Interaction-Based Privacy Threat Elicitation

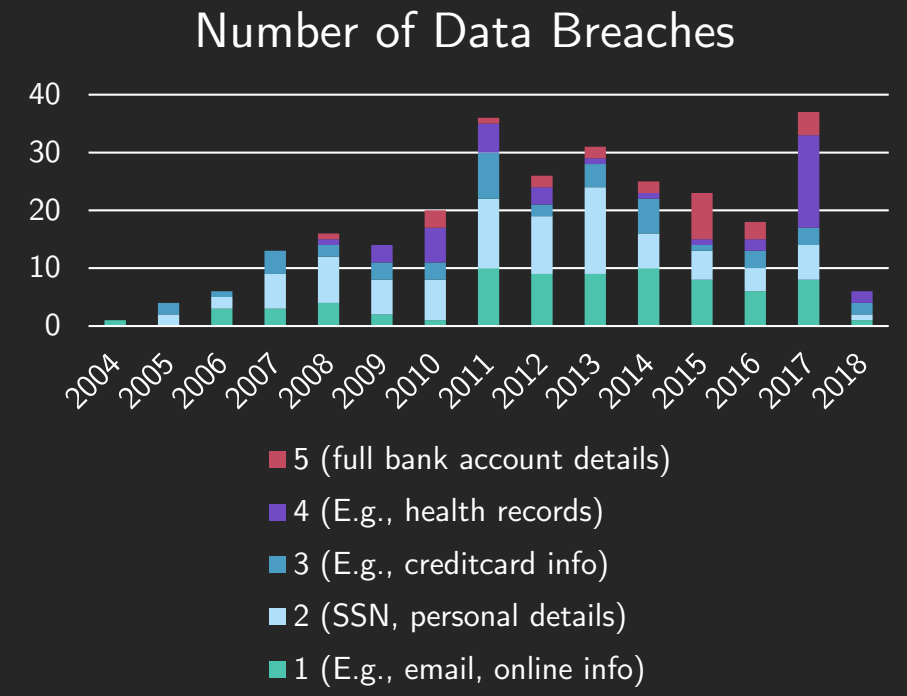
Laurens Sion, Kim Wuyts, Koen Yskout, Dimitri Van Landuyt, Wouter Joosen

27th April 2018 – IWPE2018 – London, United Kingdom

DistriNet

Importance of Considering Privacy by Design

- Data breaches

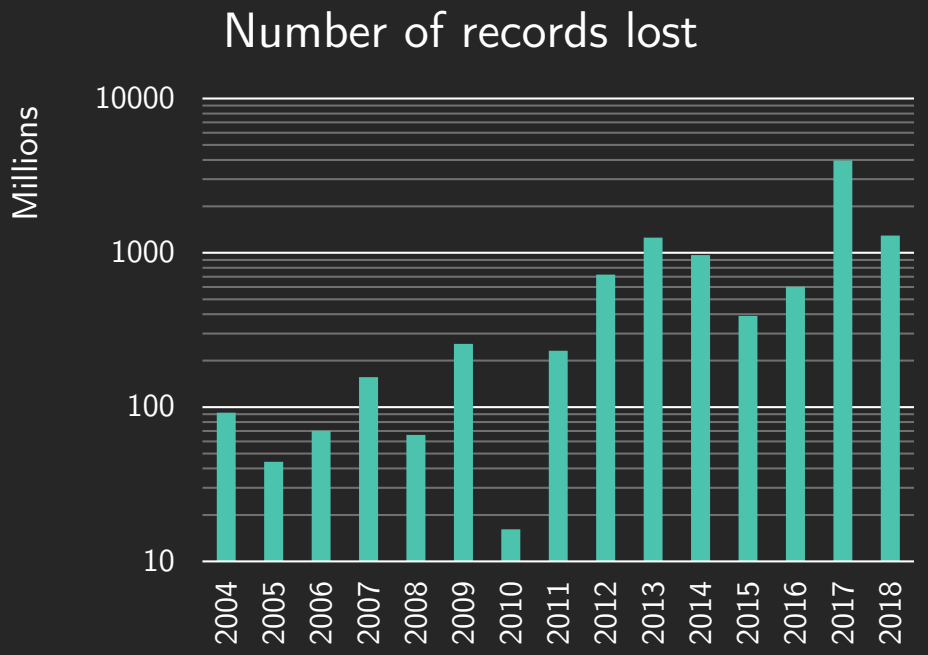


Data: *Information is beautiful: World's Biggest Data Breaches*

DistriNet

Importance of Considering Privacy by Design

- Data breaches



Data: *Information is beautiful: World's Biggest Data Breaches*

DistriNet

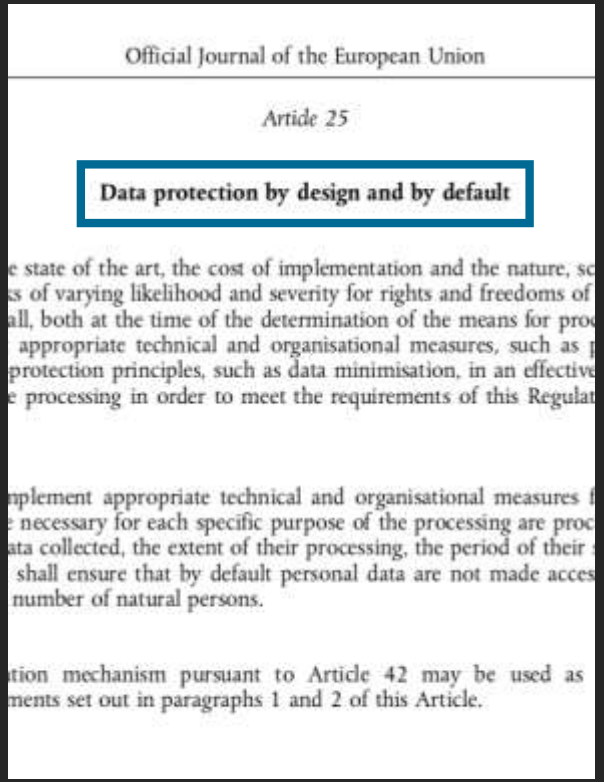
Importance of Considering Privacy by Design

- Data breaches
- Users' view inconsistent with collection/usage

Cambridge Analytica

Importance of Considering Privacy by Design

- Data breaches
- Users' view inconsistent with collection/usage
- Increasingly legislated
  - GDPR mandates privacy by design



Official Journal of the European Union

Article 25

Data protection by design and by default

e state of the art, the cost of implementation and the nature, sc
s of varying likelihood and severity for rights and freedoms of
all, both at the time of the determination of the means for proc
appropriate technical and organisational measures, such as p
protection principles, such as data minimisation, in an effective
e processing in order to meet the requirements of this Regulat

mplement appropriate technical and organisational measures f
necessary for each specific purpose of the processing are proc
ata collected, the extent of their processing, the period of their
shall ensure that by default personal data are not made acces
number of natural persons.

tion mechanism pursuant to Article 42 may be used as
ments set out in paragraphs 1 and 2 of this Article.

