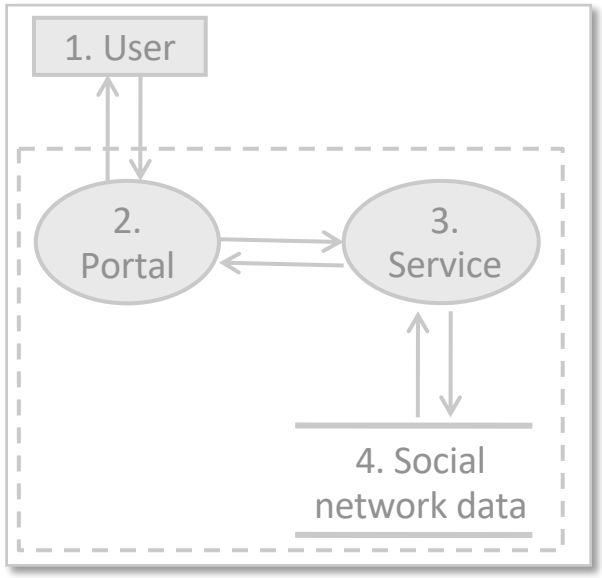
Model the system



Elicit threats



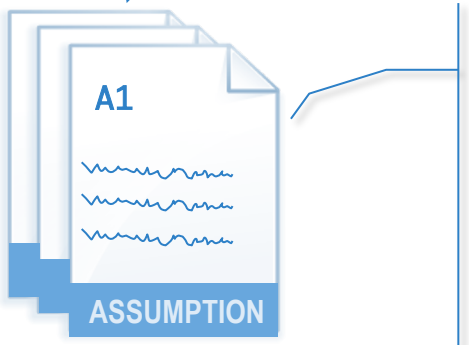
Manage threats



	Threat target	L	I	N	D	D	U	N
Data store	Social network db	**T1**	T2	A3	x	X		T3
Data flow	User-portal data stream	X	X			X		
	…	…						

MAPPING TEMPLATE

THREAT TREE CATALOG



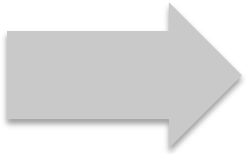
Assumptions

Preconditions / invariants that invalidate threats
e.g.:

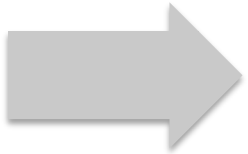
- non-repudiation threats often not applicable
- secure communication (https A+ grade)
- identifiability and linkability of data flow not applicable to closed systems

LINDDUN privacy engineering framework – step 2

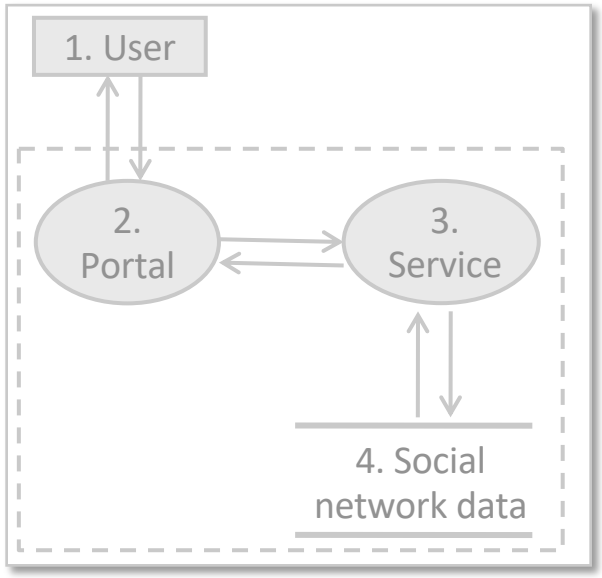
Model the system



Elicit threats



Manage threats



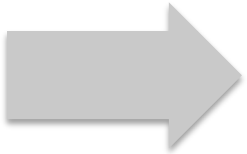
	Threat target	L	I	N	D	D	U	N
Data store	Social network db	**T1**	T2	A3	x	X		T3
Data flow	User-portal data stream	X	X			X		
	...	...						

