

# Privacy threat analysis

Mina Deng,

Kim Wuyts, Riccardo Scandariato,

Bart Preneel, Wouter Joosen

# Objectives

- Understanding the nature of privacy requirements and their relationship with anti-requirements
- Method to elicit privacy anti-requirements (LINDDUN)
- Documenting privacy threats

# Overview



- Privacy
  - What?
  - Properties
- Privacy methodology
- Example case study
- Project information

# Privacy

- what is privacy?
  - Confidentiality
  - Data minimization
  - User empowerment
  - ...



# What is privacy?

- The right to be let alone (*Warren & Brandeis, 1890*)
- The right of the individual to decide what information about himself should be communicated to others and under what circumstances (*Westin, 1970*)
- Freedom from unreasonable constraints on the construction of one's own identity (*Agre & Rotenberg, 2001*)

# People don't care about online privacy?

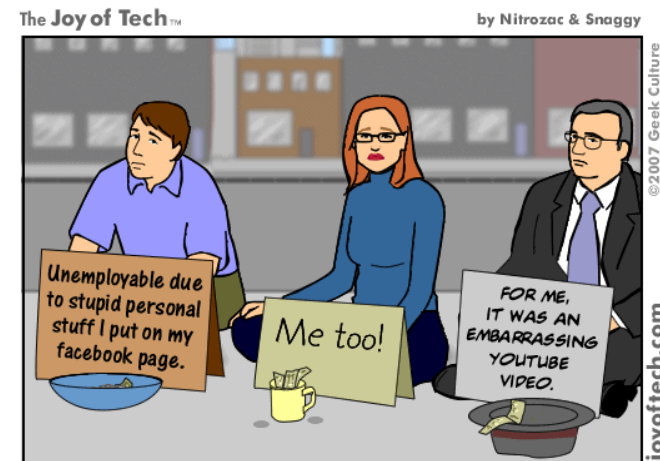
- In the “real world”: concerned about information we share
  - Who they tell what
    - You might be willing to tell your best friend that you had an argument with your girlfriend, but you don't want everybody to know about it
  - Concerns over information taken out of context
    - A picture taken at a crazy party being available to a potential employer
  - We value friends who are discreet and keep our secrets
    - We give more information to people we trust
  - The cost of gathering and analyzing information without advanced technologies has guaranteed that we had a rather high level of privacy protection

# People don't care about online privacy?

- Online:
  - less concerned or unaware of privacy violations
- This information is not necessarily secret, but would you want to broadcast it?
  - Identity attributes ( Name, age, gender, race, IQ, marital status, place of birth, address, phone number, ID number...)
  - Location (Where you are at a certain point in time, movement patterns)
  - Interests / preferences (Books you read, music you listen, films you like, sports you practice, political affiliation, religious beliefs, sexual orientation)
  - Behavior (Personality type, what you eat, what you shop, how you behave and interact with others)
  - Social network (Who your friends are, who you meet when, your different social circles)
  - Health data (Medical issues, treatments you follow, DNA, health risk factors)
  - Financial data (How much you earn, how you spend your money, credit card number, bank account)
- Combination of them all is even more troublesome

# Privacy problems

- Identity theft
  - Getting a credit card on your name
- Stalking
- Profiling
  - Find compulsive buyers, ...
- Sensitive information being shared
- Information taken out of context

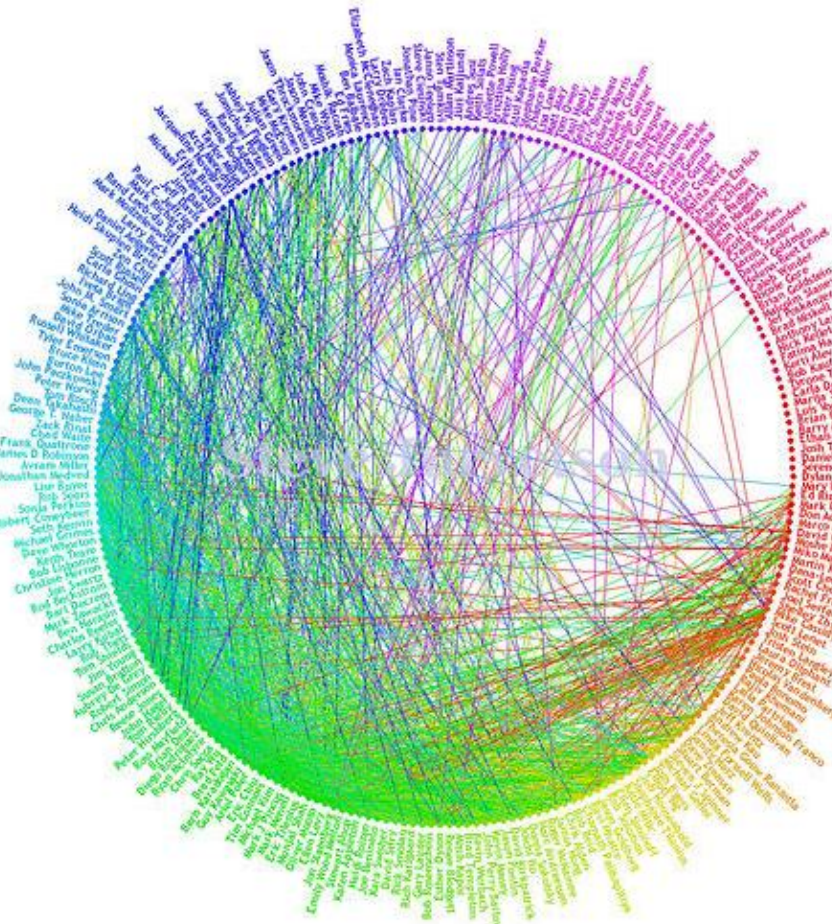


Signs of the social networking times.



# Gaydar Algorithm Outs Facebook Users

By Susannah F. Locke Posted 09.21.2009 at 12:27 pm 12 Comments



A pair of MIT students claim that they have created an algorithm that outs gay members of Facebook by analyzing the sexual orientations of their networks of friends.

The students first analyzed the networks of people who publicized their sexual orientation on Facebook. Turns out that statistically speaking, gay men have more gay friends than straight guys do. So then, they used an algorithm to run the stats on men who kept mum about their sexual orientation on the site. Their computer program was able to correctly identify 10 men whom the students personally knew to be gay in the real world but who hadn't shared that fact on Facebook. (The algorithm didn't work as well with women or with bisexual Facebookers.)

The students completed the project for a class on ethics and the Internet and hope to publish it in a scientific journal.

Their project is far from the first study showing that a simple computer program can sleuth out details you might prefer to keep private by looking at your social network on the Internet. Earlier this year, computer scientists correctly linked 30 percent of anonymous Twitter and Flickr accounts with a simple [algorithm](#) that compares who's following who on each site. And other researchers have used Internet social networks to correctly identify peoples' political affiliations or where they live.

It's a good reminder to take a look at your privacy settings. Because you might inadvertently be sharing things you'd rather keep to yourself. Even if you're only declaring to the world that someone's your friend.

What are your friends saying about you? Online social networks like this Facebook one tell more about you than you think [jurvetson](#) (CC licensed)

# Spear-phishing

- Using personal information to make phishing more successful

From info@cs.kuleuven.be <reid.frey@gpaea.k12.ia.us>☆

Subject "cs.kuleuven.be" IT HELP DESK

Reply to helpdesk@cs.kuleuven.be <help-desk@email.com>☆

To undisclosed-recipients;☆

13/01/2012 12:11

Other Actions ▾

Reply Forward Archive Junk Delete

Dear 'cs.kuleuven.be' E-mail User,

We are currently upgrading our database and all account need to be verified. To complete your account activation with us, you are required to reply to this message and enter your password in the space provided (\*\*\*\*\*) you are required to do this before the next 48 hours of the receipt of this email or your database will be de-activated from our database.

Full Name:

username:

Password:

Thank you for using cs.kuleuven.be

Copyright 2012 © cs.kuleuven.be web Team.

- Using Facebook data



[Hey Peter](#)

Hot singles are waiting for you!!

# Freddi Staur

- 41% agreed to be friends with Freddi which (often) led to access to
  - Email address
  - Full date of birth
  - Details on education and workplace
  - Current address
  - Pictures of family and friends
  - Name of their partner / relatives



The image shows a screenshot of a Facebook profile for a user named 'Freddi Staur'. The profile picture is a green and yellow frog figurine. The profile information includes: Networks: London; Sex: Male; Interested In: Women; Relationship Status: Single; Birthday: June 4, 1900. The Mini-Feed shows several friend requests, including one from 'London Friends' with 12 pending requests. The left sidebar shows the Facebook search bar and navigation menu with options like Photos, Groups, Events, and Marketplace.

facebook Profile edit Friends Networks Inbox home account privacy logout

Search find friends

Applications edit

- Photos
- Groups
- Events
- Marketplace
- more

**Freddi Staur** Profile

Update your status...

Networks: London  
Sex: Male  
Interested In: Women  
Relationship Status: Single  
Birthday: June 4, 1900

▼ Mini-Feed  
Displaying 10 stories. See All

Yesterday

- Freddi and [User] are now friends. x
- Freddi and [User] are now friends. x

August 7

- Freddi and [User] are now friends. 12 x
- Freddi and [User] are now friends. x

Edit My Profile

▼ London Friends  
6 friends in London. See All

# Privacy properties

- Unlinkability
- Anonymity/ pseudonymity
- Plausible deniability
- Undetectability
  
- Confidentiality
  
- Content awareness
- Policy and consent compliance

Hard privacy

Security

Soft privacy

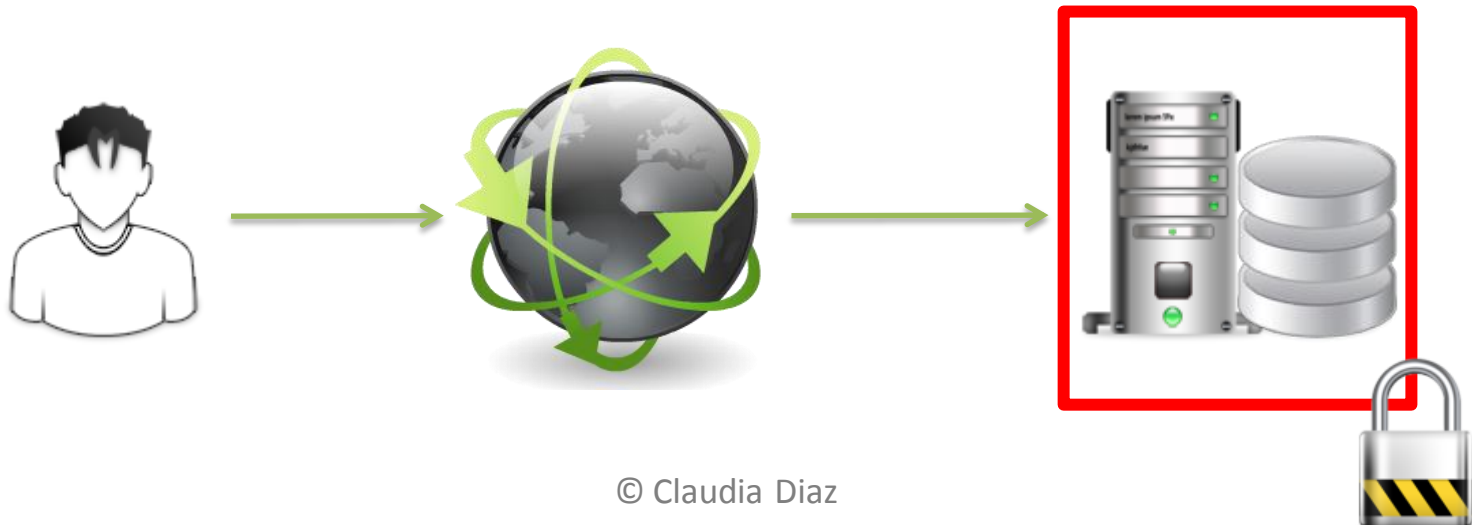
# Hard privacy

- Data minimization
  - Subject provides as little data as possible
  - Reduce as much as possible the need to “trust” other entities



# Soft privacy

- Data subject has already lost control of her data
  - In practice, very difficult for data subject to verify how her data are collected and processed



# Soft privacy

- Need to trust data controllers (honesty, competence)



# Privacy

Anonymity &  
Pseudonymity

## ***Anonymity***

*An attacker cannot sufficiently identify the subject within a set of subjects, the anonymity set*



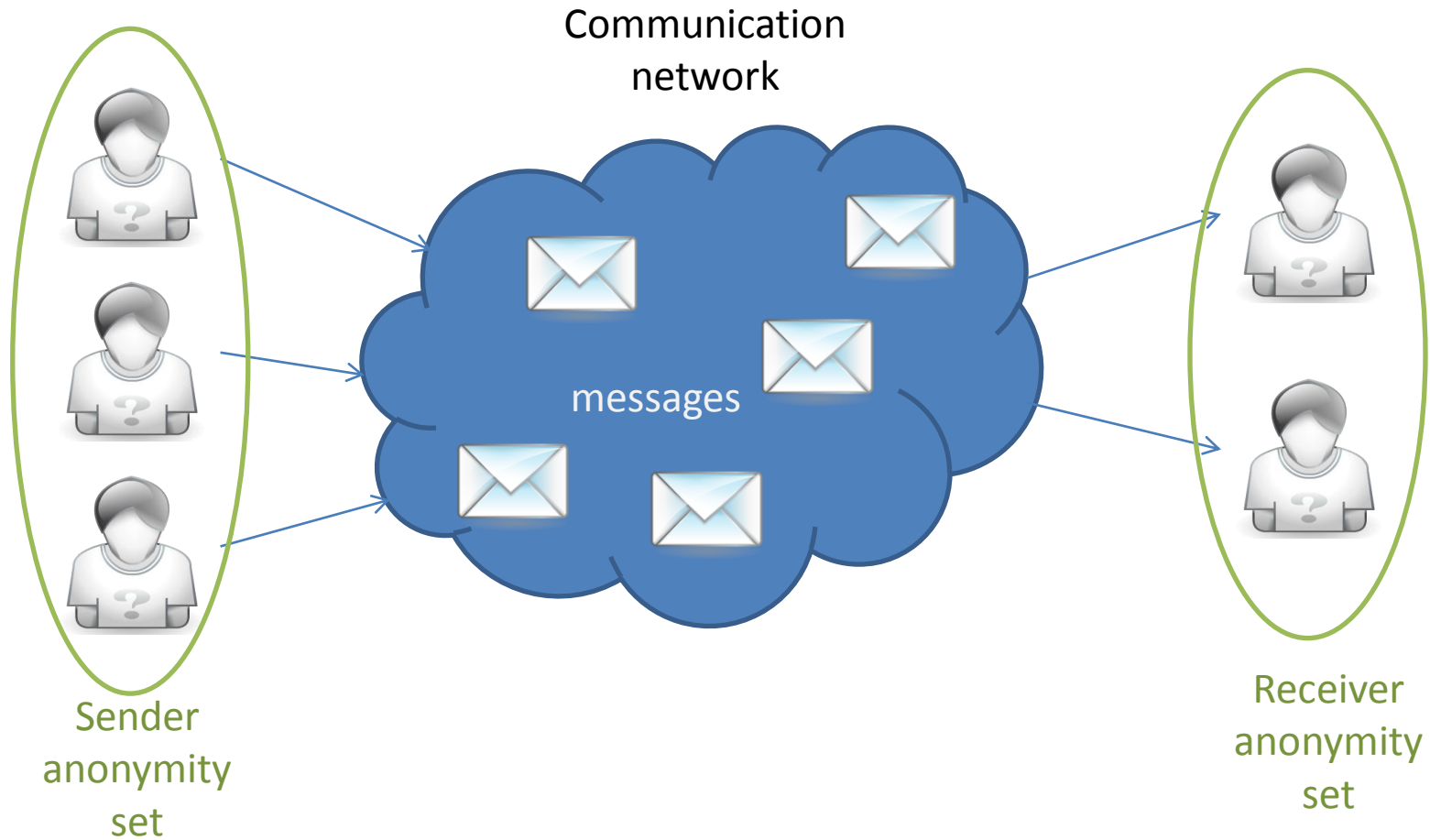


# Anonymity

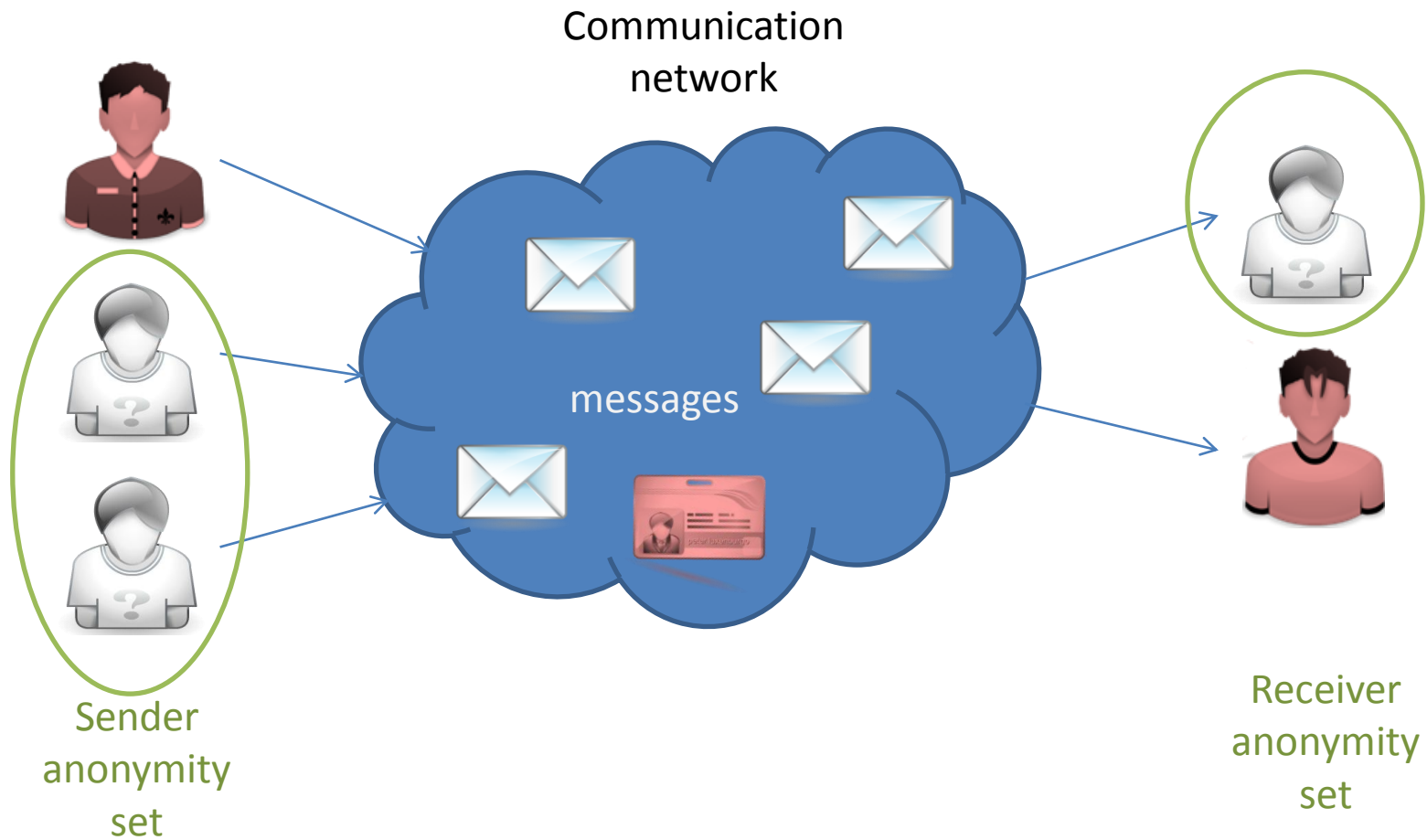
- *An attacker cannot sufficiently identify the subject within a set of subjects, the anonymity set (Pfitzmann)*
- Hiding link between identity and action / piece of information.
- Examples:
  - Reader of a web page, person accessing a service
  - Sender of an email, writer of a text
  - Person to whom an entry in a database relates
  - Person present in a physical location



# Anonymity set



# Anonymity set wrt **attacker**



# Identifiability

- *The attacker can sufficiently identify the subject within a set of subjects, the identifiability set (pfitzmann)*
- A identity is any subset of attribute values of an individual personal which sufficiently identifies this individual person with any set of persons.
  - There can thus be many “identities”

# Identifiability example

- Browser uniqueness

## Panoptick

How Unique – and Trackable – Is Your Browser?

Your browser fingerprint **appears to be unique** among the 2,123,272 tested so far.

Currently, we estimate that your browser has a fingerprint that conveys **at least 21.02 bits of identifying information**.

The measurements we used to obtain this result are listed below. You can read more about our methodology, statistical results, and some defenses against fingerprinting in [this article](#).