Realizing Privacy by Design

- GDPR mentions risk $\gg$ 70 times

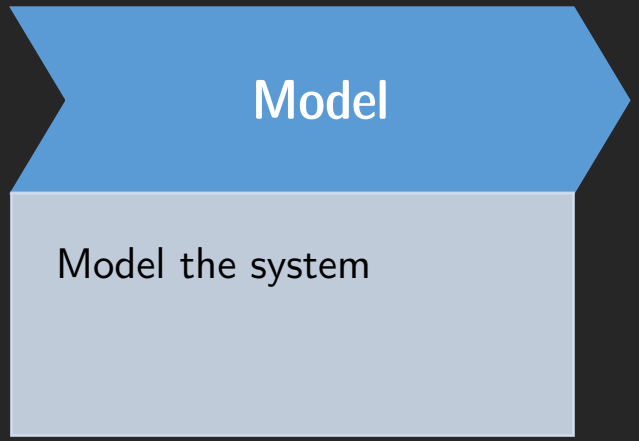
Realizing Privacy by Design

- GDPR mentions risk $\gg$ 70 times
- Appropriate technical measures
  - Identify issues

Realizing Privacy by Design

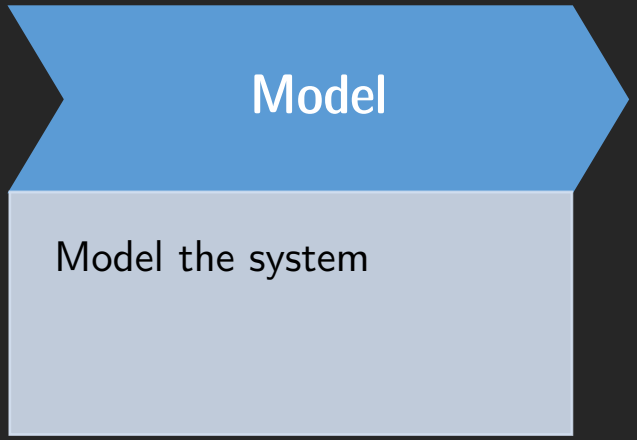
- GDPR mentions risk $\gg$ 70 times
- Appropriate technical measures
  - Identify issues
- Accountability
  - Demonstrate compliance

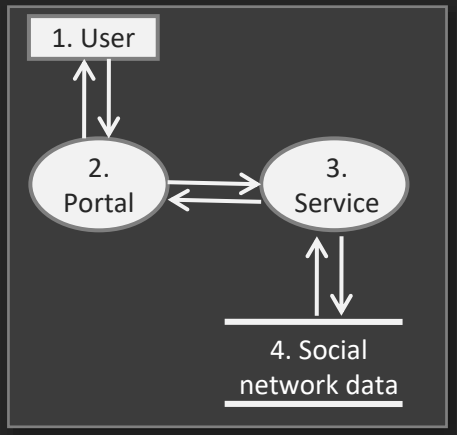
Privacy Threat Modeling Steps



Privacy Threat Modeling Steps

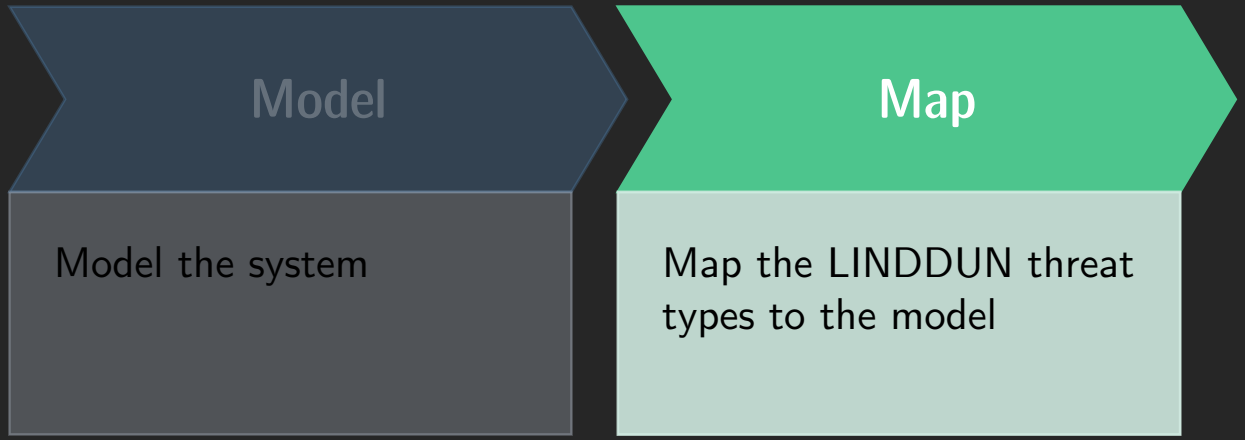
Model





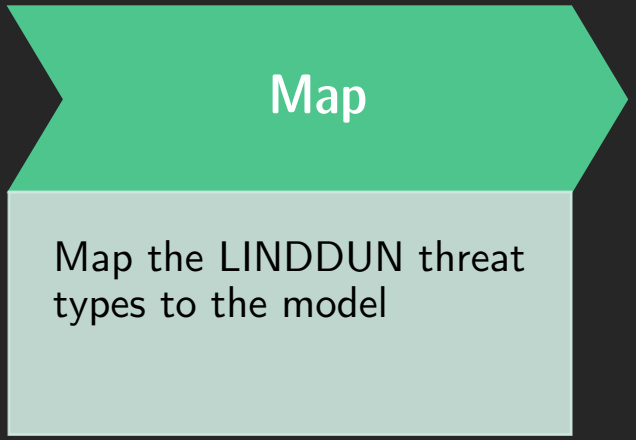
› DFD model of the system

Privacy Threat Modeling Steps



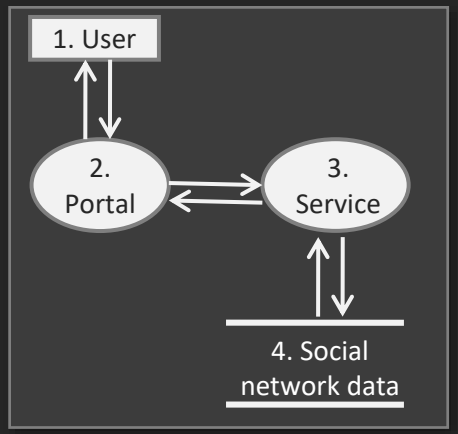
Privacy Threat Modeling Steps

Map



Privacy Threat Modeling Steps

Map



Map

Map the LINDDUN threat types to the model

MAPPING TEMPLATE

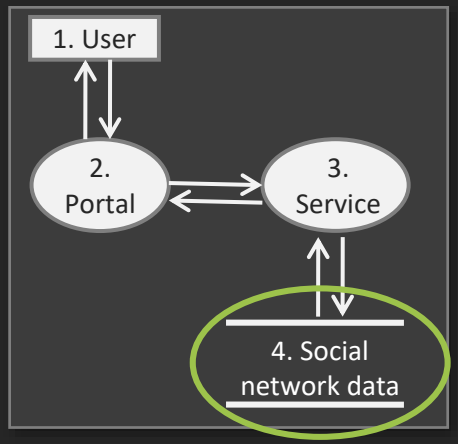
LINDDUN	L	I	N	D	D	U	N
Data store	X	X	X	X	X		X
Data flow	X	X	X	X	X		X
Process	X	X	X	X	X		X
Entity	X	X				X	