MAPPING TEMPLATE

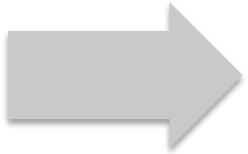
THREAT TREE CATALOG

LINDDUN privacy engineering framework – step 2

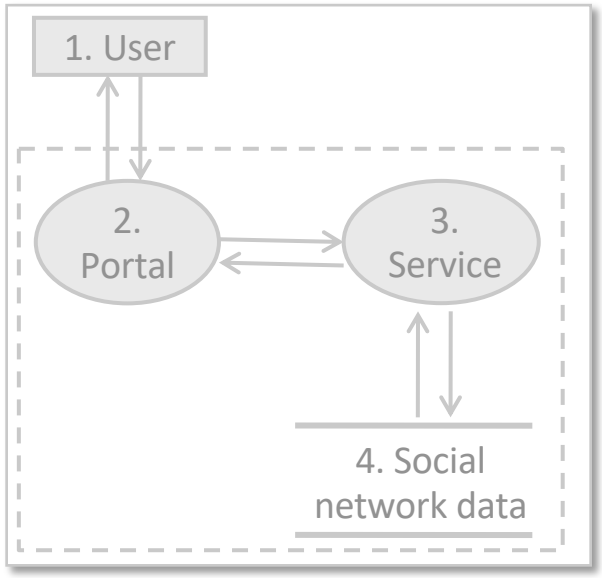
Model the system



Elicit threats



Manage threats



	Threat target	L	I	N	D	D	U	N
Data store	Social network db	**T1**	T2	A3	x	X		T3
Data flow	User-portal data stream	X	X			X		
	...	...						

MAPPING TEMPLATE

THREAT TREE CATALOG

Traceability of privacy assessment process

GDPR accountability

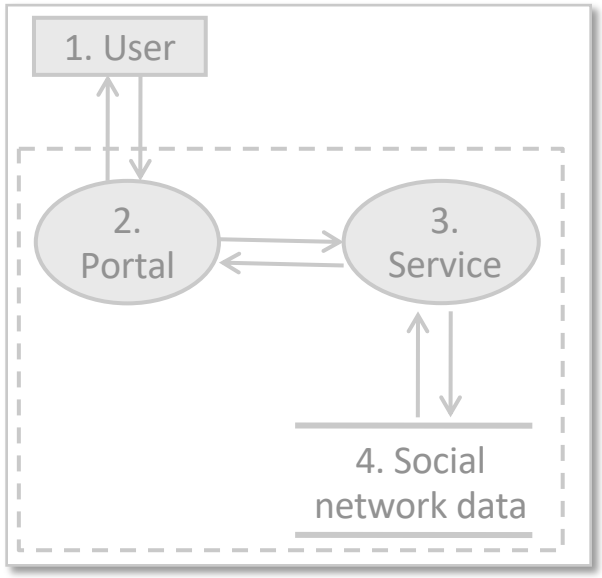
Step 2: Document identified threats - example

Threat 1	Using the forgot password feature we can identify a system user
DFD element(s)	P2. Portal
LINDDUN category(/ies)	Detectability
Description	Forgot password feature asks the email address of the user and after resetting the password says that a reset password email is successfully sent to the user. This could lead to identifiability problems where an attacker can easily check whether the user has a registration within the platform.
Countermeasure	None
Likelihood	Limited
Impact	Negligible
Action point (how would you solve it)	Modify the forgot password feature to always produce the same message making it impossible to figure out whether the user with the specified email address exists or not.
LINDDUN Reference	D_P

Inspired by misuse cases

LINDDUN privacy engineering framework – Step 3

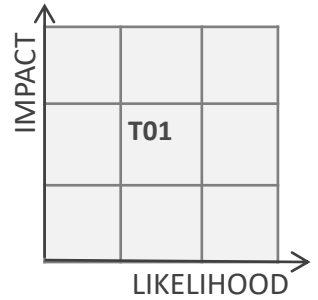
Model the system → **Elicit threats** → **Manage threats**



	Threat target	L	I	N	D	D	U	N
Data store	Social network db	**T1**	T2	A3	x	X		T3
Data flow	User-portal data stream	X	X			X		
	…	…						

MAPPING TEMPLATE

THREAT TREE CATALOG



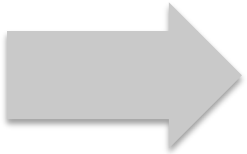
prioritize and assess
in dialog with the DPO

Risk = impact x likelihood

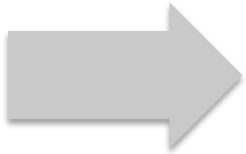
- ✓ *Accept*
- ✓ ***Mitigate***
- ✓ *Transfer*