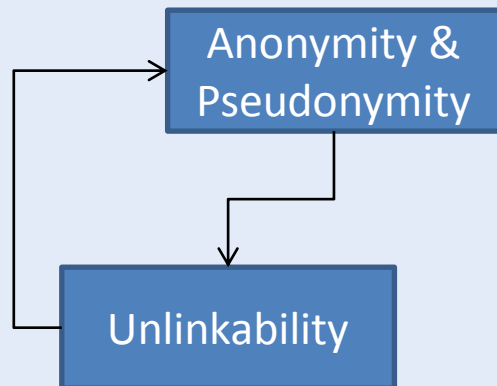
<http://panoptick.eff.org/>

- Possible to track “anonymous” visitors

# Pseudonymity

- *A pseudonym is an identifier of a subject other than one of the subjects real names.  
Pseudonymity is the use of pseudonyms as identifiers. (Pfitzmann)*
- Pseudonymity is the entire field between anonymity and identifiability

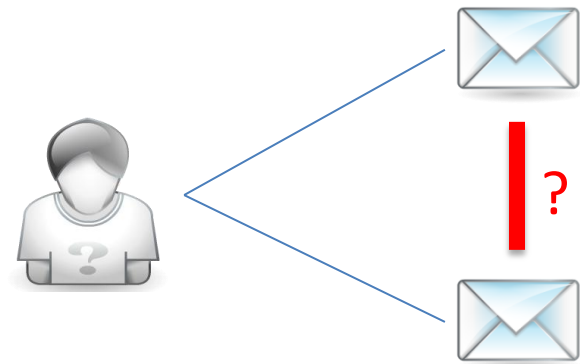
# Privacy



→ requires

## ***Unlinkability***

*Within a system, the attacker cannot sufficiently distinguish whether two or more items of interest (IOI) are related or not*

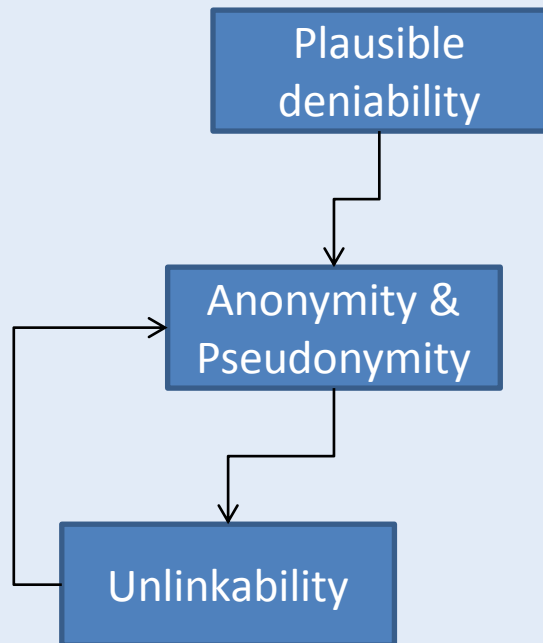


# Unlinkability

- *Within a system, the attacker cannot sufficiently distinguish whether two or more items of interest (IOI) are related or not (Pfitzman)*
- Hiding link between two or more actions / identities / pieces of information
- Examples:
  - Two anonymous letters written by the same person
  - Two web page visits by the same user
  - Entries in two databases related to the same person
  - Two people related by a friendship link
  - Same person spotted in two locations at different points in time



# Privacy



→ requires

## *Plausible deniability*

Not possible to prove user knows, has done or has said something

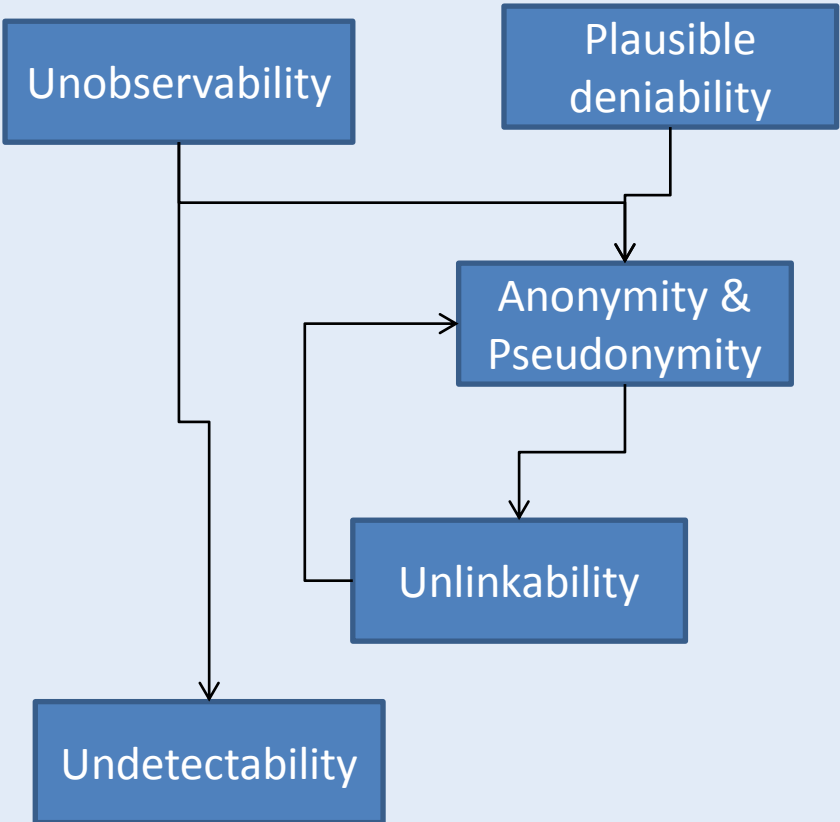


# Plausible deniability

- Not possible to prove user knows, has done or has said something
- Examples:
  - Resistance to coercion:
    - Not possible to prove that a person has hidden information in a computer
    - Not possible to know that someone has the combination of a safe
  - Possibility to deny having been in a place at a certain point in time
  - Possibility to deny that a database record belongs to a person
  - Off-the-record conversations

# Privacy

## Hard privacy



→ requires

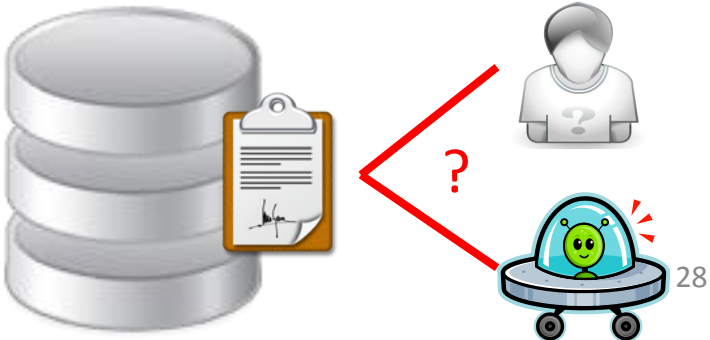
## Undetectability

*The attacker cannot sufficiently distinguish whether it exists or not*



## Unobservability

*undetectability + anonymity of subjects involved in the IOI even against the other subjects involved in that IOI*

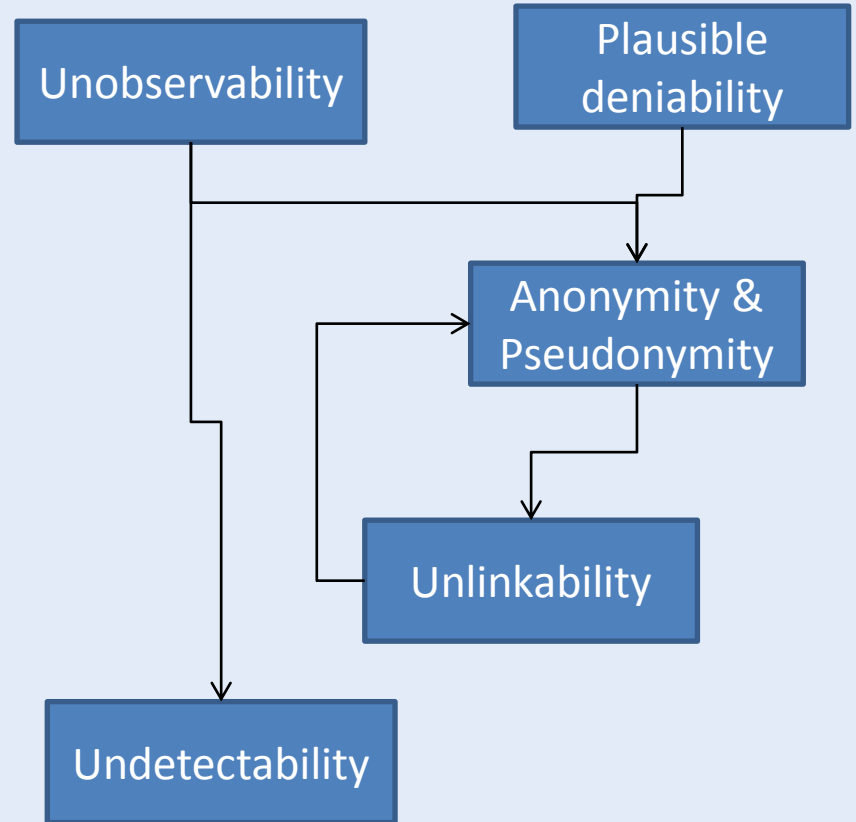


# Undetectability & Unobservability

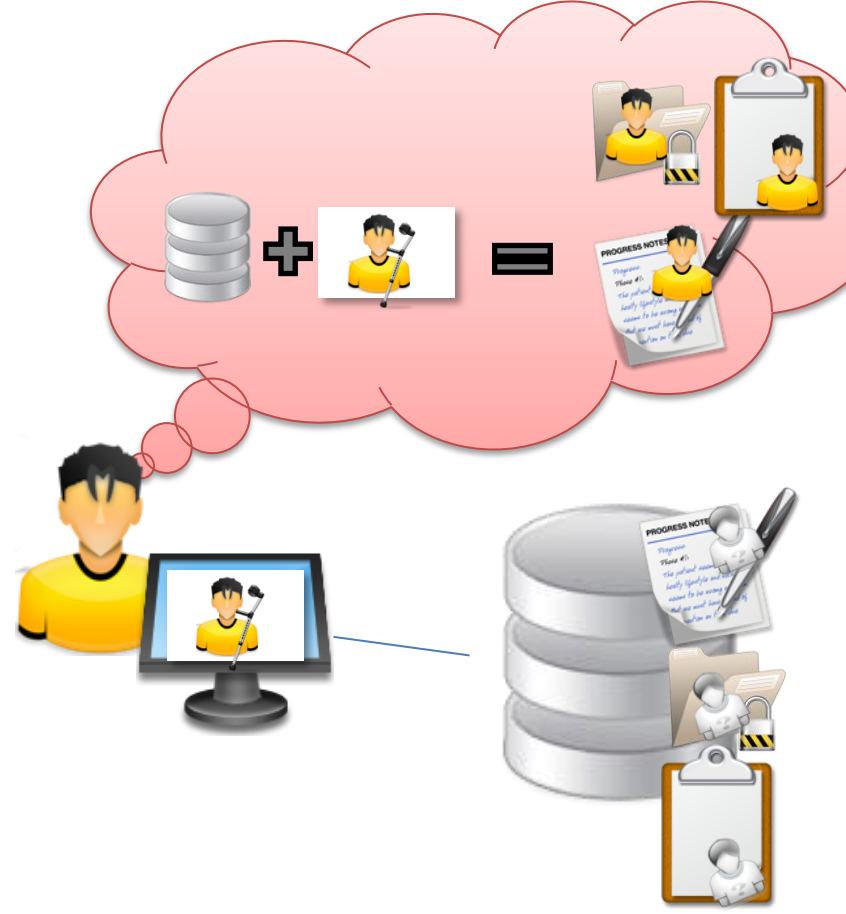
- *Undetectability: The attacker cannot sufficiently distinguish whether it exists or not (Pfitzmann)*
- *Unobservability: undetectability + anonymity of subjects involved in the IOI even against the other subjects involved in that IOI (Pfitzmann)*
- Hiding user activity
- Examples:
  - Impossible to see whether someone is accessing a web page
  - Impossible to know whether an entry in a database corresponds to a real person
  - Impossible to distinguish whether someone or no one is in a given location

# Privacy

## Hard privacy



→ requires




User awareness

### ***User awareness***

*Users are aware of the consequences of sharing information*

# Content Awareness

- Users should be made aware of the consequences of sharing information
- Suggested solution: Feedback & awareness tools


 **Rob** [redacted] Weird discovery of the day. If you type a word in Facebook (in a comment, status, etc.) that happens to be the same as your password, after you click "Share," Facebook automatically converts it to asterisks to protect your security. Allow me to demonstrate. My password is \*\*\*\*\*.  
3 hours ago · Comment · Like



 **Liesl** [redacted] \*\*\*\*\*  
2 hours ago

 **Liesl** [redacted] Weird! It totally works.  
2 hours ago

 **Jeremy** [redacted] megaman3  
2 hours ago


 **Heather** [redacted] iheartbieber  
2 hours ago

 **Sandi** [redacted] my password is 76trombones  
2 hours ago

 **B** [redacted]  
Guess who just got a CREDIT CARDDD!!!! :) :) :)  




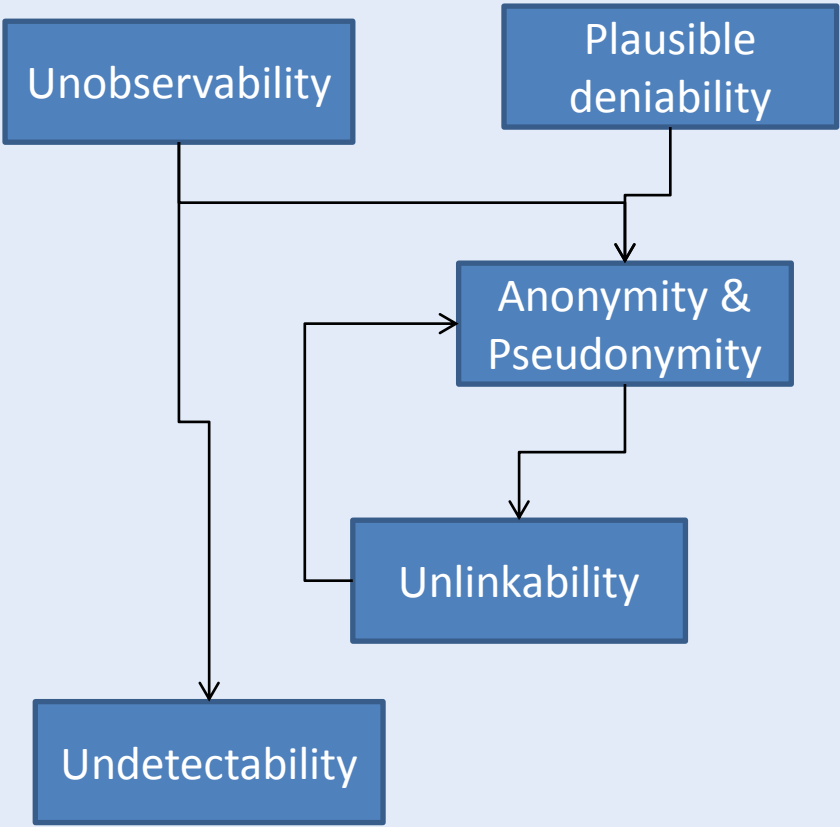
 24 minutes ago · Like · Comment · Share

 **G** [redacted] And guess who now has your credit card number???  
20 minutes ago · Like

 **G** [redacted] Me...and all 269 of the rest of your friends. You should probably take this down.  
19 minutes ago · Unlike ·  2 people

# Privacy

## Hard privacy



→ requires

DIRECTIVE 2002/58/EC OF THE EUROPEAN PARLIAMENT AND OF THE COUNCIL of 12 July 2002 concerning the processing of personal data and the protection of privacy in the electronic communications sector (Directive on privacy and electronic communications)

**Safer Social Networking Principles for the EU**

Directive 95/46/EC of the European Parliament and of the Council of 24 October 1995 on the protection of individuals with regard to the processing of personal data and on the free movement of such data



User awareness

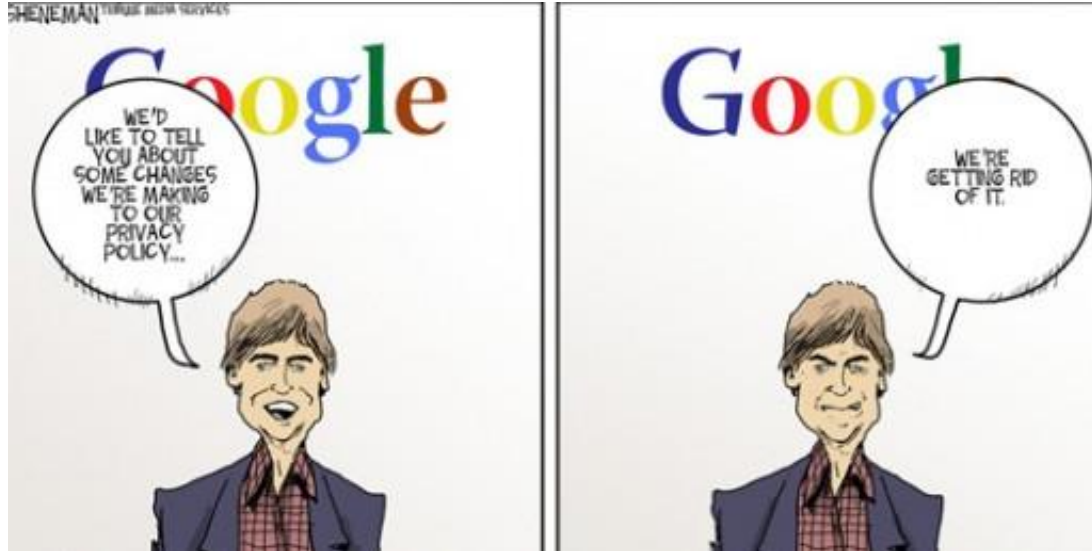
Compliance

### Compliance

*Legal compliance is obligated. e.g. consents*

# Policy & Consent compliance

- Policies
  - Corporate
  - Privacy



- Openness to users + control





# Policy & Consent compliance

- Legal compliance is obligated
  - E.g. European Data Protection Directive
    - fair and lawful processing
    - information quality
    - Consent
    - data subject control
    - purpose specification
    - sensitivity
    - minimality
    - information security
    - minimal disclosure



# Compliance example: User consent

- ***personal data*** = any information relating to an identified or identifiable natural person ("data subject")
- **Sensitive data** = personal data revealing racial or ethnic origin, political opinions, religious or philosophical beliefs, trade-union membership, and the processing of data concerning health or sex life
- Processing of **sensitive data** *prohibited* unless
  - the processing is necessary for the protection of the vital interests of the data subject,
  - the processing is necessary for purposes of preventive medicine, medical diagnosis, provision of care or treatment or
  - the data subject has given his **explicit, written consent** to the processing of the data
  - ...(art. 7)