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

DistriNet

Privacy Threat Modeling Steps

Map



Map

Map the LINDDUN threat types to the model

MAPPING TEMPLATE

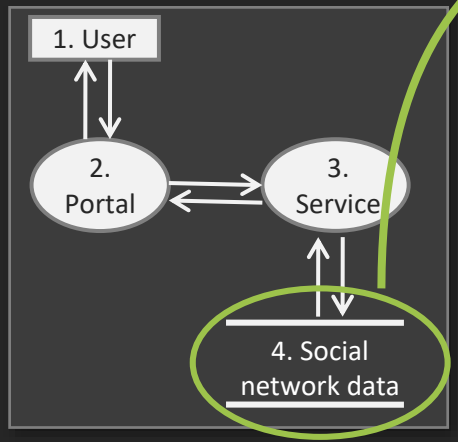
LINDDUN	L	I	N	D	D	U	N
Data store	X	X	X	X	X		X
Data flow	X	X	X	X	X		X
Process	X	X	X	X	X		X
Entity	X	X				X	

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

DistriNet

Privacy Threat Modeling Steps

Map



Map

Map the LINDDUN threat types to the model

MAPPING TEMPLATE

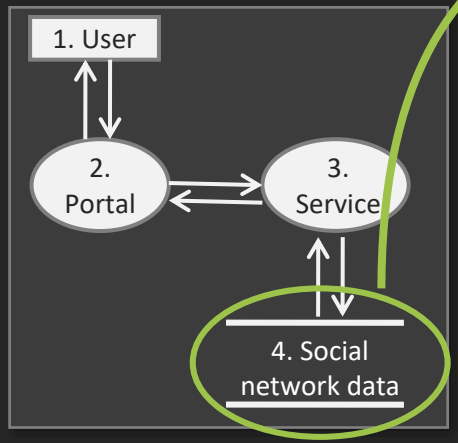
LINDDUN	L	I	N	D	D	U	N
Data store	X	X	X	X	X		X
Data flow	X	X	X	X	X		X
Process	X	X	X	X	X		X
Entity	X	X				X	

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

DistriNet

Privacy Threat Modeling Steps

Map



Map

Map the LINDDUN threat types to the model

MAPPING TEMPLATE

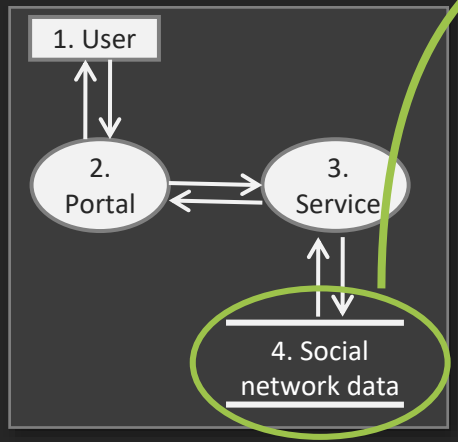
LINDDUN	L	I	N	D	D	U	N
Data store	X	X	X	X	X		X
Data flow	X	X	X	X	X		X
Process	X	X	X	X	X		X
Entity	X	X				X	