LINDDUN privacy engineering framework – Step 3

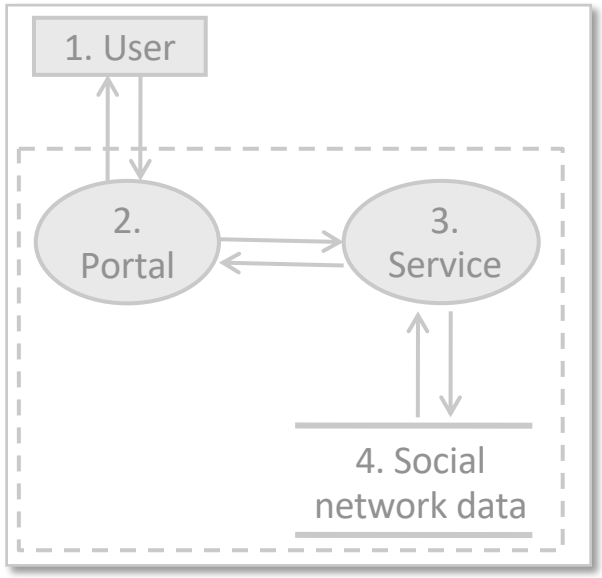
Model the system



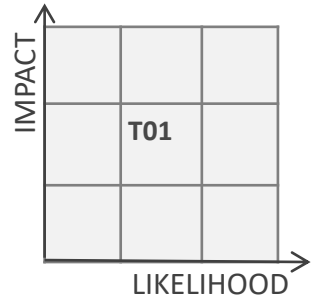
Elicit threats



Manage threats



	Threat target	L	I	N	D	D	U	N
Data store	Social network db	**T1**	T2	A3	x	X		T3
Data flow	User-portal data stream	X	X			X		
	...	...						



MAPPING TEMPLATE

THREAT TREE CATALOG

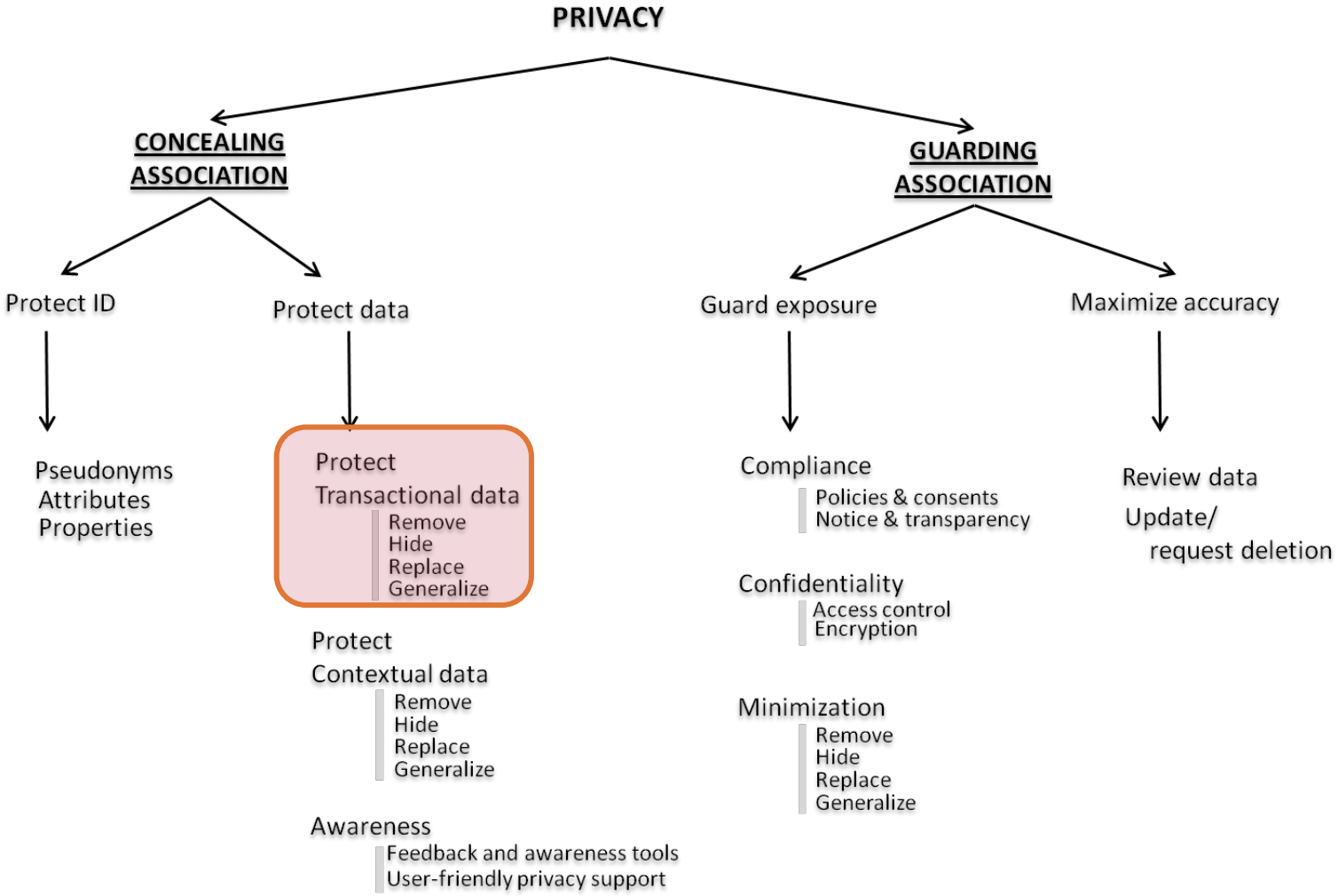
MITIGATION STRATEGIES

Protect ID
Protect data
- Transactional data
- Contextual data
- Awareness

Guard exposure
- Compliance
- Confidentiality
- Minimization

Maximize accuracy
- Review data
- Update/request deletion

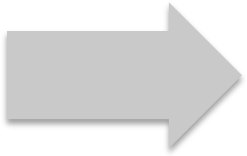
Step 3: Decision & Trade-off support with mitigation strategies