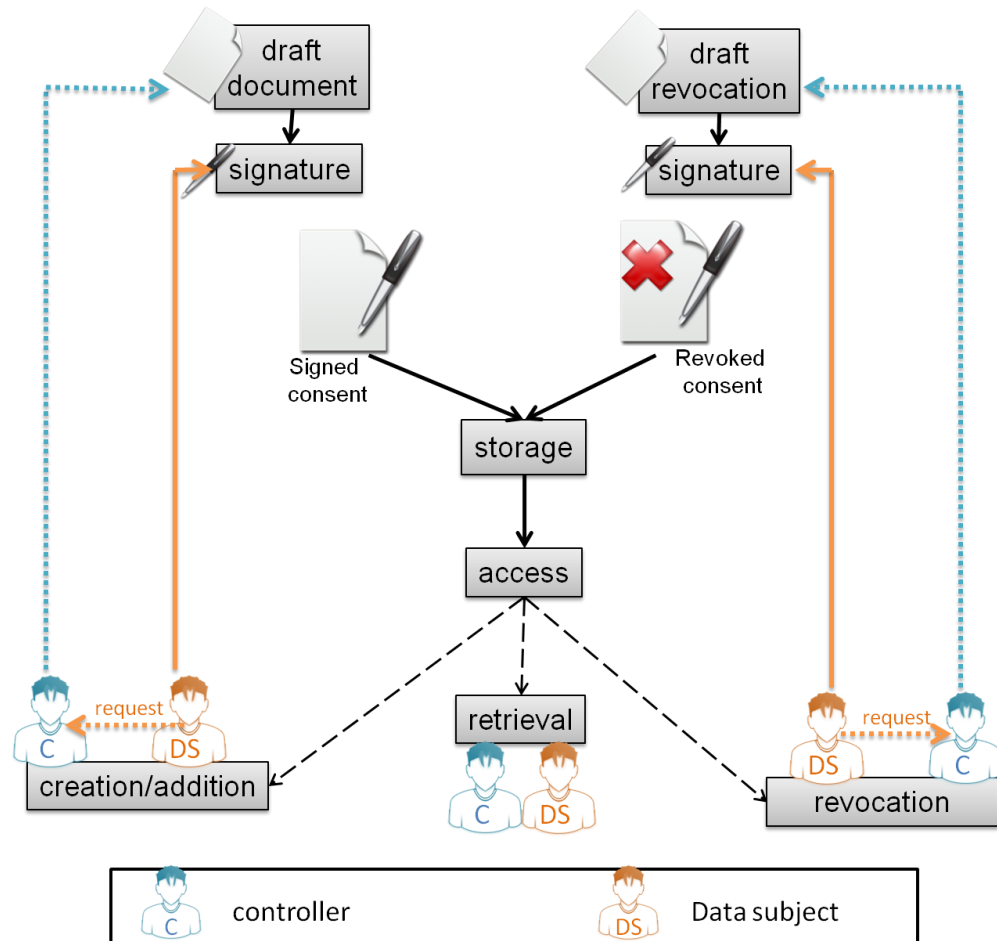
# User consent

## Legal requirements

- Informed
- Freely given
- Specific

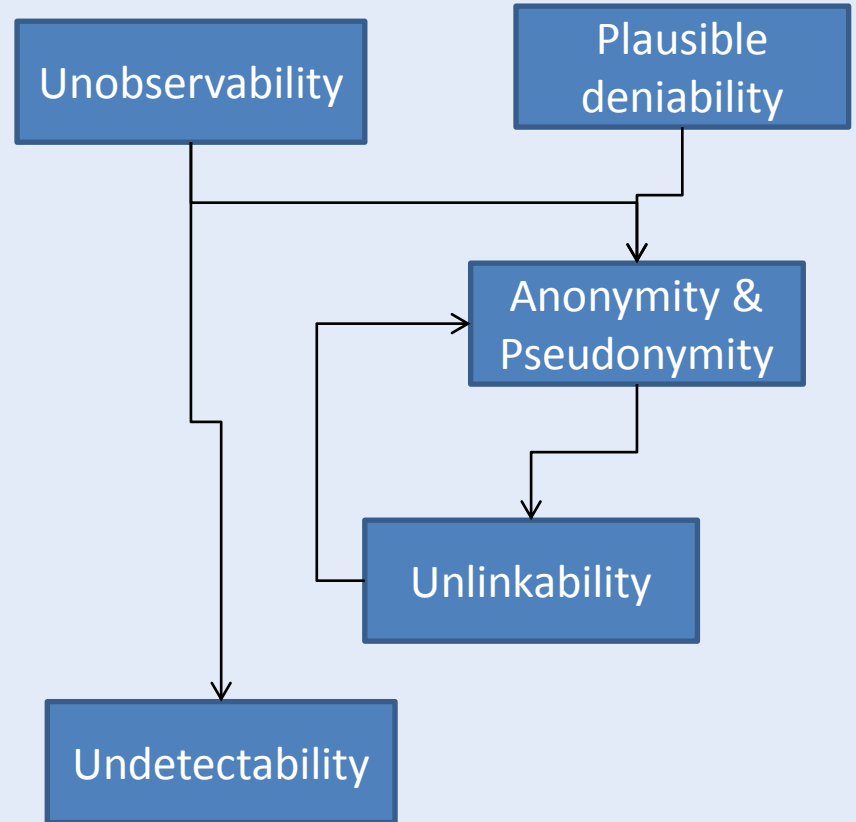
## Consent structure

- Data subject
- Controller
- Receiver
- Types of data
- Action (Upload or share)
- Purpose of sharing
- Type of consent (opt-in/opt-out)
- Revoked
- (Context (e.g., “emergency”))
- (Location)



# Privacy

## Hard privacy



→ requires



Confidentiality

User awareness

Compliance

### **Confidentiality**

*authorized restrictions on information access and disclosure*<sub>37</sub>

# Confidentiality

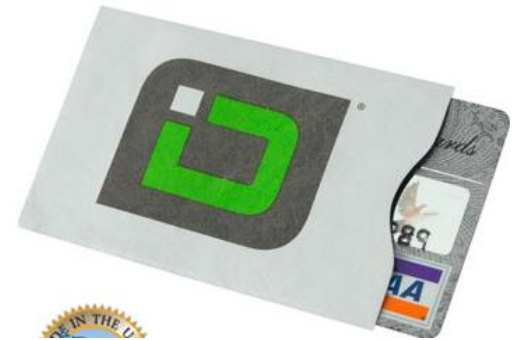
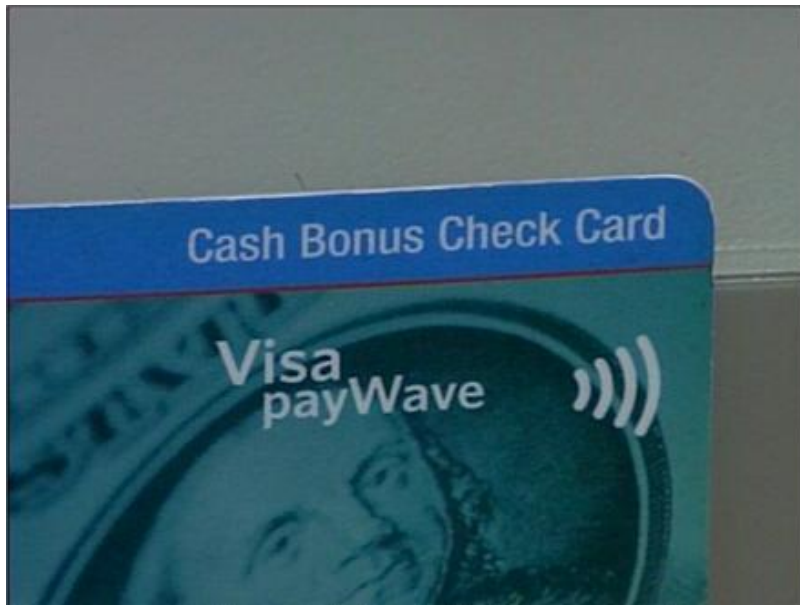
- Preserving authorized restrictions on information access and disclosure, including means for protecting personal privacy and proprietary information (*NIST*)
- Security property



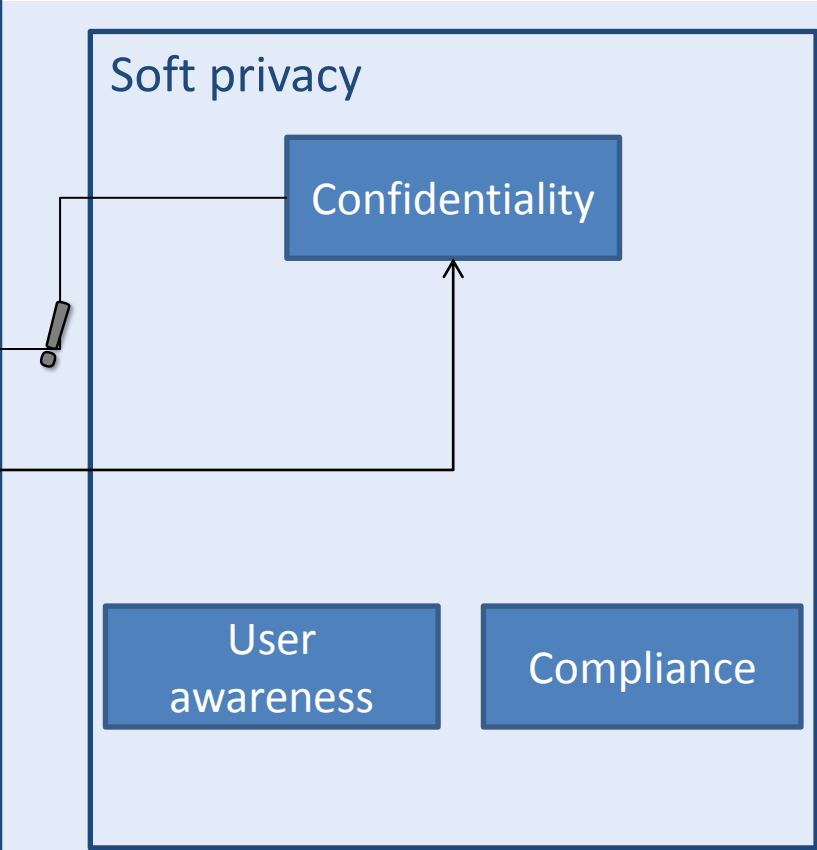
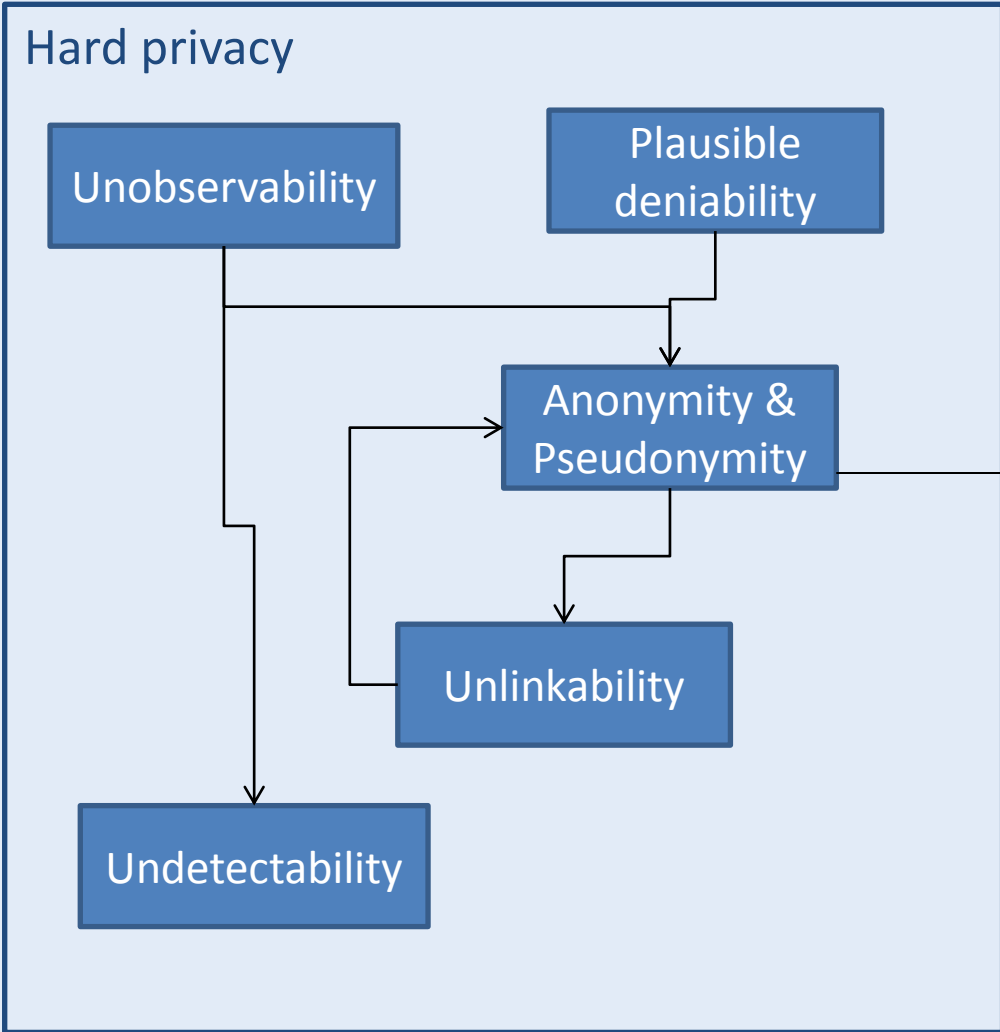
# Confidentiality: example

Problem:  
Electronic pickpocketing

Solution:  
Confidentiality



# Privacy



→ requires

! — impacts

Security

Non-repudiation

Soft privacy

Confidentiality

User awareness

Compliance

Privacy

Hard privacy

Unobservability

Plausible deniability

Anonymity & Pseudonymity

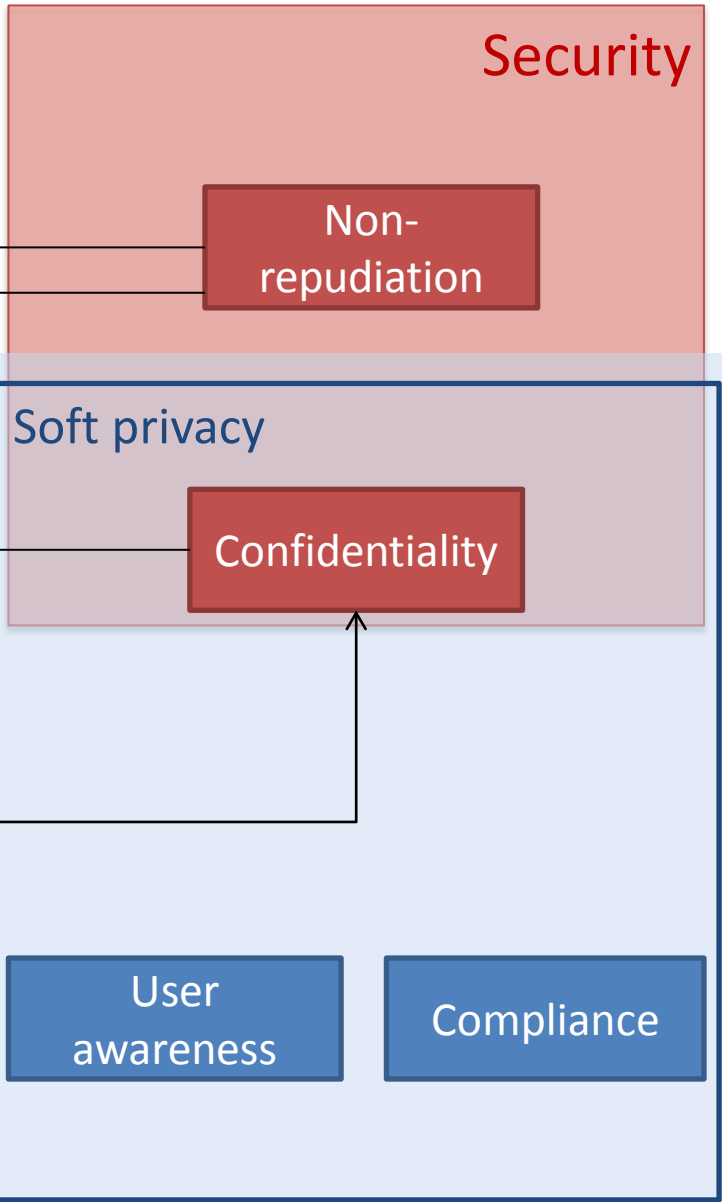
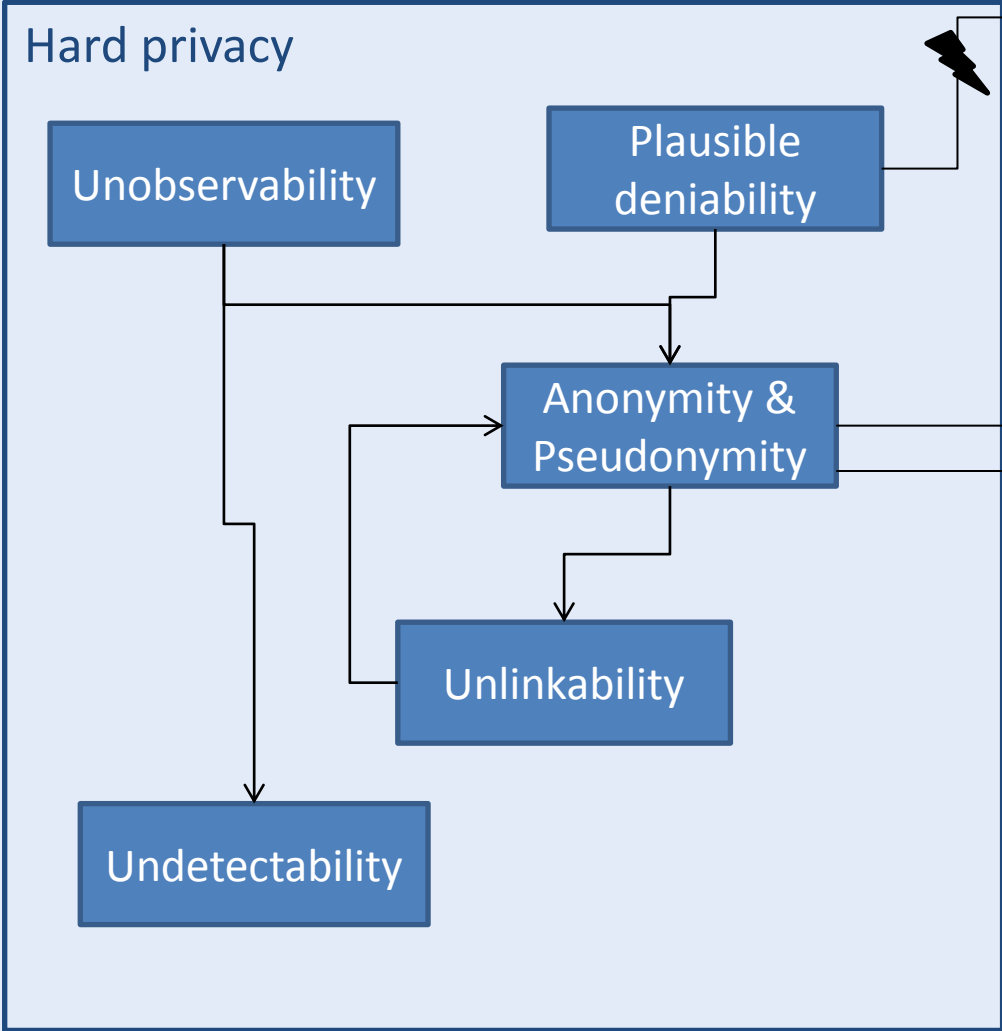
Unlinkability

Undetectability

→ requires

⚡ conflicts

! impacts





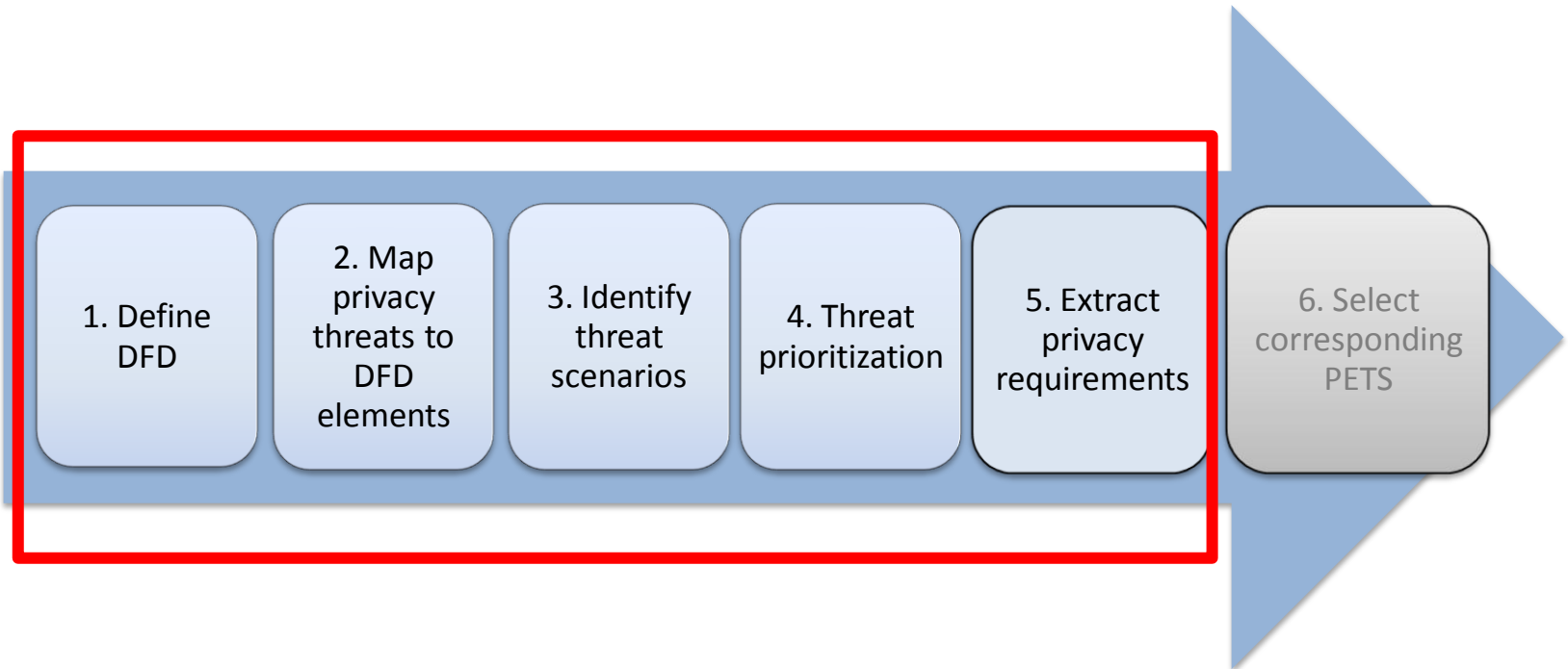
LINDDUN - Privacy threat analysis

# **PRIVACY METHODOLOGY**

# Integrating privacy in the system

- Not straight-forward
- Should be part of Software development lifecycle
- Methodology based on STRIDE