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

DistriNet

Privacy Threat Modeling Steps

Map



Map

Map the LINDDUN threat types to the model

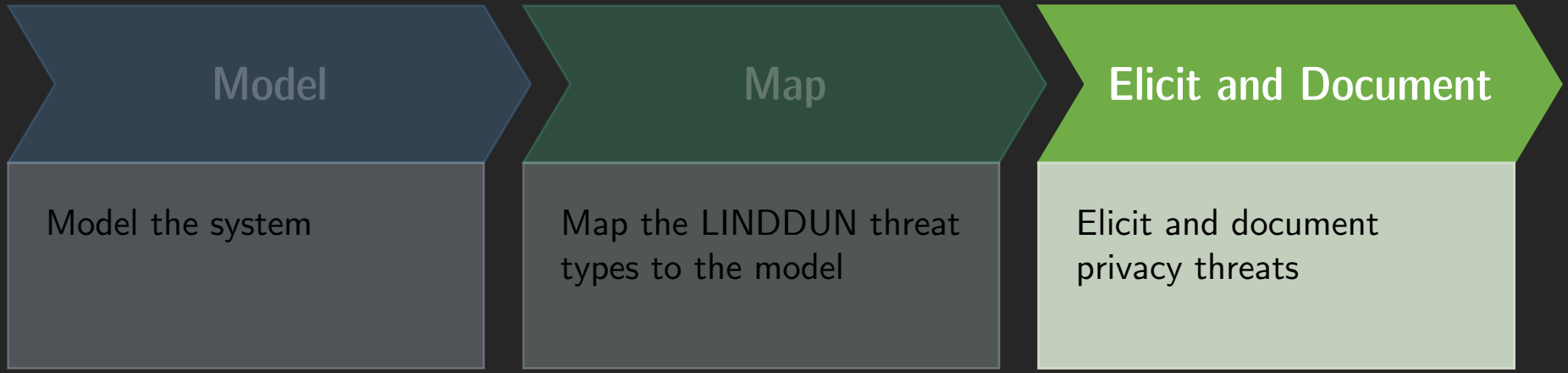
MAPPING TEMPLATE

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	

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

DistriNet

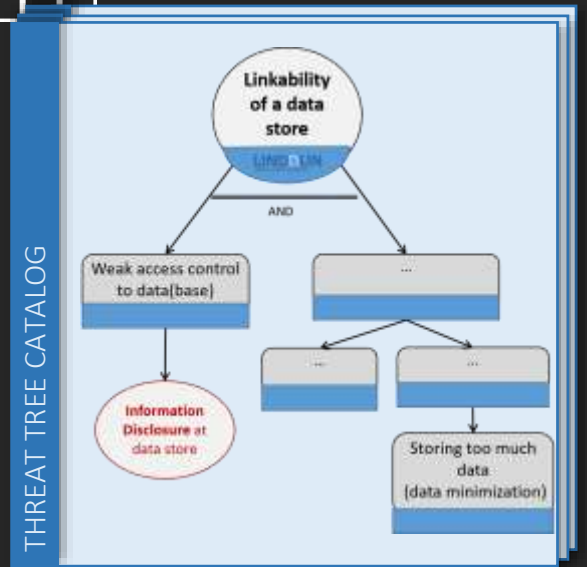
Privacy Threat Modeling Steps



Privacy Threat Modeling Steps

Elicit

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



Elicit and Document

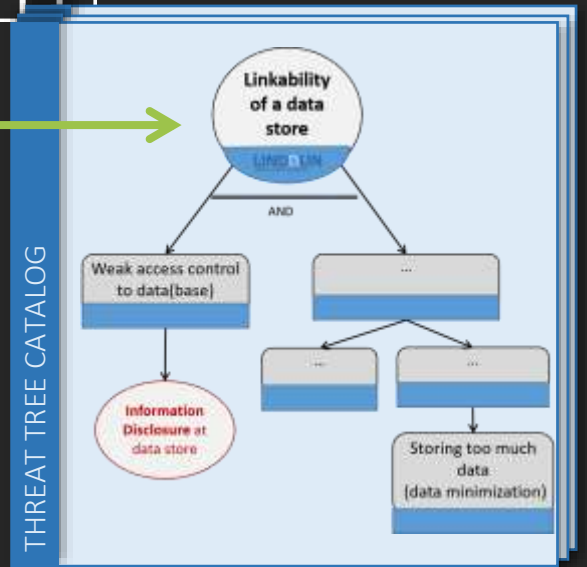
Elicit and document privacy threats

DistriNet

Privacy Threat Modeling Steps

Elicit

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

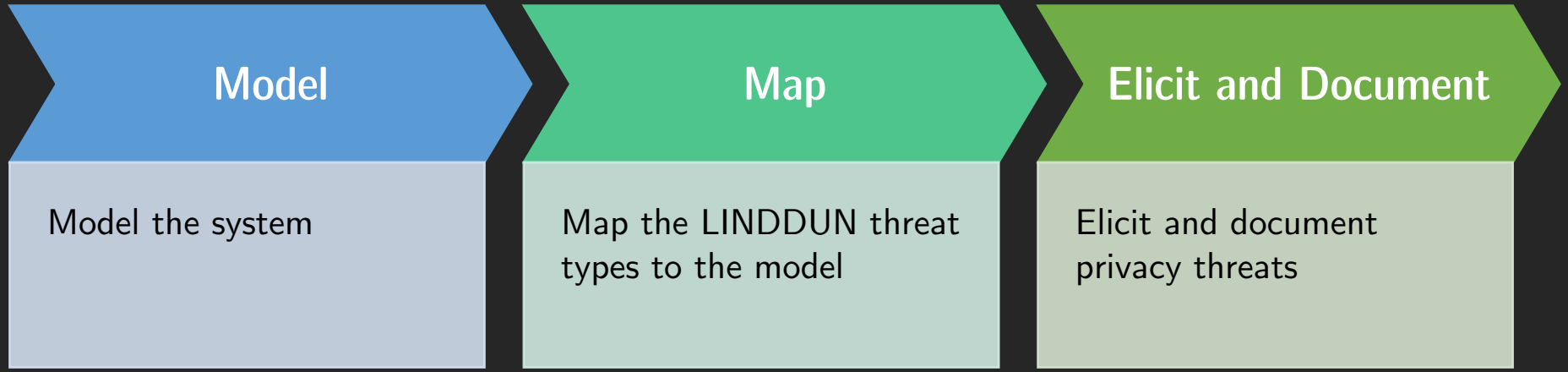


Elicit and Document

Elicit and document privacy threats

DistriNet

Privacy Threat Modeling Steps



The LINDDUN Privacy Framework

Linkability

Identifiability