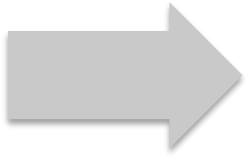
MITIGATION STRATEGY	LINDDUN THREAT TREE
Protect ID	L_e, I_e
Protect data	
Transactional data	L_df1, I_df1
Contextual data	L_df2, I_df2, D_df, NR_df
Awareness	U_1
Guard exposure	
Compliance	NC
Confidentiality	ID_ds, NR_ds, *_p
Minimization	L_ds, I_ds, D_ds
Maximize accuracy	
Review data	U_2
Update/request deletion	NR_ds3

LINDDUN privacy engineering framework – Step 3

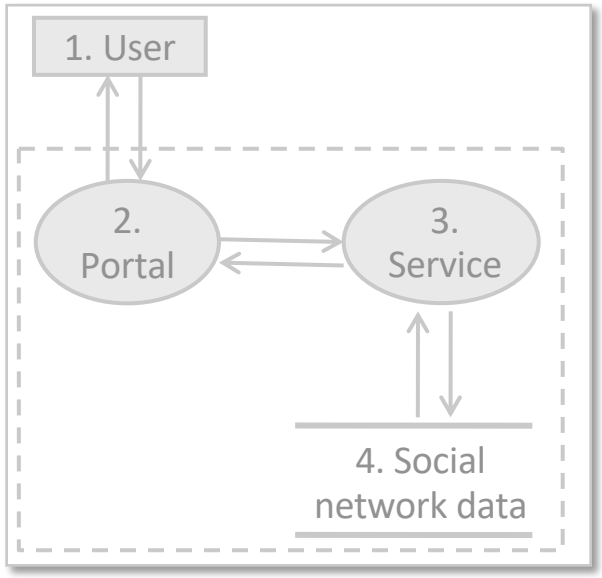
Model the system



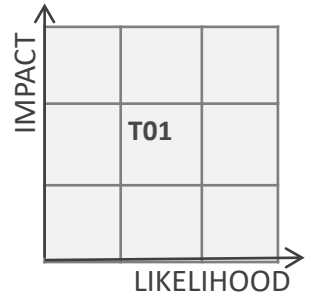
Elicit threats



Manage threats

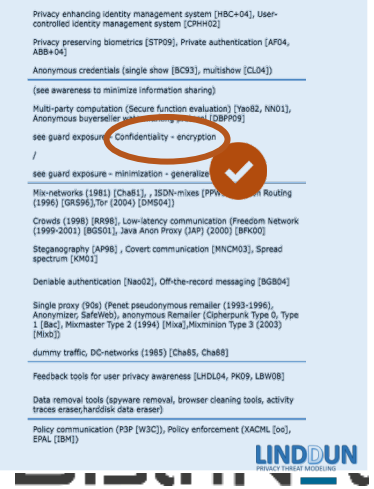


	Threat target	L	I	N	D	D	U	N
Data store	Social network db	**T1**	T2	A3	x	X		T3
Data flow	User-portal data stream	X	X			X		
	...	...						



MAPPING TEMPLATE

THREAT TREE CATALOG

MITIGATION STRATEGIES	PRIVACY ENHANCING TECHNIQUES
Protect ID **Protect data** Transactional data Contextual data Awareness **Guard exposure** Compliance Confidentiality Minimization **Maximize accuracy** Review data Update/request deletion	