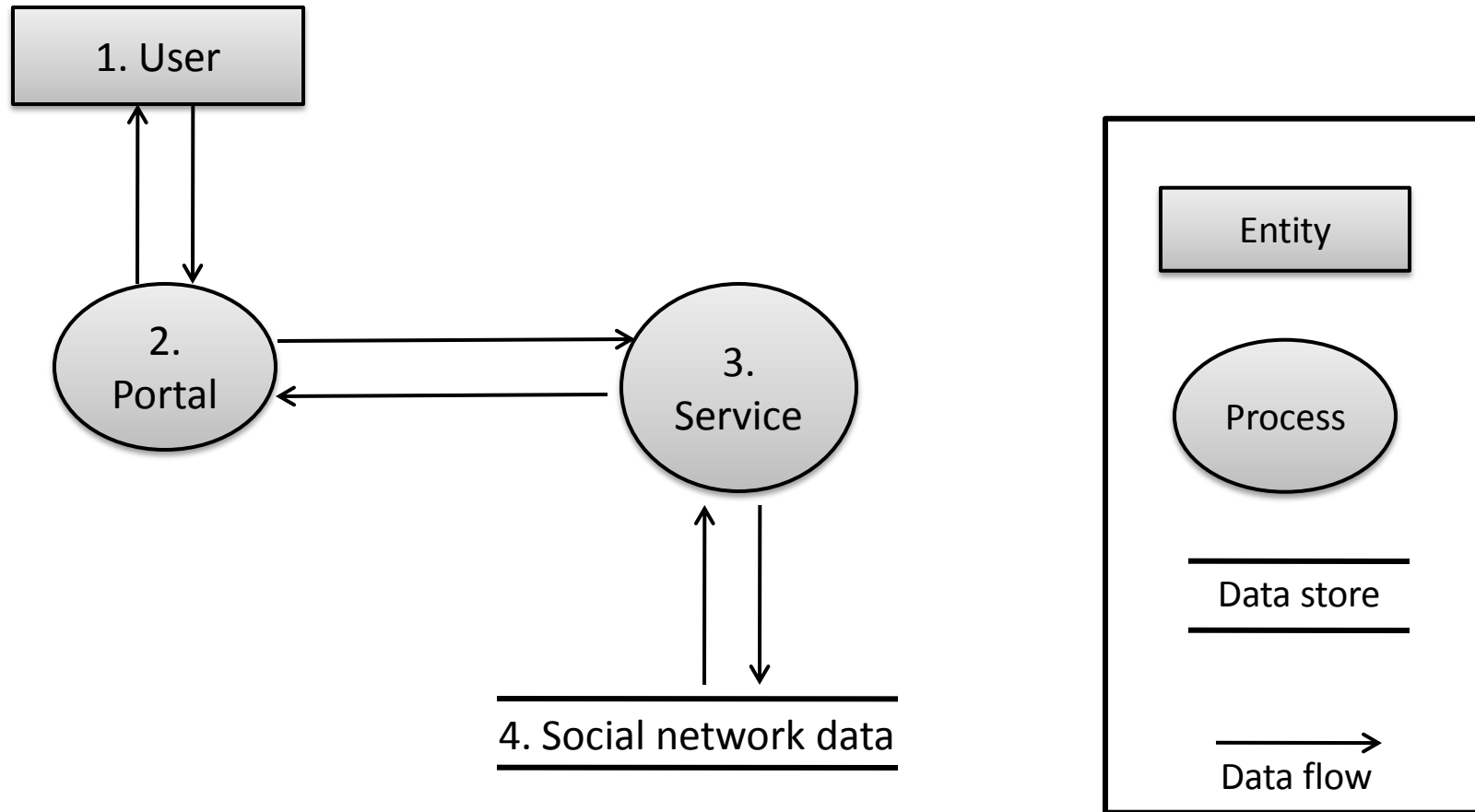
# LINDDUN Methodology



# LINDDUN Methodology

- **Step 1**
  - Create the DFD diagram (assets)
- Step 2
  - Map LINDDUN to DFD element types
- Step 3
  - Refine threats via threat tree patterns
  - Document assumptions
  - Document the threats with template
- Step 4
  - Assign priorities
- Step 5
  - Extract privacy requirements

# DFD: social network scenario



# LINDDUN Methodology

- Step 1
  - Create the DFD diagram (assets)
- **Step 2**
  - **Map LINDDUN to DFD element types**
- Step 3
  - Refine threats via threat tree patterns
  - Document assumptions
  - Document the threats with template
- Step 4
  - Assign priorities
- Step 5
  - Extract privacy requirements

# LINDDUN privacy threats

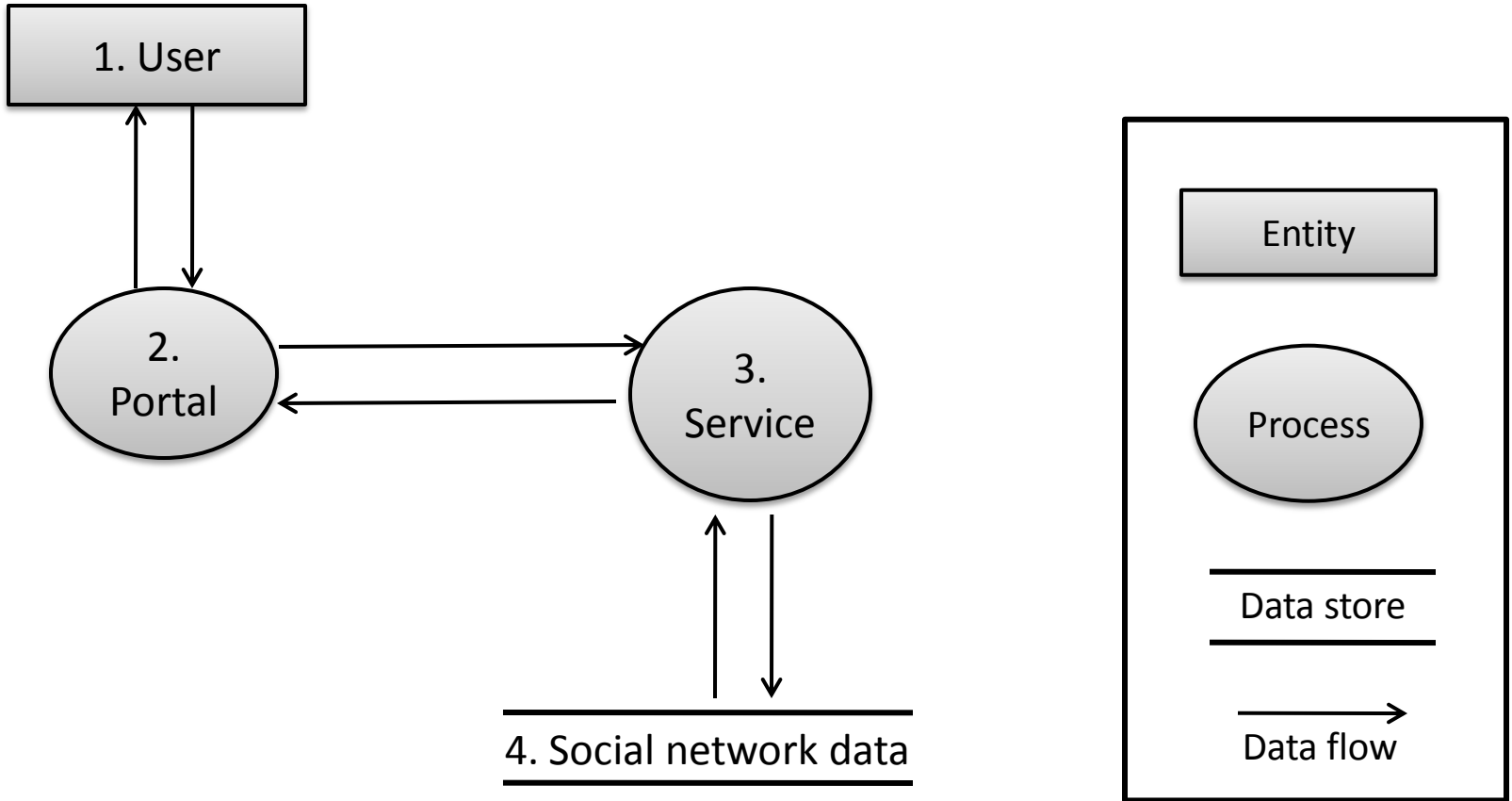
- **Linkability**
  - Sufficiently distinguish whether 2 IOI are linked or not
- **Identifiability**
  - Possible to identify the subject within a set of subjects
- **Non-repudiation**
  - Possible to gather evidence to counter the claims of the repudiating party
- **Detectability**
  - sufficiently distinguish whether IOI exists or not
- **Disclosure of Information**
  - Exposal of information to individuals who are not suppose to have access to it
- **Unawareness of the content**
  - user is unaware of the information he is supplying to the system
- **Noncompliance of policy/consent**
  - System is not compliant with its advertised policies/consents

# Mapping threats to DFD

	<b>Linkability</b>	<b>Identifiability</b>	<b>Non-repudiation</b>	<b>Detectability</b>	<b>Information Disclosure</b>	<b>Content Unawareness</b>	<b>Policy &amp; Consent Non-compliance</b>
<b>Data store</b>	X	X	X	X	X		X
<b>Data flow</b>	X	X	X	X	X		X
<b>Process</b>	X	X	X	X	X		X
<b>Entity</b>	X	X				X	



# DFD: social network scenario



# Mapping Example scenario

	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)	X	X	X	X	X		X
	Service data stream (portal-service)	X	X	X	X	X		X
	DB data stream (service – DB)	X	X	X	X	X		X
Process	Portal	X	X	X	X	X		X
	Social network service	X	X	X	X	X		X
Entity	User	X	X				X	

# LINDDUN Methodology

- Step 1
  - Create the DFD diagram (assets)
- Step 2
  - Map LINDDUN to DFD element types
- **Step 3**
  - Refine threats via threat tree patterns
  - **Document assumptions**
  - Document the threats with template
- Step 4
  - Assign priorities
- Step 5
  - Extract privacy requirements

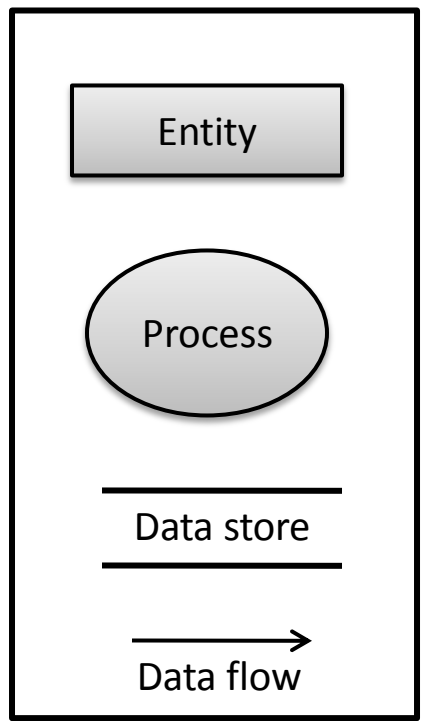
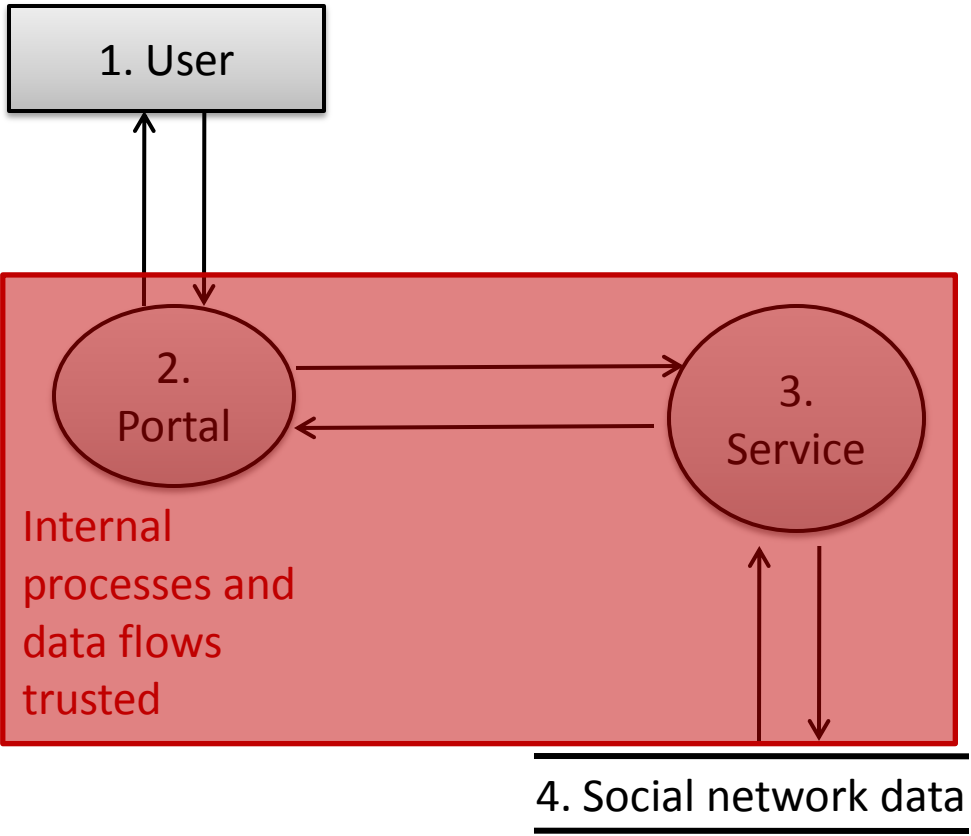
# Assumptions

- Assumptions are explicit or implicit **choices to trust an element of the system** (e.g., human, piece of software) to behave as expected
- **The privacy analyst trusts the assumption to be true**
- These assumed properties or assertions **act as domain restrictions**, i.e., they restrict the domain in some way

# Assumptions

- When adding DFD elements, the number of threats grows exponentially
  - Limit by making assumptions
- Example: assumptions for Social network 2.0:
  1. Internal DFD elements are trustworthy.
    - A. trust the processes and data flows in the back-end system.
    - B. do not trust the user and its communication with the portal or the data store containing all the user's information.
  2. non-repudiation and detectability threats are considered irrelevant for social networks. (based on threat trees)
  3. non-compliance threats are not specific to a specific DFD element, but are applicable to the entire system

# DFD: social network scenario



# Impact assumptions on example scenario

1. DFD

2. Mapping

3. threat scenarios

4. Priorities

5. privacy reqs

	Threat target	L	I	N	D	D	U	N
Data store	Social network db	1	4	X	X	7		10*
Data flow	User data stream (user-portal)	2	5	X	X	8		10*
	Service data stream (portal-service)	X	X	X	X	X		10*
	DB data stream (service – DB)	X	X	X	X	X		10*
Process	Portal	X	X	X	X	X		10*
	Social network service	X	X	X	X	X		10*
Entity	User	3	6				9	56

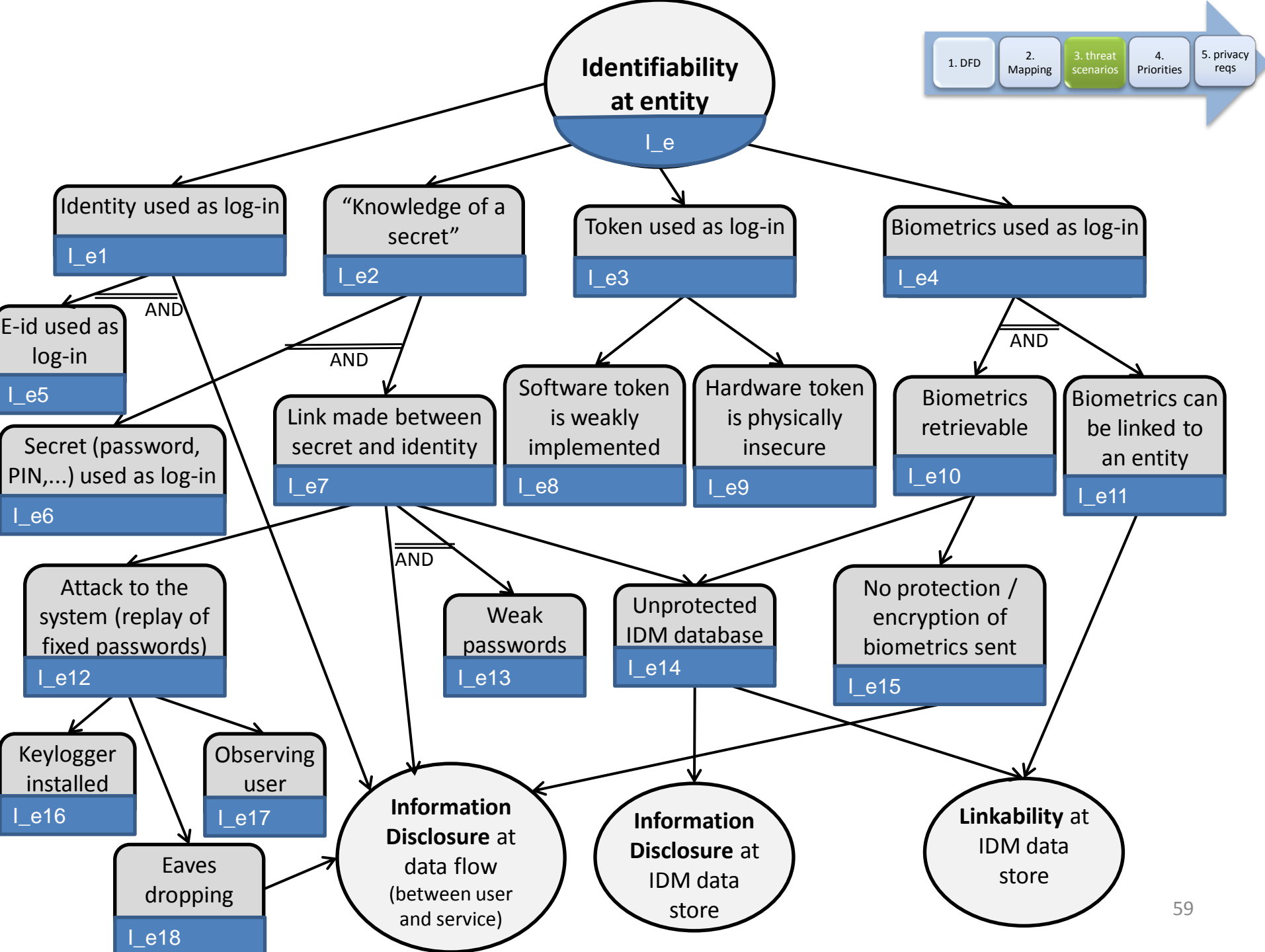
# LINDDUN Methodology

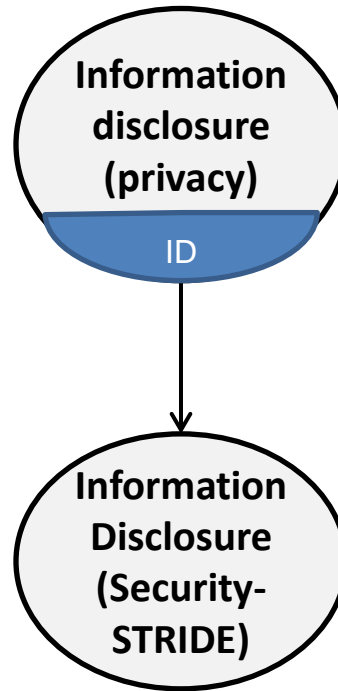
- Step 1
  - Create the DFD diagram (assets)
- Step 2
  - Map LINDDUN to DFD element types
- **Step 3**
  - **Refine threats via threat tree patterns**
  - Document assumptions
  - Document the threats with template
- Step 4
  - Assign priorities
- Step 5
  - Extract privacy requirements