Non-repudiation

Detectability

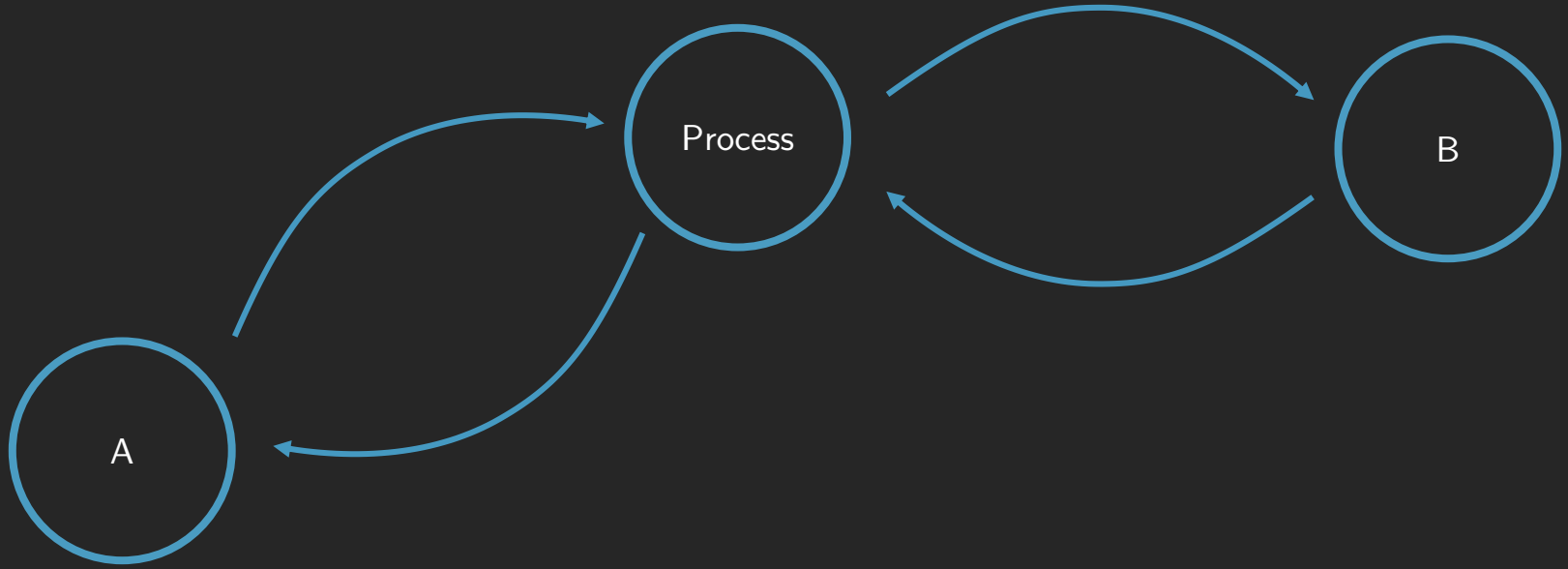
Disclosure of Information

Unawareness

Non-compliance

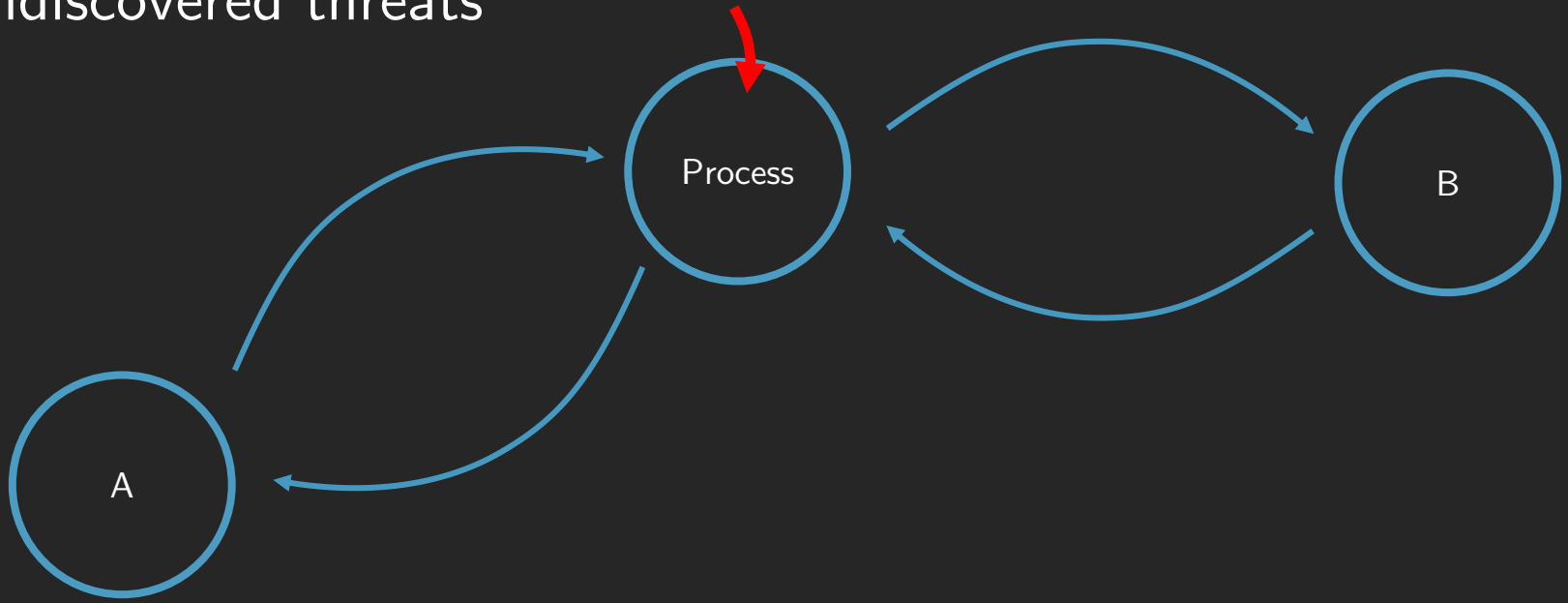
Issues with Element-Based Elicitation

› Undiscovered threats



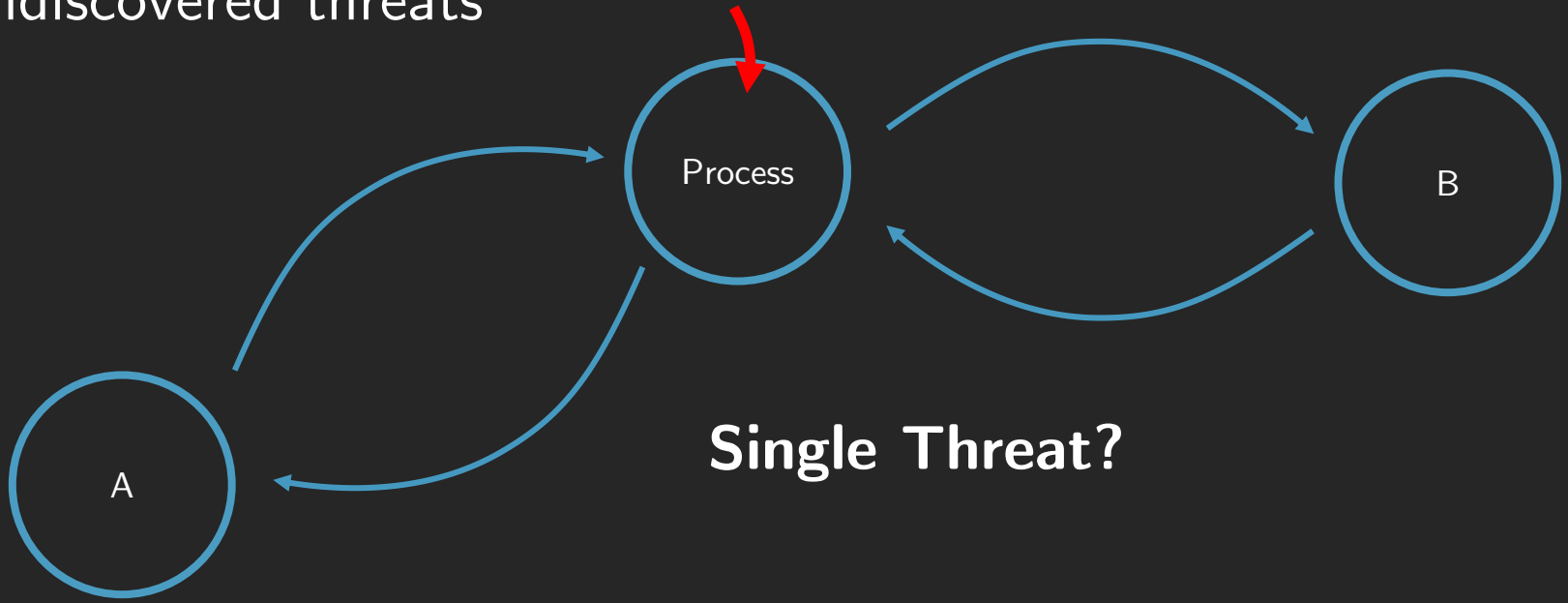
Issues with Element-Based Elicitation

› Undiscovered threats



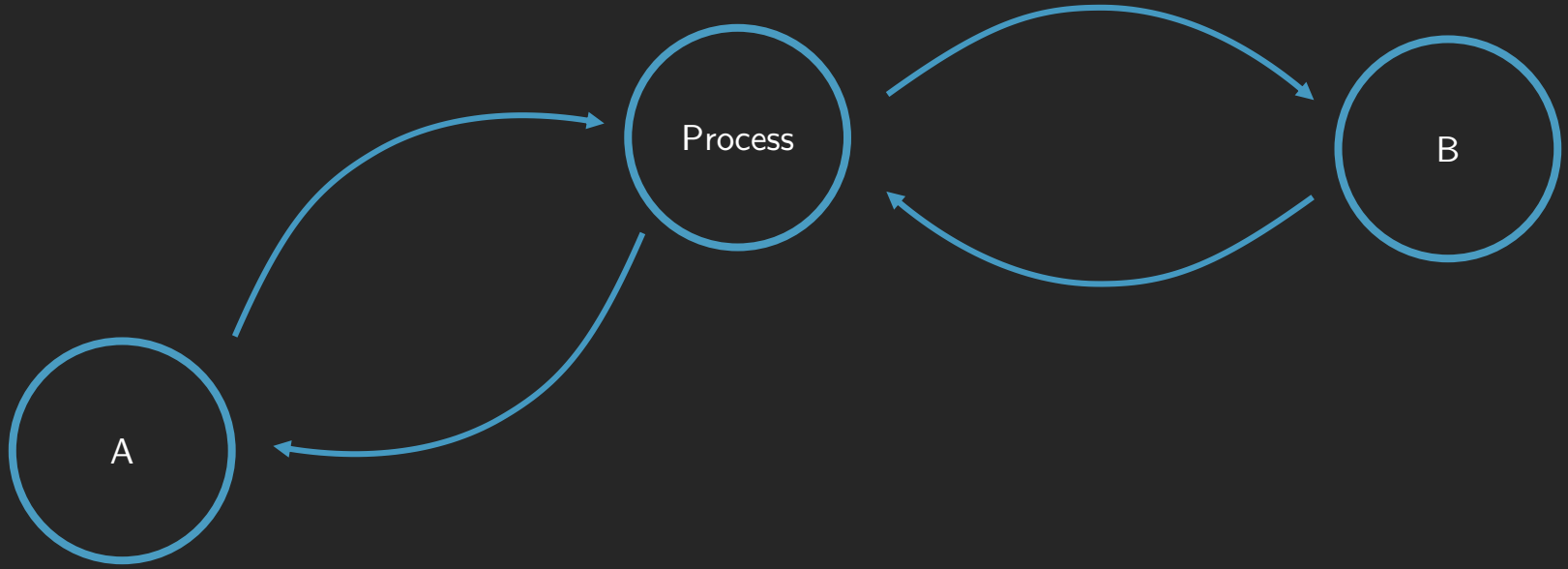
Issues with Element-Based Elicitation

› Undiscovered threats



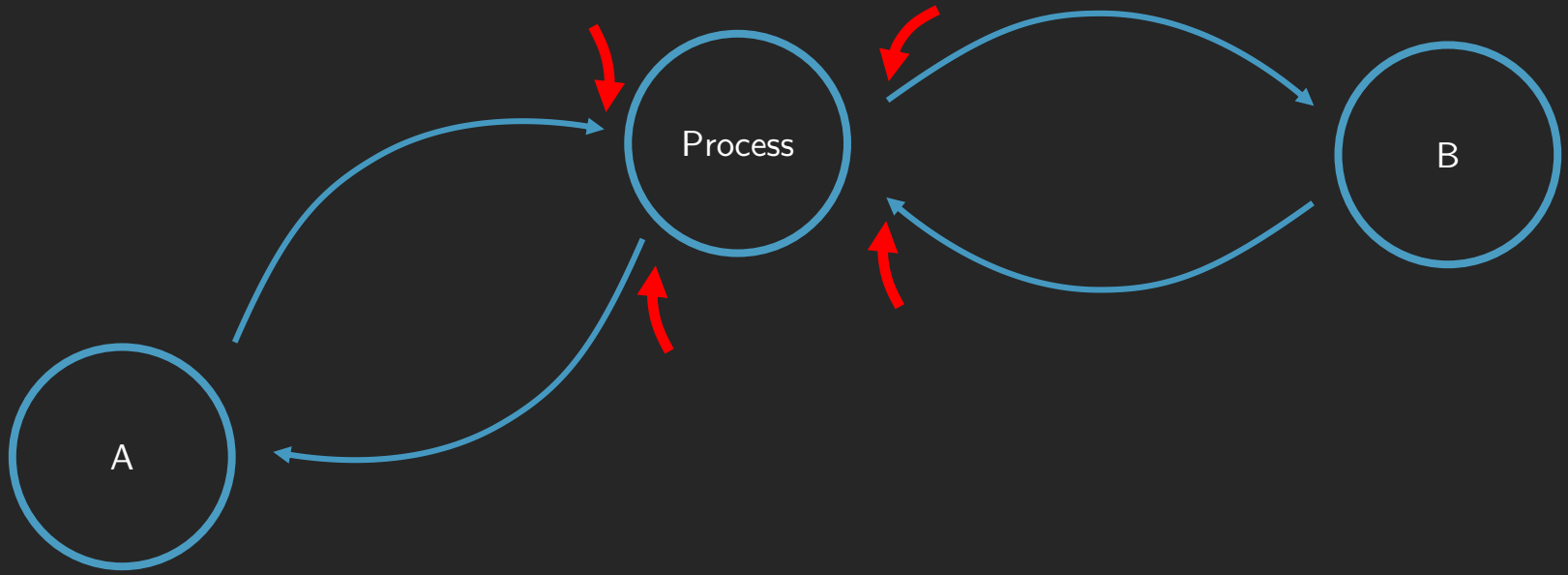
Issues with Element-Based Elicitation

› Undiscovered threats



Issues with Element-Based Elicitation

- Undiscovered threats



Issues with Element-Based Elicitation

- Undiscovered threats
- Inapplicable threats

Issues with Element-Based Elicitation

- Undiscovered threats
- Inapplicable threats

Issues with Element-Based Elicitation

- Undiscovered threats
- Inapplicable threats

Detectability threats on processes