LINDDUN privacy enhancing solutions

Mitigation Strategy				Privacy Enhancing Techniques (PETs)
Protect ID	Pseudonyms			Privacy enhancing identity management system, User-controlled identity management system
	Attributes			Privacy preserving biometrics, Private authentication
	Properties			Anonymous credentials (single show, multi-show)
Protect data	Transactional data	Remove		(see awareness to minimize information sharing)
		Hide	Data-flow specific	Multi-party computation (Secure function evaluation), Anonymous buyer-seller watermarking protocol
			General	*see guard exposure - Confidentiality - encryption*
		Replace		/
		Generalize		*see guard exposure - minimization - generalize*
	Contextual data	Remove		Mix-networks, ISDN-mixes, Onion Routing,Tor)
		Hide	General	Crowds, Low-latency communication, Java Anon Proxy
			Undetectability	Steganography, Covert communication, Spread spectrum
			Non-repudiation	Deniable authentication, Off-the-record messaging
		Replace		Single proxy (Penet pseudonymous remailer, Anonymizer, SafeWeb), anonymous Remailer (Cipherpunk Type 0, Type 1, Mixmaster Type 2,Mixminion Type 3)
		Generalize	Undetectability	dummy traffic, DC-networks
	Awareness	Feedback and awareness tools		Feedback tools for user privacy awareness
		User-friendly privacy support		Data removal tools (spyware removal, browser cleaning tools, activity traces eraser, harddisk data eraser)
Guard exposure	Compliance	Policies and Consents		Policy communication (P3P), Policy enforcement (XACML), EPAL)
		Notice and Transparency		/
	Confidentiality	Encryption		Symmetric key & public key encryption, Deniable encryption,Homomorphic encryption, Verifiable encryption
		Access control		Context-based access control, Privacy-aware access control
	Minimization	Remove		/
		Hide	Receiver privacy	Private information retrieval, Oblivious transfer
			Database privacy	Privacy preserving data mining, Searchable encryption, Private search
			General	*see guard exposure - confidentiality - encryption*
		Replace		/
		Generalize		K-anonymity model, l-Diversity
Maximize accuracy	Review data			/
	Update/ request deletion			/

privacy threat modeling

vs. security threat modeling
vs. data protection compliance

Security vs. privacy threat modeling

Requires a different mindset

- Security
  - Protecting data
  - Assets w.r.t. company
  - (external) attacker
  - Prevent (unauthorized) access to data
    - data as a whole
- Privacy
  - Protecting personal data
  - Assets w.r.t. data subject
  - Attacker + (internal) 'misbehavior'
  - Limit consequences of what you (can) do with personal data (once you have access)
    - Individual data items/attributes

Data protection compliance vs. privacy threat modeling

- Data protection impact assessment
  - Legal assessment
    - Legal roles (i.e. controller, processor, …)
    - Processing operations
    - Purpose specification
    - Compatibility assessment
    - …
- Privacy threat modeling
  - ✓ Risk-oriented
  - ✓ Model-driven
  - Architectural/technical assessment
    - ‘appropriate technical measures’
    - Privacy *by design*

LINDDUN in a nutshell

- **Systematic elicitation** and **mitigation** of privacy threats in software architectures
  - traceability / accountability
  - Thoroughness
  - Requires sufficient expertise
  - Rather high complexity/friction

LINDDUN in practice

- Applying the LINDDUN **mnemonic** (in a brainstorm-type exercise)

⚠ traceability / accountability

⚠ Thoroughness

⚠ Requires sufficient expertise

✓ ~~Rather high~~ complexity/friction

Light-weight privacy threat modeling

Lower the threshold

Requirements

Methodological support
- Simple
- Comprehensive
- Collaborative

Knowledge support
- Understandable description
- Applicability criteria

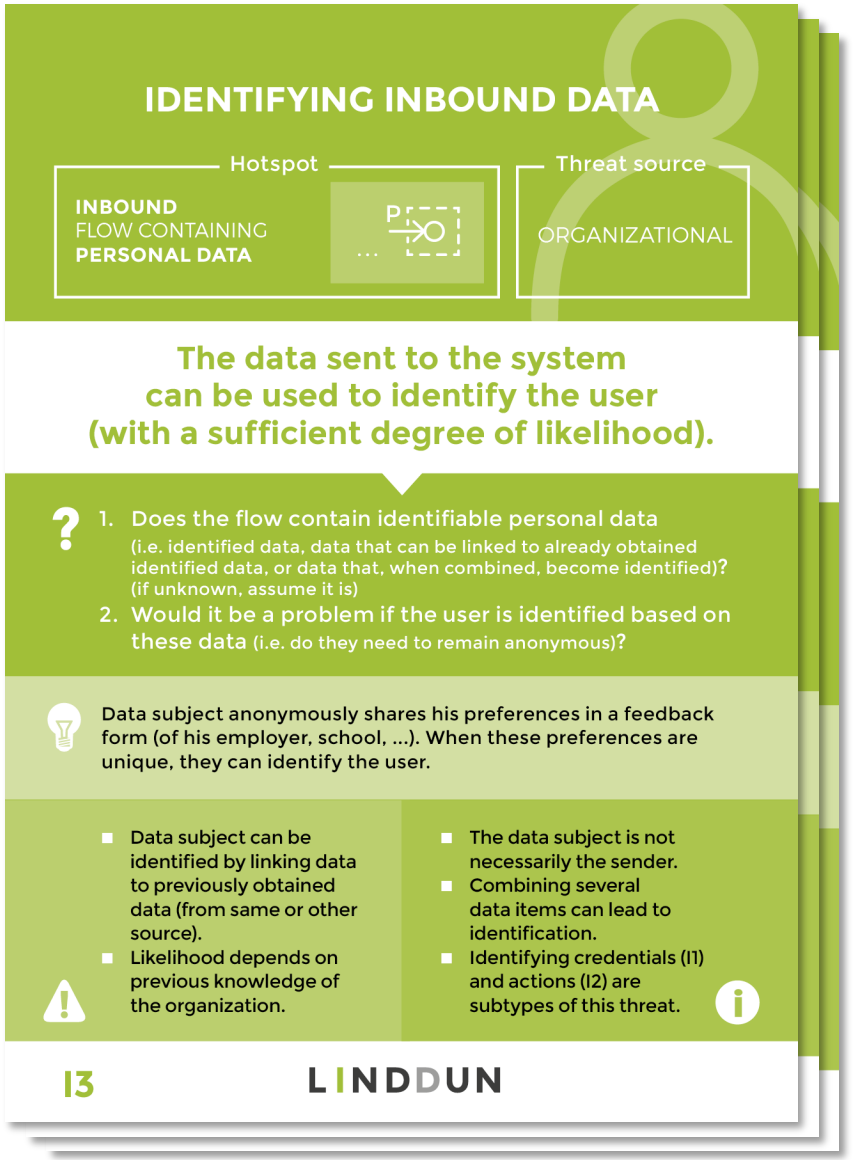
- Based on industry feedback and empirical studies
- Inspired by security threat modeling
  - EoP card game, TRIM & STRIPED extensions, cue cards, …