# Privacy threat tree patterns

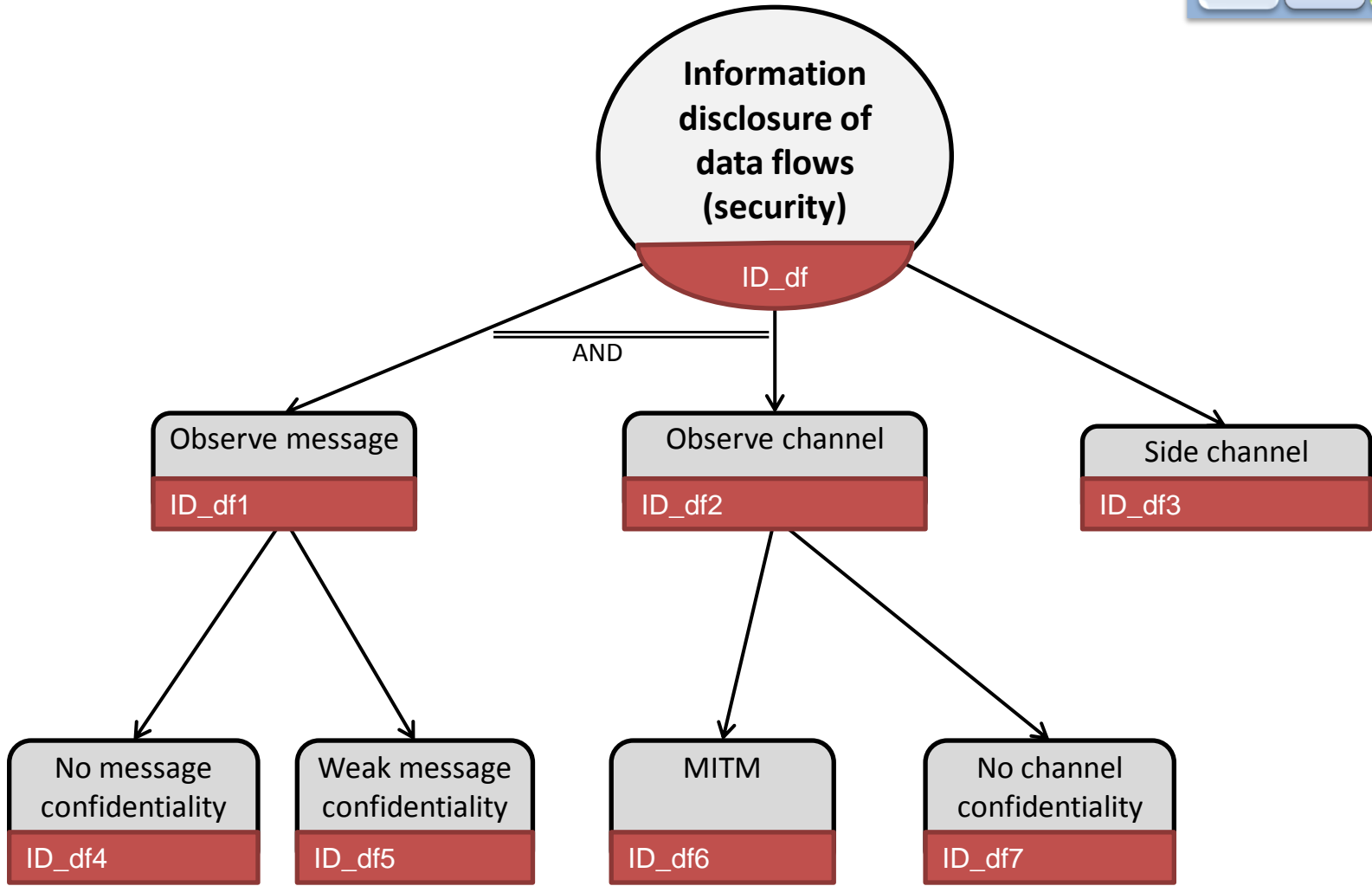
- Illustrate the most common attack patterns
- Used to determine threat applies to system
- Note:
  - Do not limit your analysis to these trees





# STRIDE revisited

- Systematic approach for security threat identification
- Spoofing, Tampering, Repudiation, Information disclosure, Denial of service, Elevation of privilege



# LINDDUN Methodology

- Step 1
  - Create the DFD diagram (assets)
- Step 2
  - Map LINDDUN to DFD element types
- **Step 3**
  - Refine threats via threat tree patterns
  - Document assumptions
  - **Document the threats with template**
- Step 4
  - Assign priorities
- Step 5
  - Extract privacy requirements

# Threat description

Inspired by Misuse Cases template

## Threat description

- ID & Title
- Summary
- Misactor profile
- Basic path
- Alternative path(s)
- Consequence
- Leaf node(s)
- Root node(s)
- DFD element(s)
- Remarks

### **In your report**

- ✓ Mention the threats in the order you found them

# Threat description

## Example (naive) 1/3

- **ID & Title**
  - T01 . Identify users of the social network system
- **Summary**
  - A misactor gains access to the “secret” sent by the user to log-in and deduces the user’s identity from it
- **Misactor profile**
  - skilled outsider



# Threat description

## Example (naive) 2/3

- **Basic path**

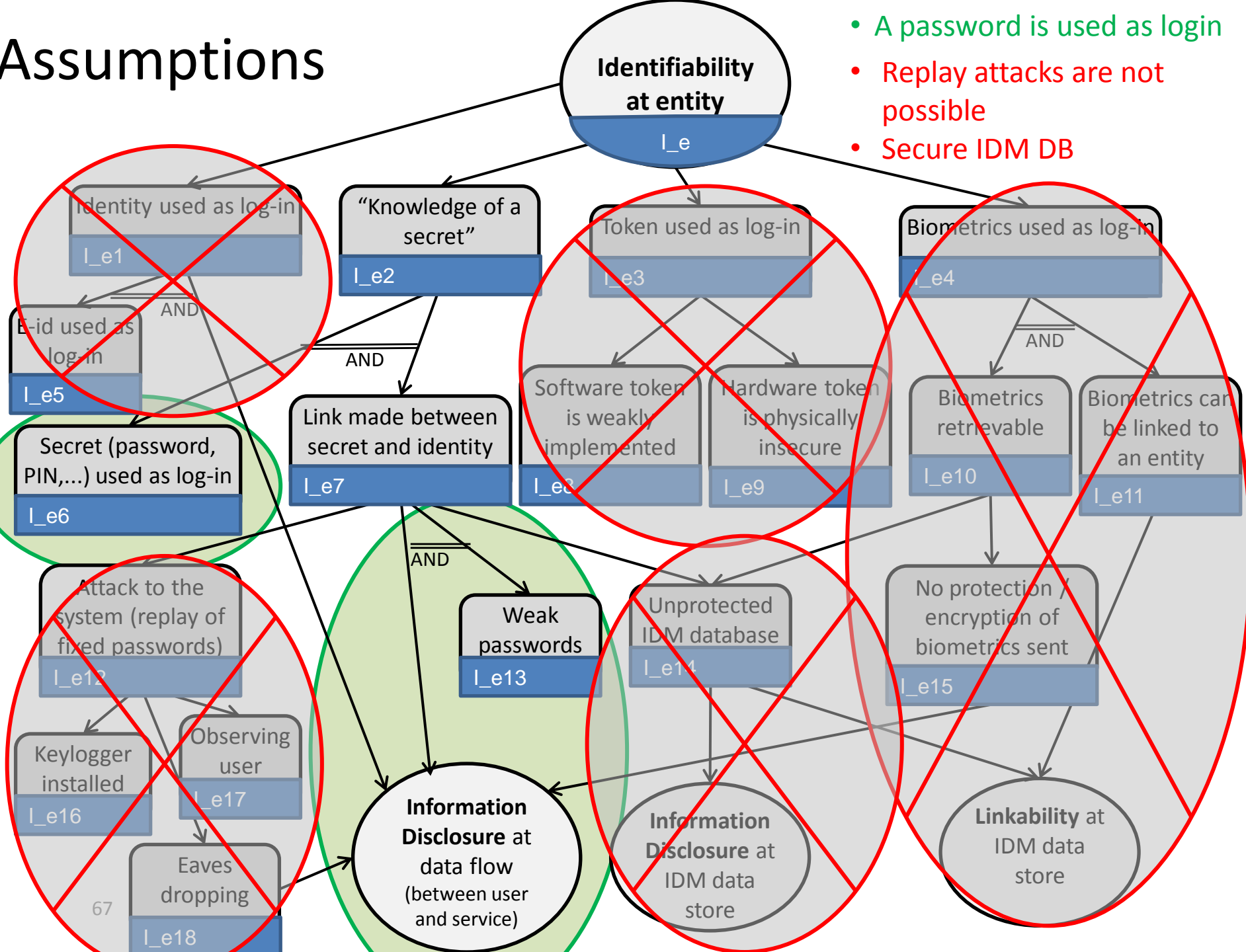
1. The misactor gains access to the data flow between the user and the portal
2. The data contains the user's password
3. The misactor can directly link the password to the user due to weak password use (e.g. initials + birthdate)

- **Consequence**

- The user's identity is compromised

# Assumptions

- A password is used as login
- Replay attacks are not possible
- Secure IDM DB



# Threat description

## Example (naive) 3/3

- **Reference to leaf node(s):** l\_e6, l\_e13
- **Reference to root node:** l\_e
- **DFD element:** User
- **Remarks:**
  - the data flow between the user and the portal is susceptible to information disclosure threats (assumption 1B). This threat is described in T06.
  - A password is used as log-in (Assumption 4)
  - Replay attacks are not considered a threat (Assumption 5)
  - The IDM database is considered secure (Assumption 6)

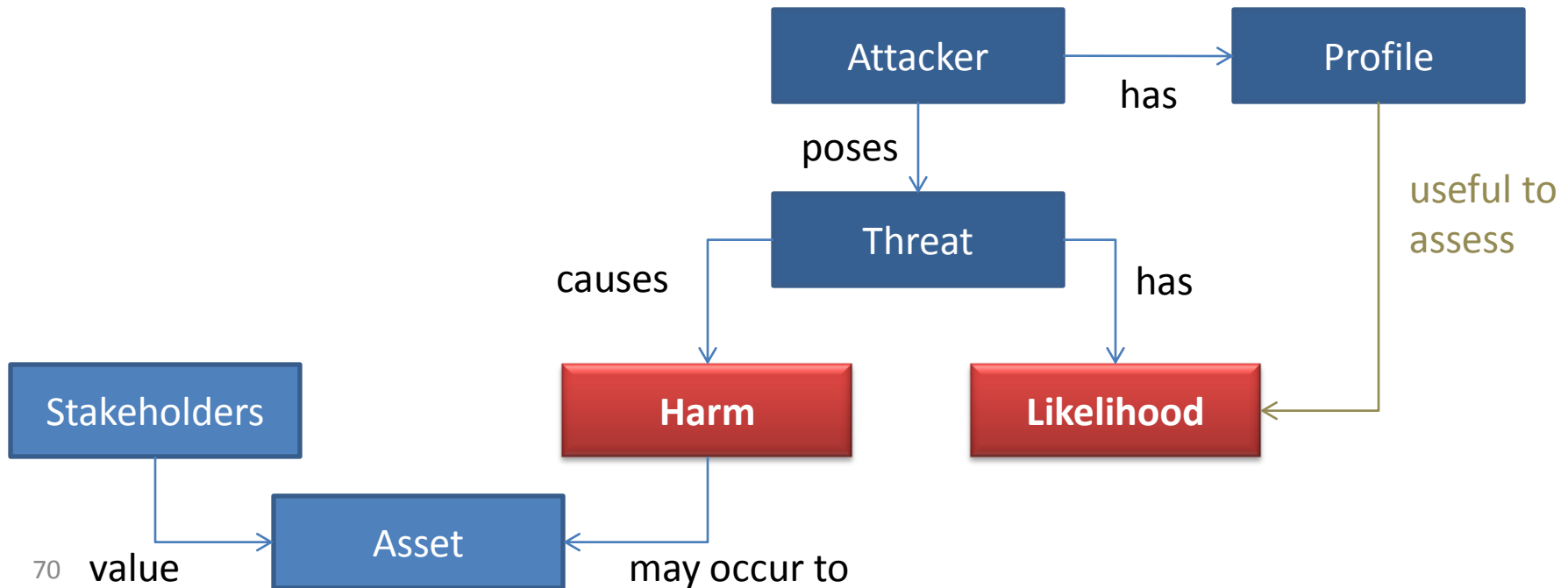
If these assumptions do not hold, the threat tree leaf nodes will result in additional threats

# LINDDUN Methodology

- Step 1
  - Create the DFD diagram (assets)
- Step 2
  - Map LINDDUN to DFD element types
- Step 3
  - Refine threats via threat tree patterns
  - Document assumptions
  - Document the threats with template
- **Step 4**
  - **Assign priorities**
- Step 5
  - Extract privacy requirements

# The role of risk

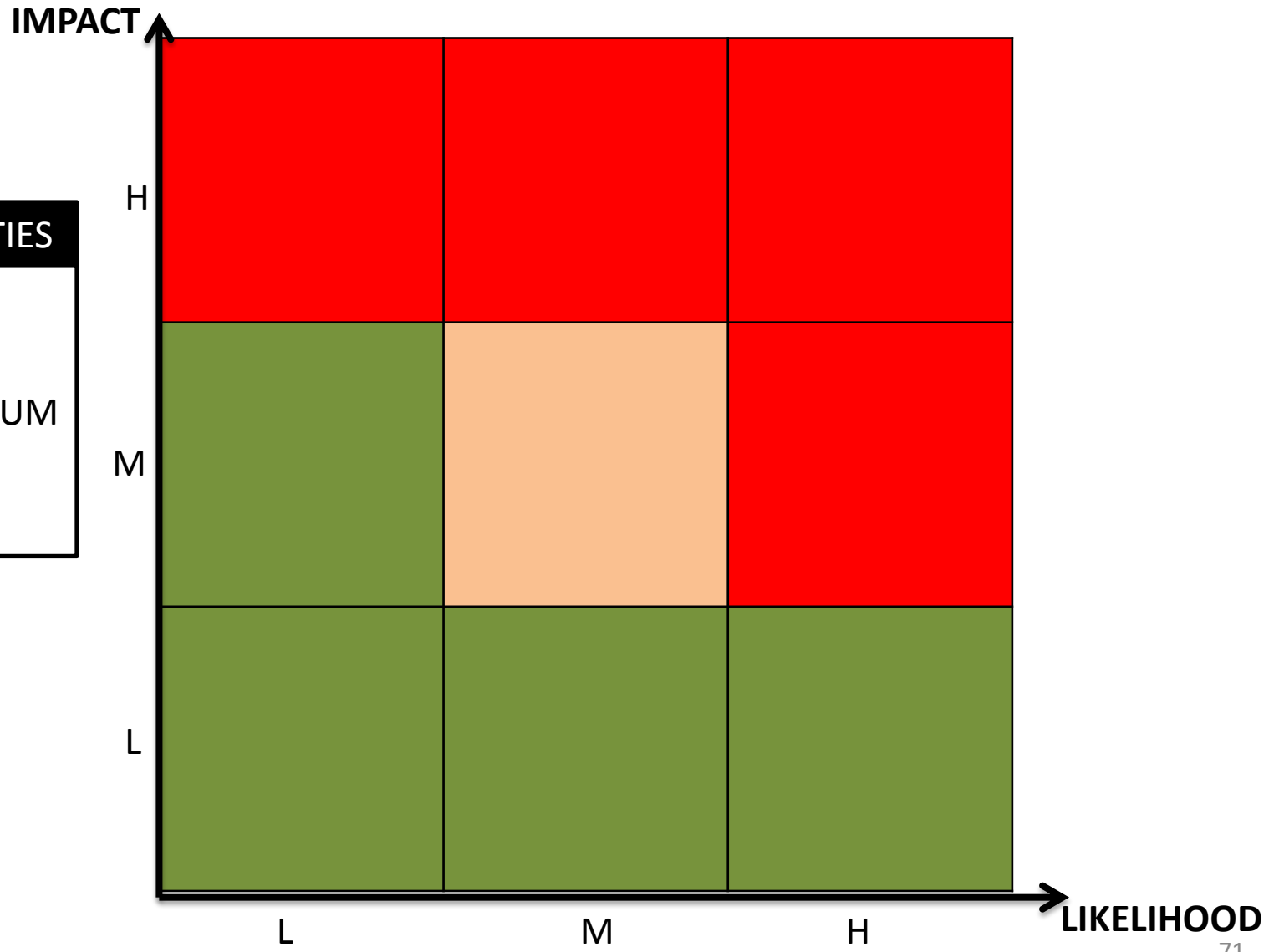
- Risk is a function of the likelihood of a threat and the severity of its impact on the organization
  - $R = f(\text{likelihood}, \text{impact})$



# Risk

**RISK PRIORITIES**

- HIGH
- MEDIUM
- LOW



# LINDDUN Methodology

- Step 1
  - Create the DFD diagram (assets)
- Step 2
  - Map LINDDUN to DFD element types
- Step 3
  - Refine threats via threat tree patterns
  - Document assumptions
  - Document the threats with template
- Step 4
  - Assign priorities
- **Step 5**
  - **Extract privacy requirements**

# Privacy requirements

- Possible mitigation techniques <sup>1</sup>
  - Do nothing
  - Remove feature
  - Turn off feature
  - Warn user
  - Counter threats
    - with preventive or reactive technology



# From threats to requirements

Threat	Requirement
Linkability	Unlinkability
Identifiability	Anonymity(/pseudonymity)
Non-repudiation	Plausible deniability
Detectability	Undetectability
Disclosure of information	Confidentiality
Unawareness of content	Content awareness
Noncompliance of policy/consent	Consent/policy compliance of the system

*Straight-forward  
mapping... BUT*

# From threats to requirements

- Requirements should **not be limited to straight-forward mapping**
  - Look at each leaf node that causes threat
  - Determine for each node the proper mitigation

Threats (misuse cases)	Caused by (leaf nodes)	Mitigated by (requirements)
Deducing identity from password	Information disclosure of data flow	Ensure confidential communication channel (encryption)
	Weak passwords	System should reject weak passwords (at registration) OR
		Users should be made aware of consequences of weak passwords (e.g. feedback given at registration)

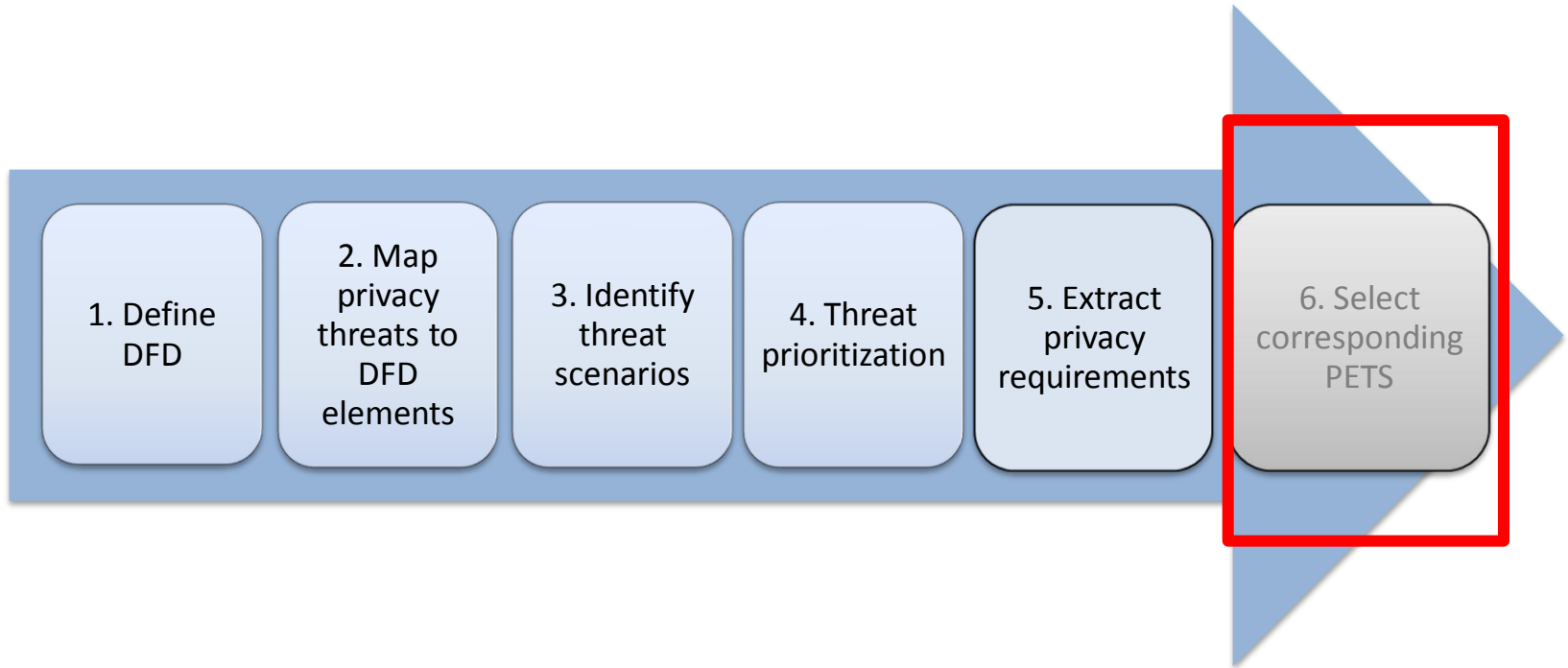
# From threats to requirements

- Add the requirements in a separate table with a clear link to its corresponding threat(s)

Requirements	Threats
Ensure confidential communication channel (encryption)	Deducing identity from password
System should reject weak passwords (at registration) OR Users should be made aware of consequences of weak passwords (e.g. feedback given at registration)	Deducing identity from password