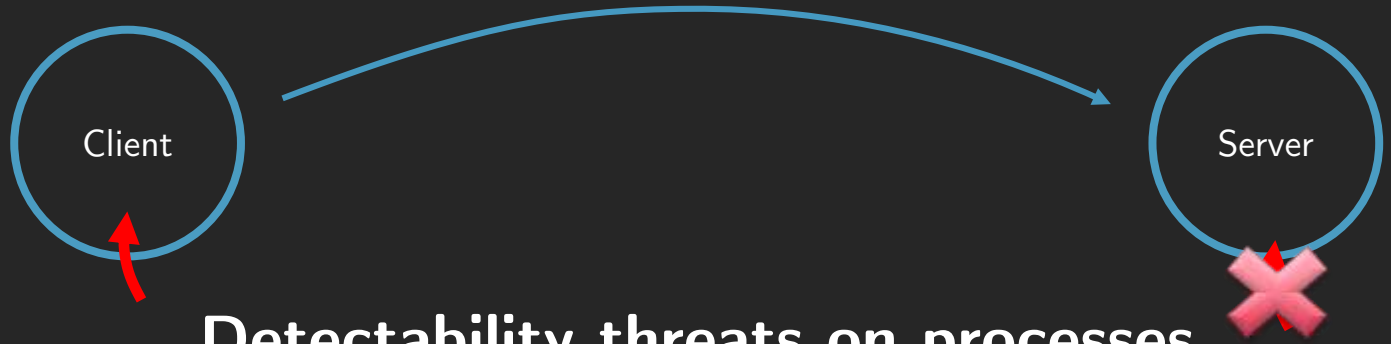
Issues with Element-Based Elicitation

- Undiscovered threats
- Inapplicable threats

Detectability threats on processes

Issues with Element-Based Elicitation

- Undiscovered threats
- Inapplicable threats



Detectability threats on processes

Issues with Element-Based Elicitation

- Undiscovered threats
- Inapplicable threats

Detectability threats on processes

Issues with Element-Based Elicitation

- Undiscovered threats
- Inapplicable threats
- Redundant threats

Issues with Element-Based Elicitation

- Undiscovered threats
- Inapplicable threats
- Redundant threats

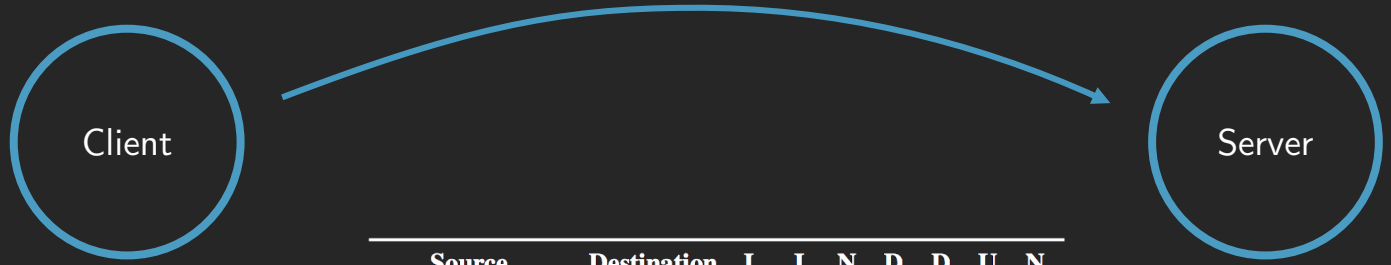
Detectability threats on processes

Element- vs. Interaction-based Elicitation

- Take local context into account
  - More explicit and precise
- Threats not caused by elements but through interactions
- $\#\{interactions\} < \#\{elements\}$
- Less or more threats?