LINDDUN GO


LINDDUN GO
DistriNet

Creating LINDDUN GO

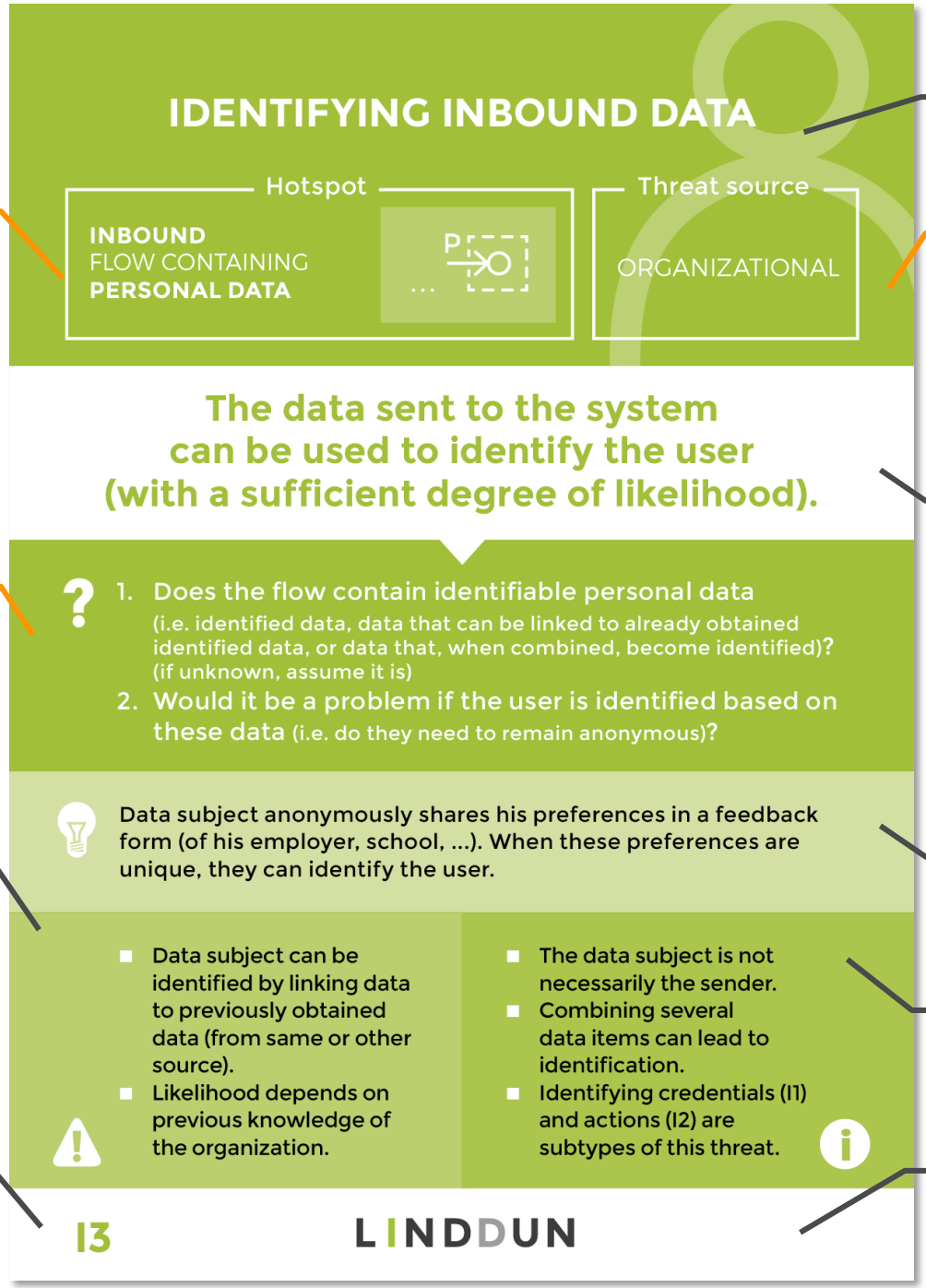
- Inspiration from EoP [1]
  - Card representation + Extended description
  - Collaborative + Process more closely resembles LINDDUN
- Reduced scope
  - 100 LINDDUN leaf nodes -> 35 threat type cards
    - Combined related threat types
    - Discarded low priority threats
- Content updates
  - Alignment with GDPR principles