**1 requirement can (partially) mitigate multiple threats**

# LINDDUN Methodology



	Mitigation techniques: PETs	U	A	P	D	C	W	O
Anonymous communication	Mix-networks (1981) [29], DC-networks (1985) [30,31], ISDN-mixes [32], Onion Routing (1996) [33], Crowds (1998) [34], Single proxy (90s) (Penet pseudonymous remailer (1993-1996), Anonymizer, SafeWeb), anonymous Remailer (Ciphertyp Type 0, Type 1 [35], Mixmaster Type 2 (1994) [36], Mixminion Type 3 (2003) [37]), and Low-latency communication (Freedom Network (1999-2001) [38], Java Anon Proxy (JAP) (2000) [39], Tor (2004) [40])	×	×			×		
	DC-net & MIX-net + dummy traffic, ISDN-mixes [32]	×	×		×	×		
	Broadcast systems [41,42] + dummy traffic	×	×		×			
Privacy preserving authentication	Private authentication [43,44]	×	×					
	Anonymous credentials (single show [45], multishow [46])	×	×					
	Deniable authentication [47]	×	×	×				
	Off-the-record messaging [48]	×	×	×			×	
Privacy preserving cryptographic protocols	Multi-party computation (Secure function evaluation) [49, 50]	×				×		
	Anonymous buyer-seller watermarking protocol [51]	×	×				×	
Information retrieval	Private information retrieval [52] + dummy traffic	×	×		×			
	Oblivious transfer [53,54]	×	×			×		
	Privacy preserving data mining [55,56]	×	×			×		
	Searchable encryption [57] / Private search [58]		×				×	
Data anonymization	K-anonymity model [23,59], l-Diversity [60]	×	×					
Information hiding	Steganography [61]	×	×		×			
	Covert communication [62]	×	×		×			
	Spread spectrum [63]	×	×		×			
Pseudonymity systems	Privacy-enhancing identity management system [64]	×	×					
	User-controlled identity management system [65]	×	×					
	Privacy-preserving biometrics [66]	×	×				×	
Encryption techniques	Symmetric key & public key encryption [67]					×		
	Deniable encryption			×		×		
	Homomorphic encryption [68]					×		
	Verifiable encryption [69]					×		
Access control techniques	Context-based access control [70]					×		
	Privacy-aware access control [71,72]					×		
Policy and feedback tools	Policy communication (P3P [19])							×
	Policy enforcement (XACML [73], EPAL [74])							×
	Feedback tools for user privacy awareness [12, 13, 75]						×	
	Data removal tools (spyware detection and removal, browser cleaning tools, activity traces eraser, harddisk data eraser)						×	

**U:** unlinkability

**A:** anonymity

**P:** plausible deniability

**D:** undetectability

**C:** confidentiality

**W:** content awareness

**O:** consent/policy compliance

# Social network example

Nr	MUC	Requirements	Solutions
1	Linkability data store	Unlinkability of data entries within the social network database	Data anonymization techniques: K-anonymity
		Protection of data store	Access control: relationship-based
2	Linkability data flow	Unlinkability of messages	Anonymous communication system: TOR
		Channel confidentiality	
...			
9	Content unawareness of user	Make users aware that they only need to provide minimal set of information	Use feedback tools to raise awareness
10	Policy and consent non-compliance	Design system in compliance with legal guidelines	Assign policy compliance responsibility to employee
		Ensure user aware of legitimate actions to perform	User can sue organization
		Employee contracts specify internal rules	Employees disclosing information are penalized

# Suggested reading

- Privacy
  - **Pfitzmann & Hansen (2010)**: A terminology for talking about privacy by data minimization: Anonymity, Unlinkability, Undetectability, Unobservability, Pseudonymity, and Identity Management
    - defines *anonymity, pseudonymity, undetectability, unobservability, unlinkability*
  - **Guerses (2010)**: Multilateral Privacy Requirements Analysis in Online Social Network Services (PhD thesis)
    - section 2.2 (pg. 22-32) provide an interesting overview of privacy. Especially interesting for the following concepts: *confidentiality, feedback and awareness*
  - **Guarda and Zannone (2008)**: Towards the development of privacy-aware systems
    - for those interested in the legal aspects of privacy
    - summarize the privacy principles from a legislation perspective, as it is clearly also important that a system is compliant with law, policies, and user consent (*policy and consent compliance*)
- Methodology
  - **LINDDUN**: a privacy threat analysis framework
    - <http://people.cs.kuleuven.be/~kim.wuyts/ERISE/LINDDUN.pdf>

LINDDUN - Privacy threat analysis

# **EXAMPLE – PATIENT COMMUNITY SYSTEM**



# Existing patient communities

patientslikeme®

Patients | Treatments | Symptoms | Research

Home > Find Patients w/ Treatments, Symptoms and Side Effects Like You > corkey3160's Profile

**What's New**

- corkey3160's Journal

**Charts**

- corkey3160's Charts

**About**

- corkey3160's Summary

**corkey3160**

Female, 56 years  
Timbuktu, CA

**Primary Condition:**  
Major Depressive Disorder and 9 more

**First symptom:** Jun 1973

**Diagnosis:** Jan 1992

[See more](#)

Display charts from: PLM 1 mo 6 mo

1 yr 2 yr All

Sort This Profile

**InstantMe**

- Very Good
- Good
- Neutral
- Bad
- Very Bad

**Mood Map**

**Mood Function**

High

Low

**Distress**

Show this chart

**Mood External Stress**

High

- Overwhelming
- Severe
- Moderate
- Low

**Symptoms**

Severity of symptoms

- None
- Mild
- Moderate
- Severe

Clicking the arrow will display treatments for that symptom

- Prescription Drug
- Psychotherapy
- Exercise

Drag the arrows or use the tools on the left to change the view of the profile. 28, 2009 Apr 3, 2012

**Neutral**

Apr 2, 2012 12:14 PM

*working at getting organized*

[More](#)

Last update: Feb 20, 2012

**General Symptoms**

- Anxious mood
- Depressed mood**
- Fatigue
- Insomnia
- Pain

**ADHD (Attention Deficit/Hyperactivity)**

- Hyperactivity
- Impulsive behaviors
- Inattention

**Dysthymia**

- Eating Disorder
- Generalized Anxiety Disorder

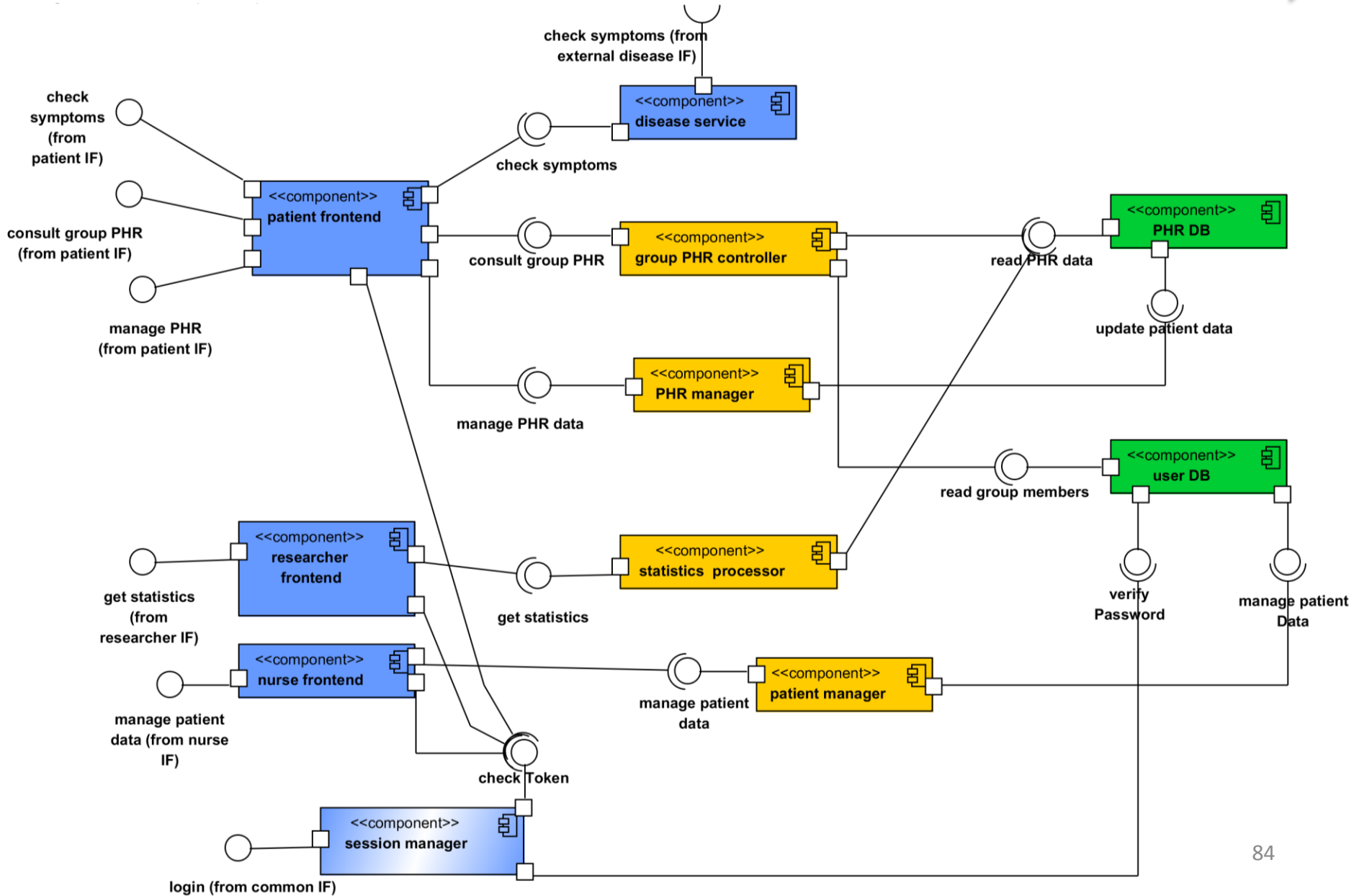
**Panic Disorder**

- Dizziness and feeling faint
- Heart palpitations
- Shortness of breath (dyspnea)
- Sweating

# Patient communities case study

- Patient
  - Store personal health data (PHR)
  - Retrieve (pseudonymized) PHR from other patients (group members) with same condition
  - Retrieve trustworthy information on diseases and treatments (from external service)
- Nurse
  - Add users and manage groups
- Researcher
  - Retrieve (anonymized) PHR data to use in analysis

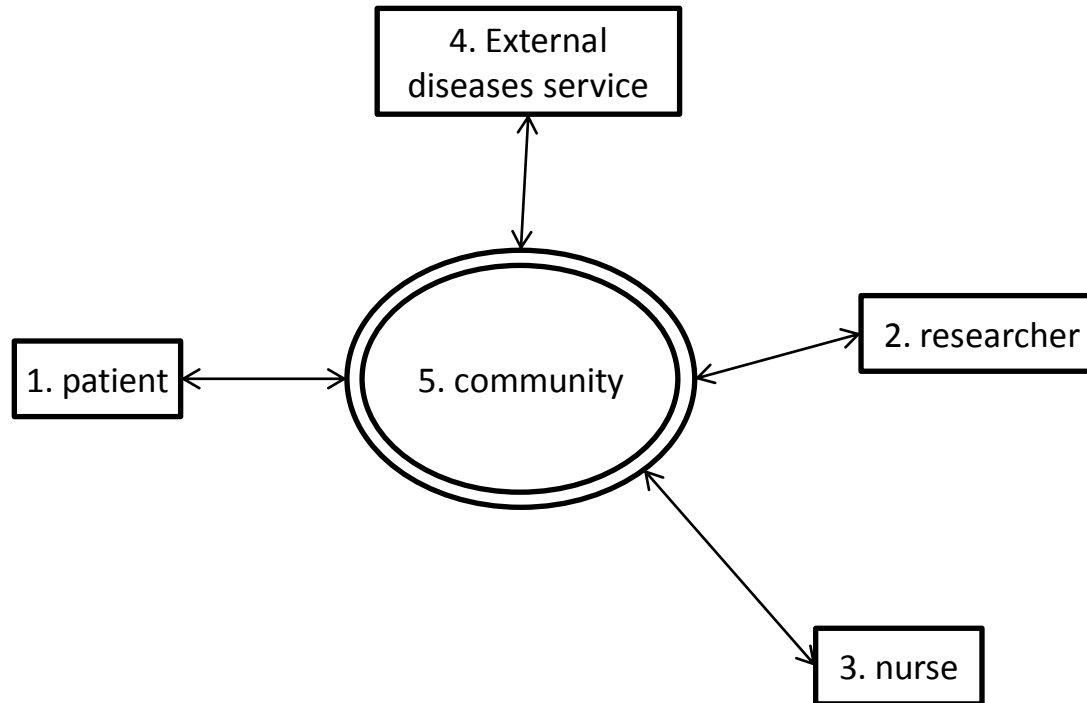
# Client-server view



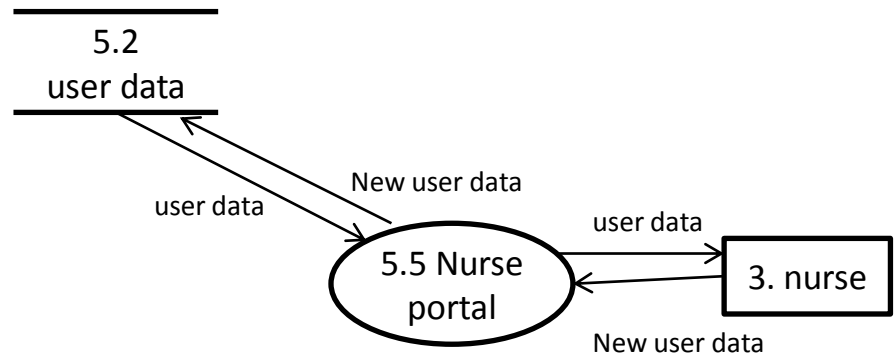
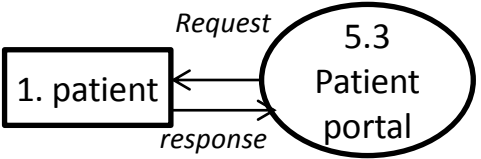
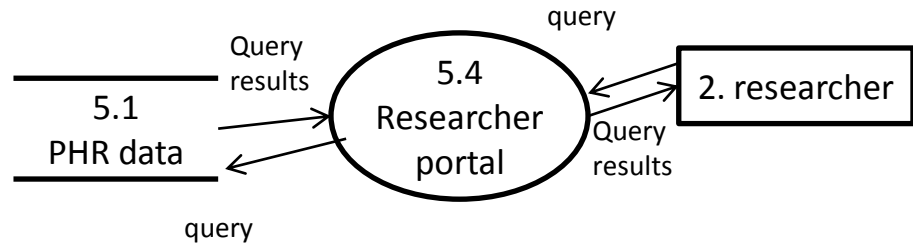
# LINDDUN Methodology

- **Step 1**
  - Create the DFD diagram (assets)
- Step 2
  - Map LINDDUN to DFD element types
- Step 3
  - Refine threats via threat tree patterns
  - Document assumptions
  - Document the threats with template
- Step 4
  - Assign priorities
- Step 5
  - Extract privacy requirements

# DFD level 0



4. External diseases services





4. External diseases services

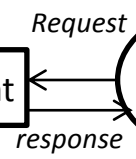


5.6 Browse diseases



5.3 Patient portal

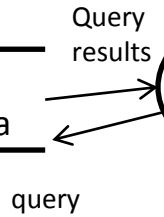
1. patient



5.7 Manage PHR

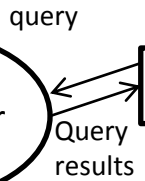


5.1 PHR data

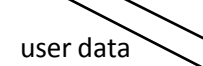


5.4 Researcher portal

2. researcher

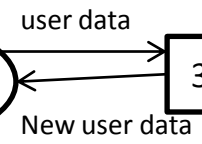


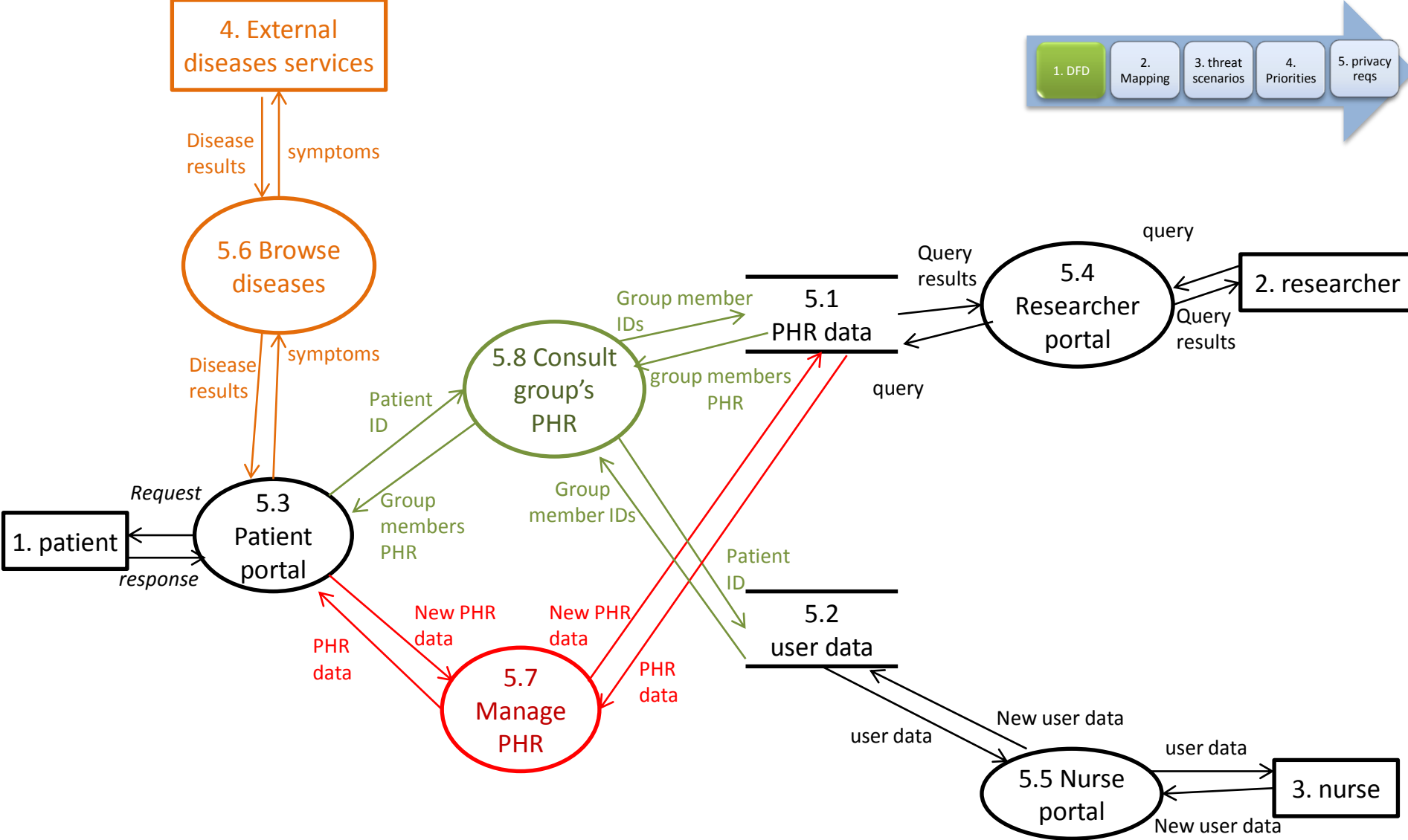
5.2 user data



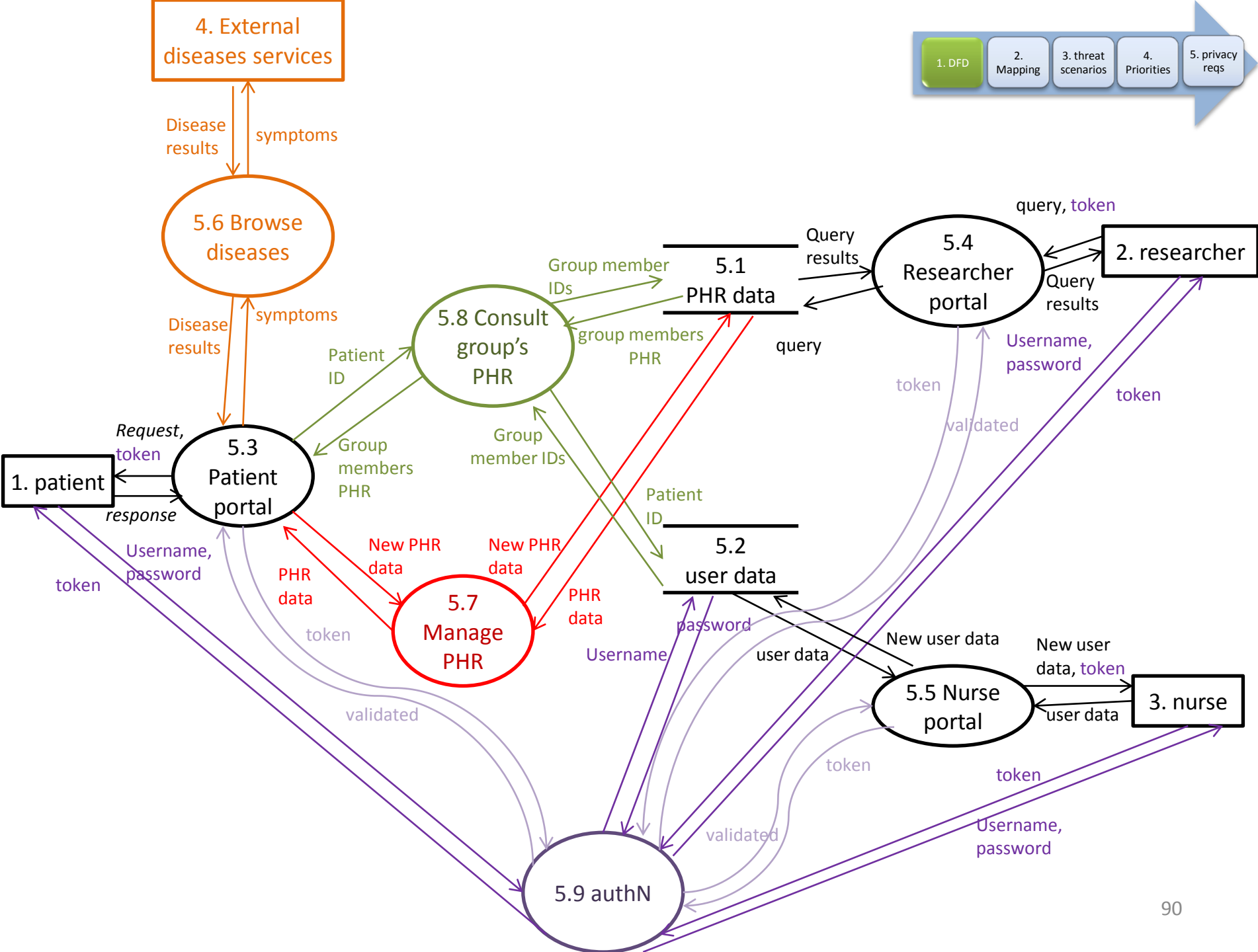
5.5 Nurse portal

3. nurse









# LINDDUN Methodology

- Step 1
  - Create the DFD diagram (assets)
- **Step 2**
  - **Map LINDDUN to DFD element types**
- Step 3
  - Refine threats via threat tree patterns
  - Document assumptions
  - Document the threats with template
- Step 4
  - Assign priorities
- Step 5
  - Extract privacy requirements