- Lack of consensus on the most appropriate approach

Interaction-based LINDDUN



Source		Destination	L	I	N	D	D	U	N
Process		Process	X	X	X	X	X	–	X
Process		DataStore	X	X	X	X	X	–	X
Process	flow	ExternalEntity	X	X	X	X	X	–	X
DataStore		Process	X	X	X	X	X	–	X
ExternalEntity		Process	X	X	X	X	X	X	–
Process		***Process***	X	X	X	–	–	–	X
DataStore		***Process***	X	X	X	–	–	–	X
ExternalEntity	flow	***Process***	X	X	X	–	–	–	X
Process		***DataStore***	X	X	X	–	X	–	X
Process		***ExternalEntity***	X	X	X	–	–	X	X
Process		Process	X	X	X	X	X	–	–
Process		DataStore	X	X	X	X	X	–	–
Process	***flow***	ExternalEntity	X	X	X	X	X	–	–
DataStore		Process	X	X	X	X	X	–	–
ExternalEntity		Process	X	X	X	X	X	–	–

DistriNet

Interaction-based LINDDUN

Source		Destination	L	I	N	D	D	U	N
Process	flow	Process	X	X	X	X	X	–	X
Process		DataStore	X	X	X	X	X	–	X
Process		ExternalEntity	X	X	X	X	X	–	X
DataStore		Process	X	X	X	X	X	–	X
ExternalEntity		Process	X	X	X	X	X	X	–
Process	flow	***Process***	X	X	X	–	–	–	X
DataStore		***Process***	X	X	X	–	–	–	X
ExternalEntity		***Process***	X	X	X	–	–	–	X
Process		***DataStore***	X	X	X	–	X	–	X
Process		***ExternalEntity***	X	X	X	–	–	X	X
Process	***flow***	Process	X	X	X	X	X	–	–
Process		DataStore	X	X	X	X	X	–	–
Process		ExternalEntity	X	X	X	X	X	–	–
DataStore		Process	X	X	X	X	X	–	–
ExternalEntity		Process	X	X	X	X	X	–	–

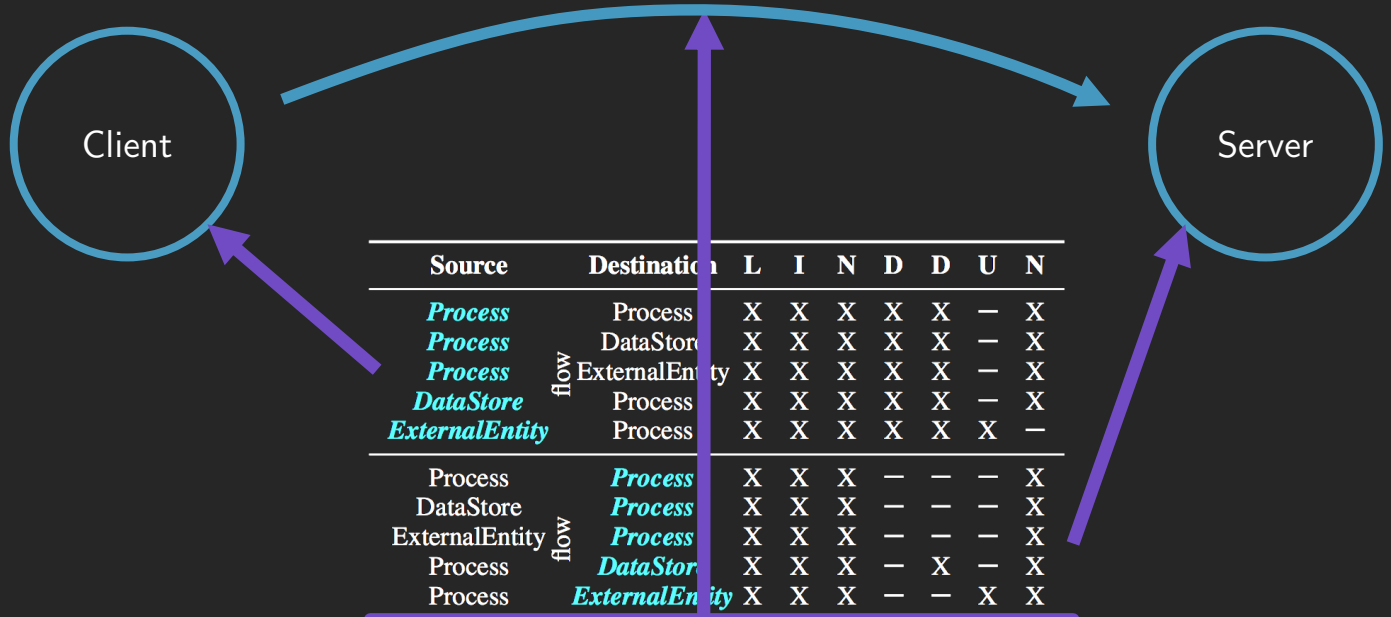
DistriNet

Interaction-based LINDDUN

Source		Destination	L	I	N	D	D	U	N
Process		Process	X	X	X	X	X	–	X
Process		DataStore	X	X	X	X	X	–	X
Process	flow	ExternalEntity	X	X	X	X	X	–	X
DataStore		Process	X	X	X	X	X	–	X
ExternalEntity		Process	X	X	X	X	X	X	–
Process		***Process***	X	X	X	–	–	–	X
DataStore		***Process***	X	X	X	–	–	–	X
ExternalEntity	flow	***Process***	X	X	X	–	–	–	X
Process		***DataStore***	X	X	X	–	X	–	X
Process		***ExternalEntity***	X	X	X	–	–	X	X
Process		Process	X	X	X	X	X	–	–
Process		DataStore	X	X	X	X	X	–	–
Process	***flow***	ExternalEntity	X	X	X	X	X	–	–
DataStore		Process	X	X	X	X	X	–	–
ExternalEntity		Process	X	X	X	X	X	–	–