LINDDUN

[1] *Shostack, A. (2014). Elevation of privilege: Drawing developers into threat modeling. In 2014 {USENIX} Summit on Gaming, Games, and Gamification in Security Education (3GSE 14). / https://www.microsoft.com/en-us/download/details.aspx?id=20303*

LINDDUN GO



Element/component where threat occurs in the system
(~ DFD interaction + additional constraints)

Questions to check applicability

Impact/ consequences
(why is it important)

Card identifier

Title

Origin of threat
(organizational, external, receiving party)

Summary

Example

Additional info

Highlighted LINDDUN category

LINDDUN

DistriNet

LINDDUN GO - hotspots

Inbound flows

Data enters the system.

A subtype of this hotspot describes an inbound flow with a user (i.e. human actor) as sender.

Outbound flows

Data leave the system.

A subtype of this hotspot describes an outbound flow with a user (i.e. human actor) as recipient.

Data storage

Data are being persisted in storage.

Data retrieval

Data are being retrieved from storage.

Processes

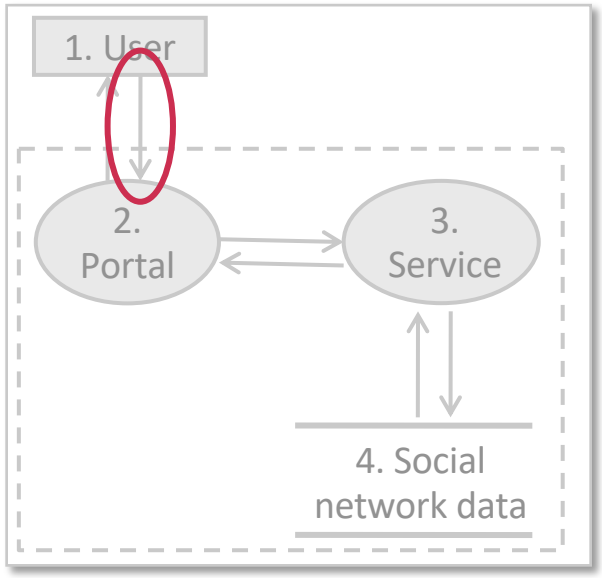
Data are being processed internally.

LINDDUN

DistriNet

Applying LINDDUN GO

Scoping with hotspots



IDENTIFYING INBOUND DATA

Hotspot

INBOUND
FLOW CONTAINING
PERSONAL DATA

Threat source

ORGANIZATIONAL

The data sent to the system can be used to identify the user (with a sufficient degree of likelihood).

1. Does the flow contain identifiable personal data (i.e. identified data, data that can be linked to already obtained identified data, or data that, when combined, become identified)? (if unknown, assume it is)
2. Would it be a problem if the user is identified based on these data (i.e. do they need to remain anonymous)?

Data subject anonymously shares his preferences in a feedback form (of his employer, school, ...). When these preferences are unique, they can identify the user.

- Data subject can be identified by linking data to previously obtained data (from same or other source).
- Likelihood depends on previous knowledge of the organization.

- The data subject is not necessarily the sender.
- Combining several data items can lead to identification.
- Identifying credentials (I1) and actions (I2) are subtypes of this threat.