# Mapping threats to DFD

	<b>Linkability</b>	<b>Identifiability</b>	<b>Non-repudiation</b>	<b>Detectability</b>	<b>Information Disclosure</b>	<b>Content Unawareness</b>	<b>Policy &amp; Consent Non-compliance</b>
<b>Data store</b>	X	X	X	X	X		X
<b>Data flow</b>	X	X	X	X	X		X
<b>Process</b>	X	X	X	X	X		X
<b>Entity</b>	X	X				X	

		L	I	N	1. DFD	2. Mapping	3. threat scenarios	4. Priorities	5. privacy reqs
Data store	PHR data (5.1)	X	X	X					
	User data (5.2)	X	X	X	X	X			x
flow	Patient – portal flow (1 -5.3)	X	X	X	X	X			x
	Portal – patient flow (5.3-1)	X	X	X	X	X			x
	Researcher – portal flow (2-5.4)	X	X	X	X	X			x
	Portal – researcher flow (5.4-2)	X	X	X	X	X			x
	Nurse – portal flow (3-5.5)	X	X	X	X	X			x
	Portal – nurse flow (5.5-3)	X	X	X	X	X			x
	Disease service – browse diseases flow (4-5.6)	X	X	X	X	X			x
	Browse disease – disease service flow (5.6-4)	X	X	X	X	X			x
	Patient portal - browse diseases flow (5.3-5.6)	X	X	X	X	X			x
	Browse diseases – patient portal flow (5.6-5.3)	X	X	X	X	X			x
	Patient portal – manage PHR flow (5.3-5.7)	X	X	X	X	X			x
	Manage PHR flow (5.7-5.3)	X	X	X	X	X			x
	Patient portal – consult group PHR (5.3-5.8)	X	X	X	X	X			x
	Consult group PHR – patient portal flow (5.8-5.3)	X	X	X	X	X			x
	Researcher portal – PHR data flow (5.4-5.1)	X	X	X	X	X			x
	PHR data – researcher portal flow (5.1-5.4)	X	X	X	X	X			x
	Nurse portal – user data flow (5.5-5.2)	X	X	X	X	X			x
	User data – nurse portal flow(5.2-5.5)	X	X	X	X	X			x
	Manage PHR – PHR data (5.7-5.1)	X	X	X	X	X			x
	PHR data – manage PHR (5.1-5.7)	X	X	X	X	X			x



		L	I	N	D	D	U	N
	Consult group PHR – PHR data flow (5.8-5.1)	X	X	X	X	X		x
	PHR data – consult group PHR flow (5.1-5.8)	X	X	X	X	X		x
	Consult group PHR – user data (5.8-5.2)	X	X	X	X	X		x
	User data – consult group PHR (5.2-5.8)	X	X	X	X	X		x
	Patient – authN flow (1-5.9)	X	X	X	X	X		x
	authN - patient flow (5.9-1)	X	X	X	X	X		x
	Research – authN flow (2-5.9)	X	X	X	X	X		x
	authN flow – researcher (5.9-2)	X	X	X	X	X		x
	Nurse – authN flow (3-5.9)	X	X	X	X	X		x
	authN – nurse (3-5.9)	X	X	X	X	X		x
	User data – authN flow (5.2-5.9)	X	X	X	X	X		x
	authN – user data flow (5.9-5.2)	X	X	X	X	X		x
	Patient portal – authN (5.3-5.9)	X	X	X	X	X		x
	authN – patient portal (5.9-5.3)	X	X	X	X	X		x
	Researcher portal – authN (5.4-5.9)	X	X	X	X	X		x
	authN – researcher portal (5.9-5.4)	X	X	X	X	X		x
	Nurse portal – authN (5.5-5.9)	X	X	X	X	X		x
	authN – nurse portal (5.9-5.5)	X	X	X	X	X		x



		L	I	N	D	D	U	N
process	Patient portal (5.3)	X	X	X	X	X		x
	Researcher portal (5.4)	X	X	X	X	X		x
	Nurse portal (5.5)	X	X	X	X	X		x
	Browse disease (5.6)	X	X	X	X	X		x
	Manage PHR (5.7)	X	X	X	X	X		x
	Consult group PHR (5.8)	X	X	X	X	X		x
	authN (5.9)	X	X	X	X	X		x
Entity	Patient (1)	X	X				X	
	Researcher (2)	X	X				X	
	Nurse (3)	X	X				X	
	External disease service (4)	X	X				X	

# LINDDUN Methodology

- Step 1
  - Create the DFD diagram (assets)
- Step 2
  - Map LINDDUN to DFD element types
- **Step 3**
  - **Refine threats via threat tree patterns**
  - **Document assumptions**
  - Document the threats with template
- Step 4
  - Assign priorities
- Step 5
  - Extract privacy requirements

# General assumptions

1. all internal processes are only susceptible to insider threats, as we consider the back-end sufficiently protected against outsider threats. We will therefore combine the process threats and examine only one, as the threats apply to all of them
2. all data flows between internal processes and between internal processes and internal data stores are only susceptible to insider threats, as we consider the back-end sufficiently protected against outsider threats. We will therefore combine the data flow threats and examine only one, as the threats apply to all of them
3. data flows between an entity and a process are not considered trusted (as it involves transactions of an external entity to and from a trusted process over an insecure communication line)
4. data stores are not considered confidential, as no access control system is present



Positive assumptions can help understand reasoning



		L	I	N	1. DFD	2. Mapping	3. threat scenarios	4. Priorities	5. privacy reqs
Data store	PHR data (5.1)	X	X	X					
	User data (5.2)	X	X	X	X	X			x
flow	Patient – portal flow (1 -5.3)	X	X	X	X	X			x
	Portal – patient flow (5.3-1)	X	X	X	X	X			x
	Researcher – portal flow (2-5.4)	X	X	X	X	X			x
	Portal – researcher flow (5.4-2)	X	X	X	X	X			x
	Nurse – portal flow (3-5.5)	X	X	X	X	X			x
	Portal – nurse flow (5.5-3)	X	X	X	X	X			x
	Disease service – browse diseases flow (4-5.6)	X	X	X	X	X			x
	Browse disease – disease service flow (5.6-4)	X	X	X	X	X			x
	Patient portal - browse diseases flow (5.3-5.6)	X	X	X	X	X			x
Internal data flows combined	Browse diseases – patient portal flow (5.6-5.3)	X	X	X	X	X			x
	Patient portal – manage PHR flow (5.3-5.7)	X	X	X	X	X			x
	Manage PHR flow (5.7-5.3)	X	X	X	X	X			x
	Patient portal – consult group PHR (5.3-5.8)	X	X	X	X	X			x
	Consult group PHR – patient portal flow (5.8-5.3)	X	X	X	X	X			x
	Researcher portal – PHR data flow (5.4-5.1)	X	X	X	X	X			x
	PHR data – researcher portal flow (5.1-5.4)	X	X	X	X	X			x
	Nurse portal – user data flow (5.5-5.2)	X	X	X	X	X			x
	User data – nurse portal flow(5.2-5.5)	X	X	X	X	X			x
	Manage PHR – PHR data (5.7-5.1)	X	X	X	X	X			x
PHR data – manage PHR (5.1-5.7)	X	X	X	X	X			x	

		L	I	N	D	D	U	N
<b>Internal data flows combined</b>	Consult group PHR – PHR data flow (5.8-5.1)	X	X	X	X	X		x
	PHR data – consult group PHR flow (5.1-5.8)	X	X	X	X	X		x
	Consult group PHR – user data (5.8-5.2)	X	X	X	X	X		x
	User data – consult group PHR (5.2-5.8)	X	X	X	X	X		x
	Patient – authN flow (1-5.9)	X	X	X	X	X		x
	authN - patient flow (5.9-1)	X	X	X	X	X		x
	Research – authN flow (2-5.9)	X	X	X	X	X		x
	authN flow – researcher (5.9-2)	X	X	X	X	X		x
	Nurse – authN flow (3-5.9)	X	X	X	X	X		x
	authN – nurse (3-5.9)	X	X	X	X	X		x
<b>Internal data flows combined</b>	User data – authN flow (5.2-5.9)	X	X	X	X	X		x
	authN – user data flow (5.9-5.2)	X	X	X	X	X		x
	Patient portal – authN (5.3-5.9)	X	X	X	X	X		x
	authN – patient portal (5.9-5.3)	X	X	X	X	X		x
	Researcher portal – authN (5.4-5.9)	X	X	X	X	X		x
	authN – researcher portal (5.9-5.4)	X	X	X	X	X		x
	Nurse portal – authN (5.5-5.9)	X	X	X	X	X		x
authN – nurse portal (5.9-5.5)	X	X	X	X	X		x	



		L	I	N	D	D	U	N
process	Patient portal (5.3)	X	X	X	X	X		x
Internal processes combined	Researcher portal (5.4)	X	X	X	X	X		x
	Nurse portal (5.5)	X	X	X	X	X		x
	Browse disease (5.6)	X	X	X	X	X		x
	Manage PHR (5.7)	X	X	X	X	X		x
	Consult group PHR (5.8)	X	X	X	X	X		x
	authN (5.9)	X	X	X	X	X		x
Entity	Patient (1)	X	X				X	
	Researcher (2)	X	X				X	
	Nurse (3)	X	X				X	
	External disease service (4)	X	X				X	

		L	I	N	1. DFD	2. Mapping	3. threat scenarios	4. Priorities	5. privacy reqs
Data store	PHR data (5.1)	X	X	X	X	X			X
	User data (5.2)	X	X	X	X	X			X
flow	Patient – portal flow (1 -5.3)	X	X	X	X	X			X
	Portal – patient flow (5.3-1)	X	X	X	X	X			X
	Researcher – portal flow (2-5.4)	X	X	X	X	X			X
	Portal – researcher flow (5.4-2)	X	X	X	X	X			X
	Nurse – portal flow (3-5.5)	X	X	X	X	X			X
	Portal – nurse flow (5.5-3)	X	X	X	X	X			X
General internal DF	Disease service – browse diseases flow (4-5.6)	X	X	X	X	X			X
	Browse disease – disease service flow (5.6-4)	X	X	X	X	X			X
	Patient portal - browse diseases flow (5.3-5.6)	X	X	X	X	X			X
	Patient – authN flow (1-5.9)	X	X	X	X	X			X
	authN - patient flow (5.9-1)	X	X	X	X	X			X
	Research – authN flow (2-5.9)	X	X	X	X	X			X
	authN flow – researcher (5.9-2)	X	X	X	X	X			X
General internal P	Nurse – authN flow (3-5.9)	X	X	X	X	X			X
	authN – nurse (3-5.9)	X	X	X	X	X			X
process	Patient portal (5.3)	X	X	X	X	X			X
Entity	Patient (1)	X	X					X	
	Researcher (2)	X	X					X	
	Nurse (3)	X	X					X	
	External disease service (4)	X	X					X	

# General assumptions

5. No non-repudiation threats exist in the system, as the data flows, processes and data stores do not require plausible deniability
6. detectability is not considered a threat for this specific system. The privacy concerns of this system are all focused on the data itself, not on the detectability of it
7. non-compliance is an important threat, however, it is not specific to one part of the system, but poses to the system as a whole. We will therefore not make a distinction between the different DFD elements for this threat.

		L	I	N	D	D	U	N
Data store	PHR data (5.1)	X	X	X	X	X		x
	User data (5.2)	X	X	X	X	X		x
flow	Patient – portal flow (1 -5.3)	X	X	X	X	X		x
	Portal – patient flow (5.3-1)	X	X	X	X	X		x
	Researcher – portal flow (2-5.4)	X	X	X	X	X		x
	Portal – researcher flow (5.4-2)	X	X	X	X	X		x
	Nurse – portal flow (3-5.5)	X	X	X	X	X		x
	Portal – nurse flow (5.5-3)	X	X	X	X	X		x
	Disease service – browse diseases flow (4-5.6)	X	X	X	X	X		x
	Browse disease – disease service flow (5.6-4)	X	X	X	X	X		x
	Patient portal - browse diseases flow (5.3-5.6)	X	X	X	X	X		x
	Patient – authN flow (1-5.9)	X	X	X	X	X		x
	authN - patient flow (5.9-1)	X	X	X	X	X		x
	Research – authN flow (2-5.9)	X	X	X	X	X		x
	authN flow – researcher (5.9-2)	X	X	X	X	X		x
	Nurse – authN flow (3-5.9)	X	X	X	X	X		x
	authN – nurse (3-5.9)	X	X	X	X	X		x
process	Patient portal (5.3)	X	X	X	X	X		x
Entity	Patient (1)	X	X	No non-repudiation or detectability threat			X	
	Researcher (2)	X	X				X	
	Nurse (3)	X	X				X	
	External disease service (4)	X	X				X	

# Assumptions

8. Identifiability of entities (researchers, nurses, patients or the external service) is not considered a threat, as all entities should have their own unique (long-term) identifier and there is no need to hide the entity's identity. Knowing that an entity is using the community service is not considered an issue.
11. Linkability of entities (sensors, cardiologists, nurses, or patients) is not considered a threat, as all entities should have their own unique (long-term) identifier and there is no need to hide the entity's identity. Knowing that an entity is using the community service is not considered an issue.

		L	I	N	D	D	U	N
Data store	PHR data (5.1)	X	X	X	X	X		x
	User data (5.2)	X	X	X	X	X		x
flow	Patient – portal flow (1 -5.3)	X	X	X	X	X		x
	Portal – patient flow (5.3-1)	X	X	X	X	X		x
	Researcher – portal flow (2-5.4)	X	X	X	X	X		x
	Portal – researcher flow (5.4-2)	X	X	X	X	X		x
	Nurse – portal flow (3-5.5)	X	X	X	X	X		x
	Portal – nurse flow (5.5-3)	X	X	X	X	X		x
	Disease service – browse diseases flow (4-5.6)	X	X	X	X	X		x
	Browse disease – disease service flow (5.6-4)	X	X	X	X	X		x
	Patient portal - browse diseases flow (5.3-5.6)	X	X	X	X	X		x
	Patient – authN flow (1-5.9)	X	X	X	X	X		x
	authN - patient flow (5.9-1)	X	X	X	X	X		x
	Research – authN flow (2-5.9)	X	X	X	X	X		x
	authN flow – researcher (5.9-2)	X	X	X	X	X		x
	Nurse – authN flow (3-5.9)	X	X	X	X	X		x
	authN – nurse (3-5.9)	X	X	X	X	X		x
process	Patient portal (5.3)	X	X	X	X	X		x
Entity	Patient (1)	X	X				X	
	Researcher (2)	X	X				X	
	Nurse (3)	X	X				X	
	External disease service (4)	X	X				X	



# Assumptions

14. Linkability and identifiability do not pose a threat to the data flows between entities (patient, nurse, and researcher) and (portal) processes because of assumptions 8 and 11
9. Identifiability of the data flow only poses a threat to one specific data flow: 5.6 ->4 (browse diseases to external disease services), as the external service should not be able to identify the patient that is using this disease browsing service.
10. Linkability of the data flow to the external disease service (5.6 -> 4) is the only linkability threat to data flows in the patient community system. Although less likely, when the patient identifiers are replaced by pseudonyms, linking the different symptoms (of different searches) together can still result in an identifiability threat
15. Linkability and identifiability do not apply to internal data flows as knowing that 2 requests belong to the same user, or knowing who made a request does not violate the patient's privacy. The patient's privacy is only violated when the content of the communication is revealed (information disclosure threat)
16. Linkability and identifiability do not apply to internal processes as knowing that 2 actions belong to the same user does not violate the patient's privacy. The patient's privacy is only violated when the content of the action is revealed (information disclosure threat)

		L	I	N	D	D	U	N
Data store	PHR data (5.1)	X	X	X	X	X		x
	User data (5.2)	X	X	X	X	X		x
flow	Patient – portal flow (1 -5.3)	X	X	X	X	X		x
	Portal – patient flow (5.3-1)	X	X	X	X	X		x
	Researcher – portal flow (2-5.4)	X	X	X	X	X		x
	Portal – researcher flow (5.4-2)	X	X	X	X	X		x
	Nurse – portal flow (3-5.5)	X	X	X	X	X		x
	Portal – nurse flow (5.5-3)	X	X	X	X	X		x
	Disease service – browse diseases flow (4-5.6)	X	X	X	X	X		x
	Browse disease – disease service flow (5.6-4)	X	X	X	X	X		x
	Patient portal - browse diseases flow (5.3-5.6)	X	X	X	X	X		x
	Patient – authN flow (1-5.9)	X	X	X	X	X		x
authN - patient flow (5.9-1)	X	X	X	X	X		x	
Research – authN flow (2-5.9)	X	X	X	X	X		x	
authN flow – researcher (5.9-2)	X	X	X	X	X		x	
Nurse – authN flow (3-5.9)	X	X	X	X	X		x	
authN – nurse (3-5.9)	X	X	X	X	X		x	
process	Patient portal (5.3)	X	X	X	X	X		x
Entity	Patient (1)	X	X				X	
	Researcher (2)	X	X				X	
	Nurse (3)	X	X				X	
	External disease service (4)	X	X				X	



# Assumptions

- 12. Information disclosure between the external disease service and the browse disease process does not pose a threat, as it does not contain any sensitive or personal information
- 19. Content unawareness only applies to the patient, as the researcher does not add any information, a nurse only registers patients, and the external disease service does not directly input any data
- 17. Identifiability and linkability are applicable to both data stores, and will therefore be examined in a combined fashion

		L	I	N	D	D	U	N
Data store	PHR data (5.1)	X	X	X	X	X		x
	User data (5.2)	X	X	X	X	X		x
flow	Patient – portal flow (1 -5.3)	X	X	X	X	X		x
	Portal – patient flow (5.3-1)	X	X	X	X	X		x
	Researcher – portal flow (2-5.4)	X	X	X	X	X		x
	Portal – researcher flow (5.4-2)	X	X	X	X	X		x
	Nurse – portal flow (3-5.5)	X	X	X	X	X		x
	Portal – nurse flow (5.5-3)	X	X	X	X	X		x
	Disease service – browse diseases flow (4-5.6)	X	X	X	X	X		x
	Browse disease – disease service flow (5.6-4)	X	X	X	X	X		x
	Patient portal - browse diseases flow (5.3-5.6)	X	X	X	X	X		x
	Patient – authN flow (1-5.9)	X	X	X	X	X		x
	authN - patient flow (5.9-1)	X	X	X	X	X		x
	Research – authN flow (2-5.9)	X	X	X	X	X		x
	authN flow – researcher (5.9-2)	X	X	X	X	X		x
	Nurse – authN flow (3-5.9)	X	X	X	X	X		x
	authN – nurse (3-5.9)	X	X	X	X	X		x
process	Patient portal (5.3)	X	X	X	X	X		x
Entity	Patient (1)	X	X				X	
	Researcher (2)	X	X				X	
	Nurse (3)	X	X				X	
	External disease service (4)	X	X				X	