DistriNet

Interaction-based LINDDUN



Source		Destination	L	I	N	D	D	U	N
Process	flow	Process	X	X	X	X	X	–	X
Process	flow	DataStore	X	X	X	X	X	–	X
Process	flow	ExternalEntity	X	X	X	X	X	–	X
DataStore	flow	Process	X	X	X	X	X	–	X
ExternalEntity	flow	Process	X	X	X	X	X	X	–
Process	flow	***Process***	X	X	X	–	–	–	X
DataStore	flow	***Process***	X	X	X	–	–	–	X
ExternalEntity	flow	***Process***	X	X	X	–	–	–	X
Process	flow	***DataStore***	X	X	X	–	X	–	X
Process	flow	***ExternalEntity***	X	X	X	–	–	X	X
Process	***flow***	Process	X	X	X	X	X	–	–
Process	***flow***	DataStore	X	X	X	X	X	–	–
Process	***flow***	ExternalEntity	X	X	X	X	X	–	–
DataStore	***flow***	Process	X	X	X	X	X	–	–
ExternalEntity	***flow***	Process	X	X	X	X	X	–	–

DistriNet

Source		Destination	L	I	N	D	D	U	N
Process	flow	Process	X	X	X	X	X	—	X
Process		DataStore	X	X	X	X	X	—	X
Process		ExternalEntity	X	X	X	X	X	—	X
DataStore		Process	X	X	X	X	X	—	X
ExternalEntity		Process	X	X	X	X	X	X	—
Process	flow	***Process***	X	X	X	—	—	—	X
DataStore		***Process***	X	X	X	—	—	—	X
ExternalEntity		***Process***	X	X	X	—	—	—	X
Process		***DataStore***	X	X	X	—	X	—	X
Process		***ExternalEntity***	X	X	X	—	—	X	X
Process	***flow***	Process	X	X	X	X	X	—	—
Process		DataStore	X	X	X	X	X	—	—
Process		ExternalEntity	X	X	X	X	X	—	—
DataStore		Process	X	X	X	X	X	—	—
ExternalEntity		Process	X	X	X	X	X	—	—

DistriNet

Source		Destination	L	I	N	D	D	U	N
Process	flow	Process	X	X	X	X	X	—	X
Process		DataStore	X	X	X	X	X	—	X
Process		ExternalEntity	X	X	X	X	X	—	X
DataStore		Process	X	X	X	X	X	—	X
ExternalEntity		Process	X	X	X	X	X	X	—
Process	flow	***Process***	X	X	X	—	—	—	X
DataStore		***Process***	X	X	X	—	—	—	X
ExternalEntity		***Process***	X	X	X	—	—	—	X
Process		***DataStore***	X	X	X	—	X	—	X
Process		***ExternalEntity***	X	X	X	—	—	X	X
Process	***flow***	Process	X	X	X	X	X	—	—
Process		DataStore	X	X	X	X	X	—	—
Process		ExternalEntity	X	X	X	X	X	—	—
DataStore		Process	X	X	X	X	X	—	—
ExternalEntity		Process	X	X	X	X	X	—	—

DistriNet

Source		Destination	L	I	N	D	D	U	N
Process	flow	Process	X	X	X	X	X	—	X
Process		DataStore	X	X	X	X	X	—	X
Process		ExternalEntity	X	X	X	X	X	—	X
DataStore		Process	X	X	X	X	X	—	X
ExternalEntity		Process	X	X	X	X	X	X	—
Process	flow	***Process***	X	X	X	—	—	—	X
DataStore		***Process***	X	X	X	—	—	—	X
ExternalEntity		***Process***	X	X	X	—	—	—	X
Process		***DataStore***	X	X	X	—	X	—	X
Process		***ExternalEntity***	X	X	X	—	—	X	X
Process	***flow***	Process	X	X	X	X	X	—	—
Process		DataStore	X	X	X	X	X	—	—
Process		ExternalEntity	X	X	X	X	X	—	—
DataStore		Process	X	X	X	X	X	—	—
ExternalEntity		Process	X	X	X	X	X	—	—

DistriNet

Source		Destination	L	I	N	D	D	U	N
Process	flow	Process	X	X	X	X	X	—	X
Process		DataStore	X	X	X	X	X	—	X
Process		ExternalEntity	X	X	X	X	X	—	X
DataStore		Process	X	X	X	X	X	—	X
ExternalEntity		Process	X	X	X	X	X	X	—
Process	flow	*Process*	X	X	X	—	—	—	X
DataStore		*Process*	X	X	X	—	—	—	X
ExternalEntity		*Process*	X	X	X	—	—	—	X
Process		*DataStore*	X	X	X	—	X	—	X
Process		*ExternalEntity*	X	X	X	—	—	X	X
Process	*flow*	Process	X	X	X	X	X	—	—
Process		DataStore	X	X	X	X	X	—	—
Process		ExternalEntity	X	X	X	X	X	—	—
DataStore		Process	X	X	X	X	X	—	—
ExternalEntity		Process	X	X	X	X	X	—	—

DistriNet

LINDDUN Examples

- Full LINDDUN table of threats

LINDDUN Examples

- Full LINDDUN table of threats
- Concrete examples

LINDDUN Examples

Source		Destination	L	I	N	D	D	U	N
Process		Process	X	X	X	X	X	–	X
Process		DataStore	X	X	X	X	X	–	X
ExternalEntity		Process	X	X	X	X	X	X	
Process		*Process*	X	X	X	–	–	–	X
DataStore		*Process*	X	X	X	–	–	–	X
ExternalEntity	flow	*Process*	X	X	X	–	–	–	X
Process		*DataStore*	X	X	X	–	X	–	X
Process		*ExternalEntity*	X	X	X	–	–	X	X
Process		Process	X	X	X	X	X	–	–
Process		DataStore	X	X	X	X	X	–	–
Process	*flow*	ExternalEntity	X	X	X	X	X	–	–
DataStore		Process	X	X	X	X	X	–	–
ExternalEntity		Process	X	X	X	X	X	–	–

Website (S) showing incorrect password error reveals account existence.

Qualities

- Expressivity

Qualities

- Expressivity
- Elimination of inapplicable threat types

Qualities

- Expressivity
- Elimination of inapplicable threat types
- Finding undiscovered threats

Qualities

- Expressivity
- Elimination of inapplicable threat types
- Finding undiscovered threats
- Effort-precision trade-off

Discussion

- Semantics and ambiguities of privacy threats

Discussion

- Semantics and ambiguities of privacy threats
- Threat trees

Discussion

- Semantics and ambiguities of privacy threats
- Threat trees
- Usage & tool support

Discussion

- Semantics and ambiguities of privacy threats
- Threat trees
- Usage & tool support
- Granularity for threat elicitation

Conclusion

- Element-based elicitation is sub-optimal

Conclusion

- Element-based elicitation is sub-optimal
- Interaction-based LINDDUN extension

Conclusion

- Element-based elicitation is sub-optimal
- Interaction-based LINDDUN extension
- Provide detailed LINDDUN interaction examples

Conclusion

- Element-based elicitation is sub-optimal
- Interaction-based LINDDUN extension
- Provide detailed LINDDUN interaction examples
- Beyond interaction-based: to DFD patterns

Conclusion

- Element-based elicitation is sub-optimal
- Interaction-based LINDDUN extension
- Provide detailed LINDDUN interaction examples
- Beyond interaction-based: to DFD patterns

Questions?

Thank you!

Interaction-Based Privacy Threat Elicitation

Laurens Sion, Kim Wuyts, Koen Yskout, Dimitri Van Landuyt, Wouter Joosen

DistriNet