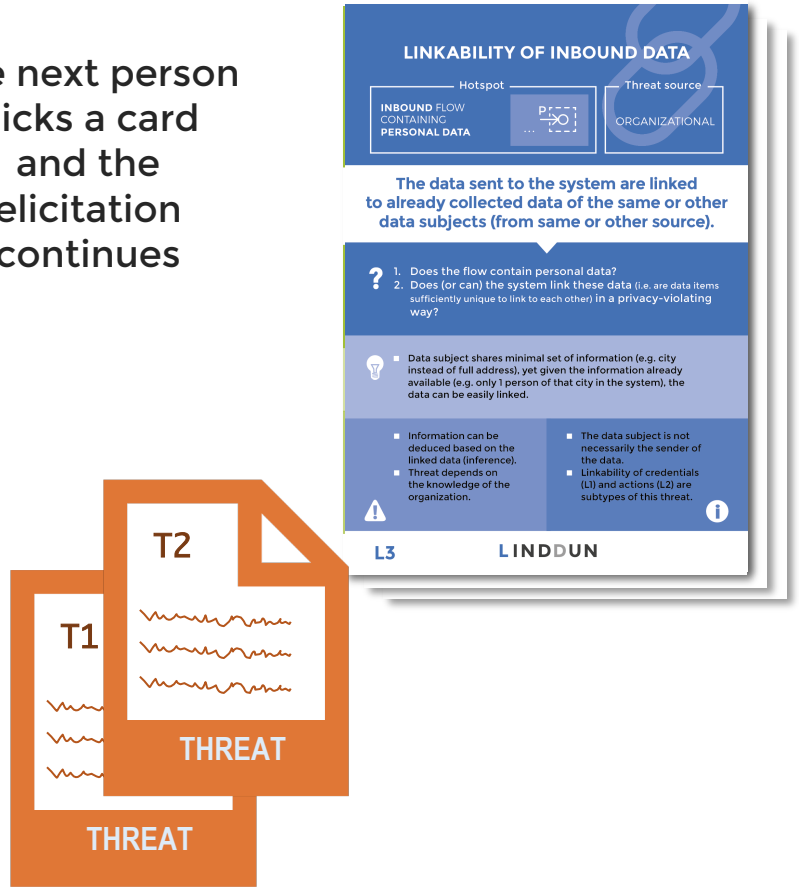
I3 LINDDUN

LINDDUN

DistriNet

LINDDUN GO - instructions

The next person picks a card and the elicitation continues



LINDDUN GO

DistriNet

LINDDUN GO - Variants

- **Quick** - Only the card drawer elicits an applicable threat. No group iteration over each card.
- **Time-boxed** - Time-box the exercise (or limit the number of cards) and do multiple threat modeling sessions
- **Fun** - Turn it into a game and earn points for each identified threat
- **Solitary** - use the threat type cards as input for an individual privacy threat elicitation exercise.
- **Freestyle** - Only use the LINDDUN GO category cards to ideate privacy threats. *(Note that this requires sufficient privacy expertise to be executed successfully)*

LINDDUN

DistriNet

LINDDUN GO category cards

LINKABILITY

What?

Being able to sufficiently distinguish whether two IOI (items of interest) are linked or not, even without knowing the actual identity of the subject of the linkable IOI. [PH2010]

Tell me more!

Data items can be linked because they belong to the same data subject, with a certain probability.

Examples: web page visits by the same user, entries in two databases related to the same person, people related by a friendship link, etc.

Data items can also be linked because they share the same property.

Examples: linking people who visit the same restaurant, linking people with a similar disease, etc.

So what?

Can result in:

Inference [WP29]
Deduce information from a set of data items.

Singling out [WP29] **/ attribution**
isolate some or all records which belong to precisely one individual (without necessarily identifying).

Identifiability
Link data items to identity of data subject.

LINDDUN GO

LINKABILITY

FLOWS TO/FROM SYSTEM

INBOUND

The system can link personal data it receives to other data items

OUTBOUND

The receiving parties can link the personal data to other data items

DATA STORAGE

STORE

The system stores personal data that can be linked to data items (from the same or other databases)

RETRIEVE

The retrieved data can be linked to other data items

LINDDUN GO

- **Summarize** each threat category
- Highlight the applicable **hotspots** to take into consideration

DistriNet

Preliminary evaluation

Trial run – students' hands-on experience * – feedback from industry professionals

- LINDDUN GO easier to apply than LINDDUN threat trees
- Cards and approach easy to understand
  - Applicability questions and examples most valued
  - Varying opinions on hotpots
  - Bonus points for collaborative aspect
- Suggestions
  - Documentation support
  - Solutions suggestions/selection

> While intended as a support privacy engineering at the design stage, LINDDUN GO helps all participants learn by doing in a collaborative way, confidently brainstorming different solutions. This makes it particularly suited to agile / DevOps organisations that don't have the luxury of wading through extensive documentation.
>
> Abigail Dubiniecki
> *Privacy Laws & Business - UK report september 2020*

*Special thanks to Ala'a Al-Momani, Christoph Bosch & Frank Kargl from ULM for sharing their results

Want to try?

www.linddun.org

We want your feedback!

Resources

- www.linddun.org

- Some recommendations
  - ENISA. *Privacy and Data Protection by Design – from policy to engineering, December 2014*
  - *ISO27550 on privacy engineering, 2019*
  - EDPS. *Preliminary opinion on privacy by design, May 2018*
  - The NIST Privacy Framework: *A Tool for Improving Privacy through Enterprise Risk Management Version 1.0* (January 2020)
  - Adam Shostack. *Threat modeling*, Wiley, 2014

LINDDUN privacy threat modeling

Kim Wuyts

@wuytski

https://www.linkedin.com/in/kwuyts/

DistriNet

WWW.LINDDUN.ORG