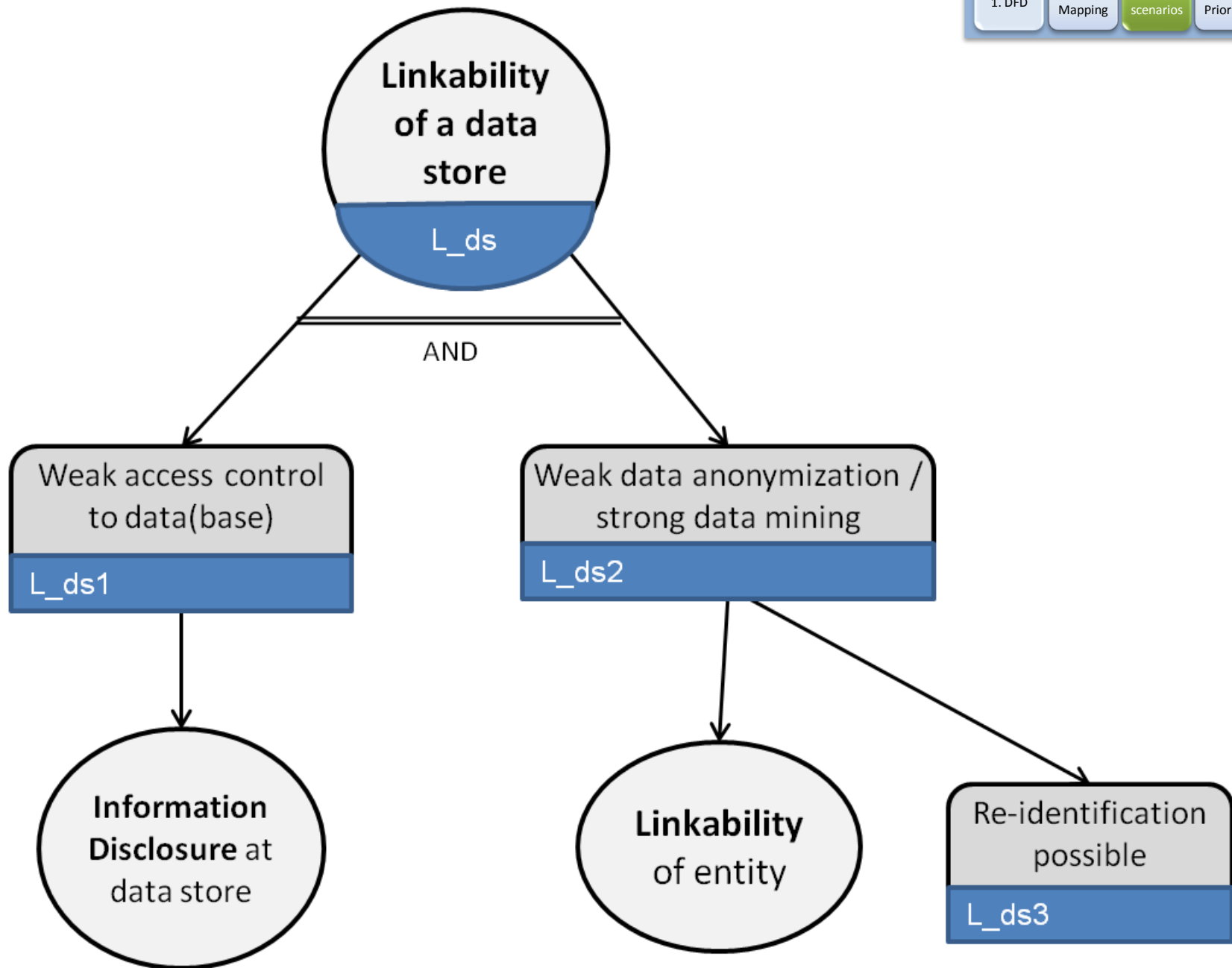
		L	I	N	D	D	U	N
Data store	PHR data (5.1)	X	X			X		x
	User data (5.2)	X	X			X		x
flow	Patient – portal flow (1 -5.3)					X		x
	Portal – patient flow (5.3-1)					X		x
	Researcher – portal flow (2-5.4)					X		x
	Portal – researcher flow (5.4-2)					X		x
	Nurse – portal flow (3-5.5)					X		x
	Portal – nurse flow (5.5-3)					X		x
	Disease service – browse diseases flow (4-5.6)					X		x
	Browse disease – disease service flow (5.6-4)	X	X					x
	Patient portal - browse diseases flow (5.3-5.6)					X		x
	process	Patient – authN flow (1-5.9)					X	
authN - patient flow (5.9-1)						X		x
Research – authN flow (2-5.9)						X		x
authN flow – researcher (5.9-2)						X		x
Nurse – authN flow (3-5.9)						X		x
authN – nurse (3-5.9)						X		x
Patient portal (5.3)						X		x
Entity	Patient (1)						X	
	Researcher (2)							
	Nurse (3)							
	External disease service (4)							110

# LINDDUN Methodology

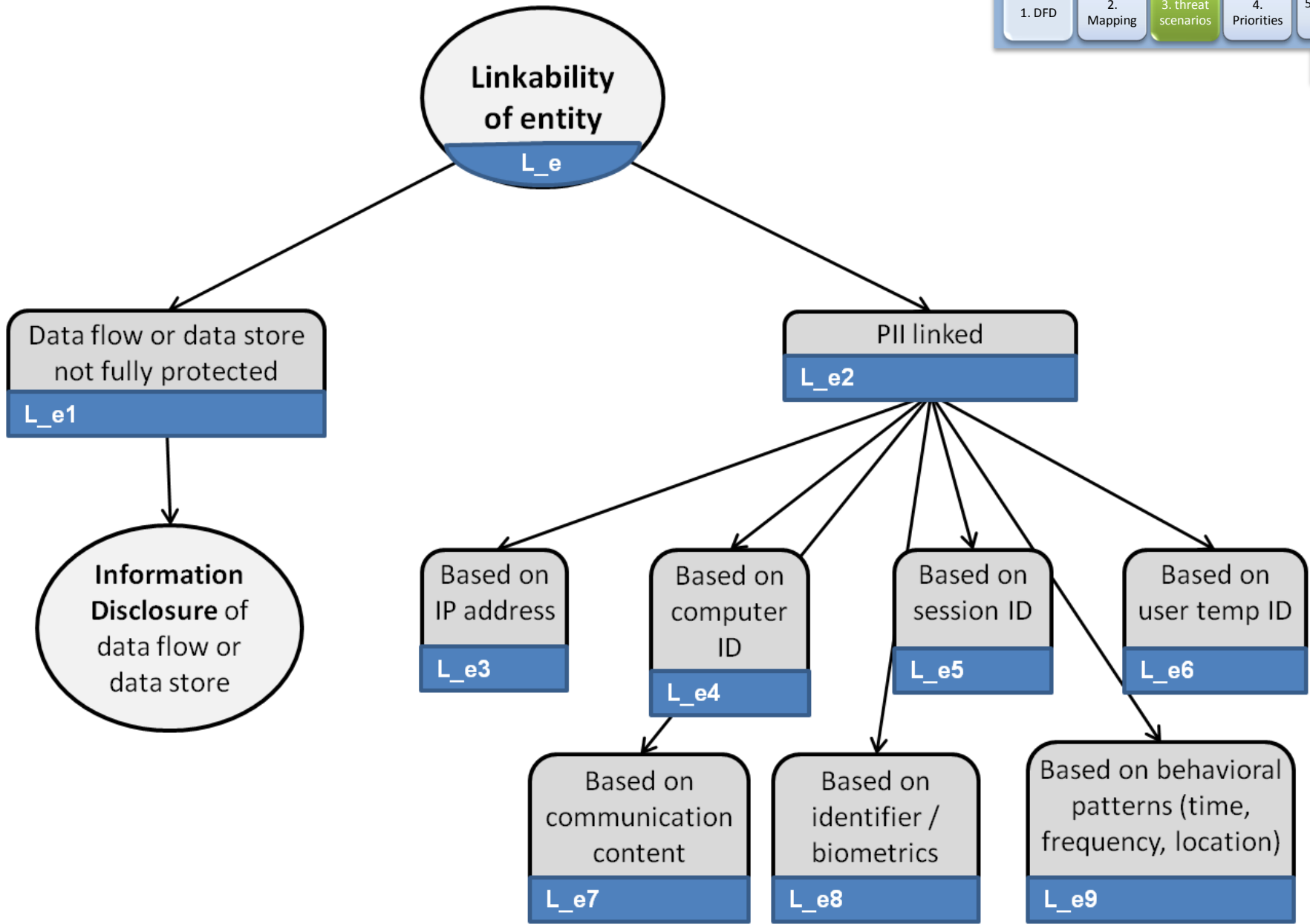
- Step 1
  - Create the DFD diagram (assets)
- Step 2
  - Map LINDDUN to DFD element types
- **Step 3**
  - **Refine threats via threat tree patterns**
  - Document assumptions
  - **Document the threats with template**
- Step 4
  - Assign priorities
- Step 5
  - Extract privacy requirements

# Linking community data

- Assumption: *Identifiability and linkability are applicable to both data stores, and will therefore be examined in a combined fashion*
- linking PHR data
  - Applies also to user data







# T01 - Profiling PHR data (linking)

**Summary:** A researcher or other insider with malicious intent links PHR data (or user data)

**Primary mis-actor:** unskilled insider (authenticated user, e.g. researcher)

**Basic path:**

bf1. The misactor performs a set of targeted queries on the PHR data or user data store and retrieves very detailed results

bf2. The misactor links the results of the queries together (e.g. based on medication which is usually combined, medical conditions which occur together, or pseudo-identifiers like street and age)

**Consequence:** By combining the query results, the misactor has access to more information about the patient than anticipated

**Reference to threat tree node(s):** L\_ds2, L\_e2

**Parent threat tree(s):** L\_ds, I\_ds

**DFD element(s):** 5.1 PHR data, 5.2 user data

**Remarks:**

r1. This threat can be used as precondition for the identifiability threat at the data store (T03 - Identifying a patient from his PHR data)

r2. This threat was inspired by L\_ds2 and L\_e2, however none of L\_e2's leaf nodes matched

r3. The (weak) access requirement (L ds1) is fulfilled because the misactor is an insider who has access to the database

r4. Although this threat mainly describes the PHR data case, it also applies to the user data store (assumption 4)

# Linking community data

- Assumption: *Identifiability and linkability are applicable to both data stores, and will therefore be examined in a combined fashion*
- linking PHR data
  - Applies also to user data
- Linking PHR data to user data

# T02 - Linking PHR data to user data

**Summary:** The administrator or other insider with access to both the PHR data store and user data store is able to link the data from both databases (and sell this information to advertisers, insurance companies, etc.)

**Primary mis-actor:** unskilled insider with access to both data stores

**Basic path:**

bf1. The misactor retrieves information from both the PHR data store and the user data store

bf2. The misactor links both sets of data (e.g. based on a shared foreign key)

**Consequence:** The combined set of data contains (possibly sensitive) personal identifiable information and especially poses a privacy threat when the misactor sells the information (e.g. to a company selling medication, to the patient's insurance company, etc.)

**Reference to threat tree node(s):** L\_ds2, L\_e6

**Parent threat tree(s):** L\_ds, I\_ds

**DFD element(s):** 5.1 PHR data, 5.2 user data

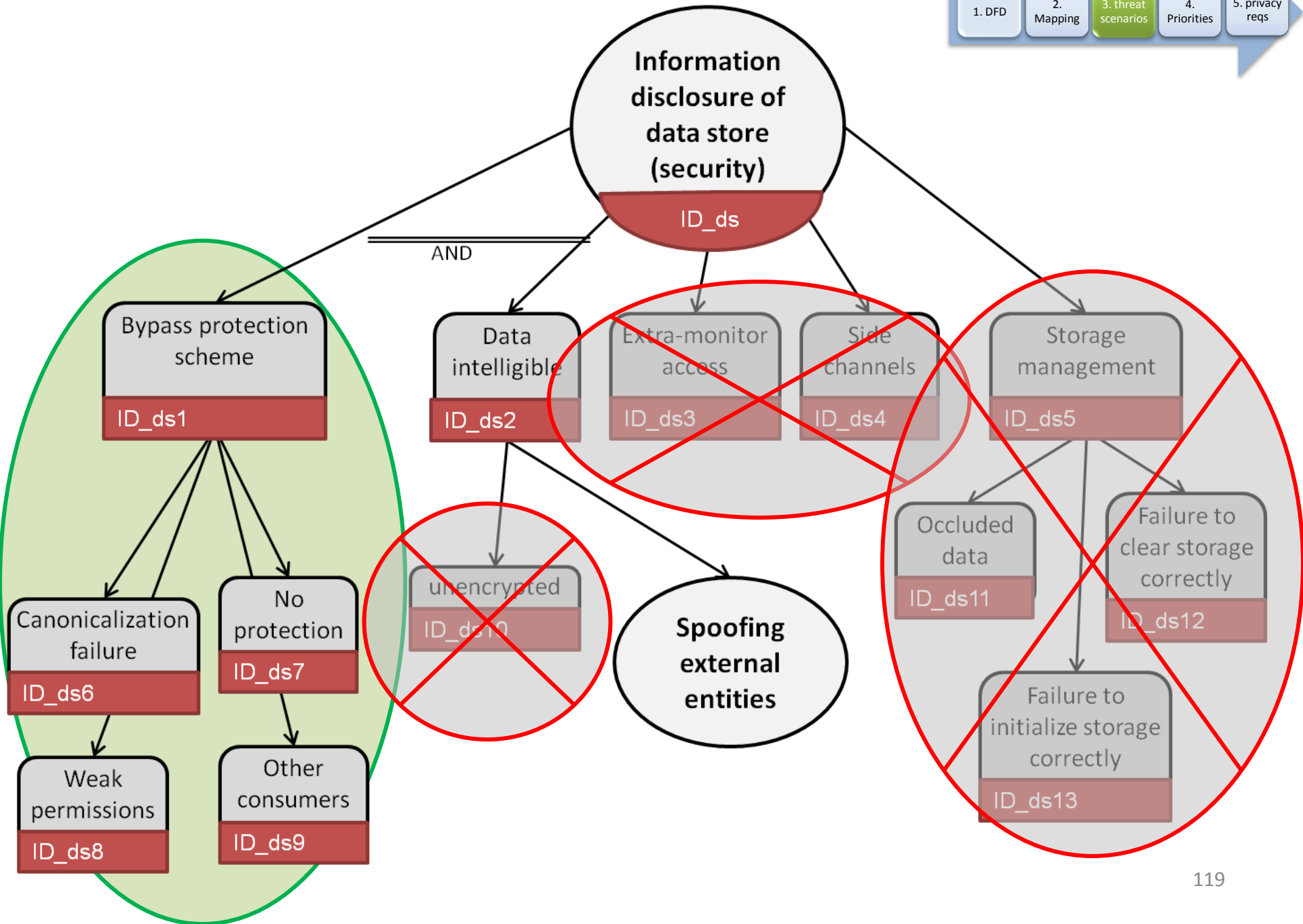
**Remarks:**

r1. The L\_ds1 requirement of (weak) access is fulfilled, as this threat only involves insiders who have access to the data stores

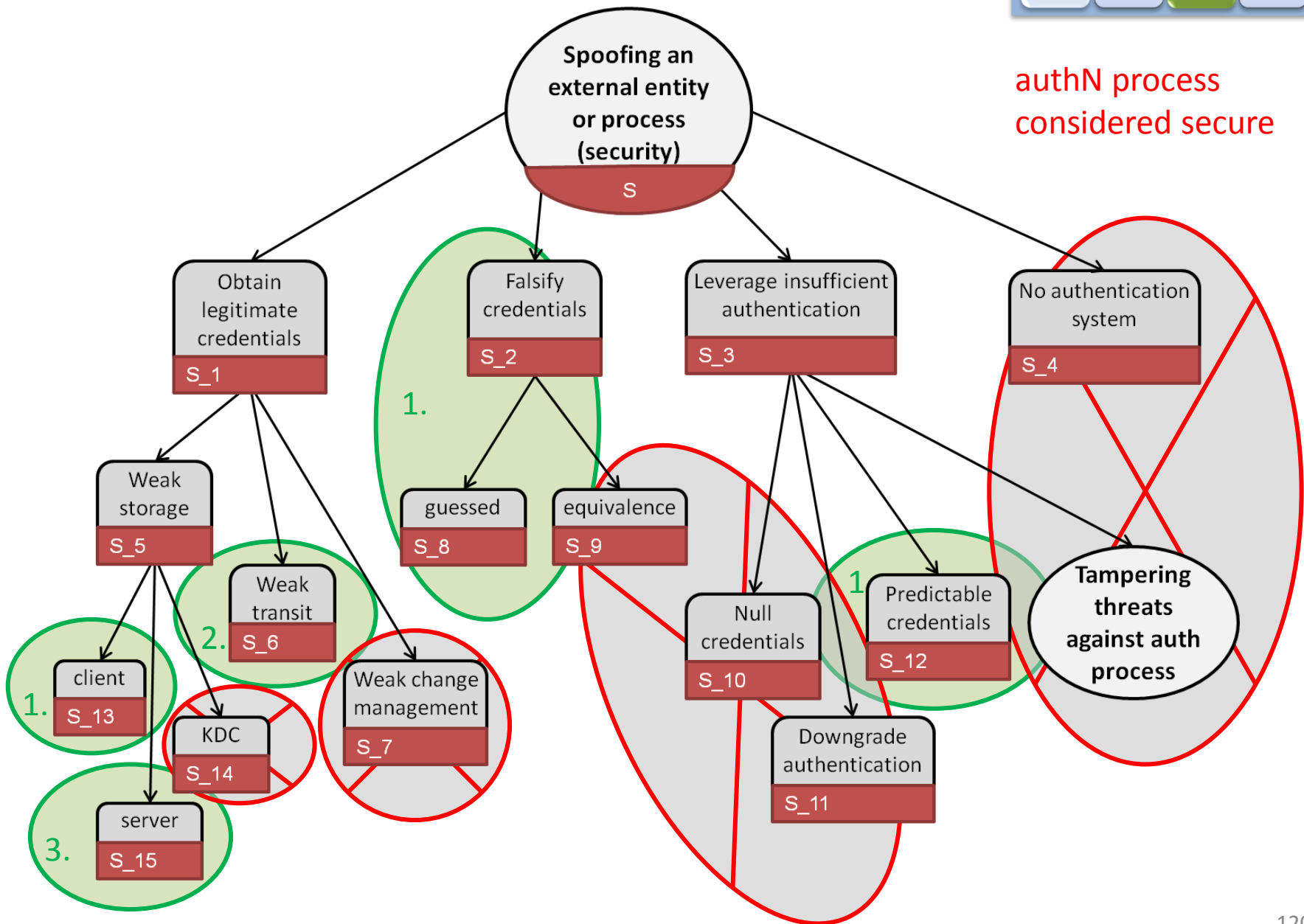
r2. The linkability of entity leaf node L\_e6, indicating linkability based on the user's temporary ID inspired to this data store linkability threat

# Information disclosure of community data

- no access control system is present (assumption 4)
- We assume that the data stores are sufficiently protected and that side-channel attacks, extra-monitor and bad storage management are not possible (assumption 20)



authN process considered secure



# Spoofing users

(patients, researchers, nurses)



- Spoofing by falsifying credentials
- Spoofing by eavesdropping communication
  - Information disclosure of transmitted credentials
  - Information disclosure of transmitted session token
- Spoofing because of weak credential storage
  - Information disclosure of community data





4. External diseases services

Disease results symptoms

5.6 Browse diseases

Disease results symptoms

1. patient

5.3 Patient portal

Request, token response

Username, password token

5.7 Manage PHR

PHR data token

validated

5.9 authN

Username password

5.2 user data

password user data

validated

5.4 Researcher portal

Query results

query

token validated

query, token

2. researcher

Query results

token

Username, password

New user data, token

user data

Username, password

3. nurse

5.5 Nurse portal

token

token

# spoofing external disease service

## Spoofing external disease service

**Summary:** The external disease service is spoofed (e.g. by a competitor or a advertising company for medication)

**Primary mis-actor:** Skilled outsider

### **Basic path:**

bf1. The misactor pretends to be the disease service

bf2. The community browse service contacts the spoofed disease service with symptoms

bf3. The misactor returns false information

**Consequence:** The patient community system returns false disease information to the patient which has an impact on the system's reputation (as one of the benefits of the provided service is the trustworthiness of the information)

**Reference to threat tree node(s):** S 4

**Parent threat tree(s):** S

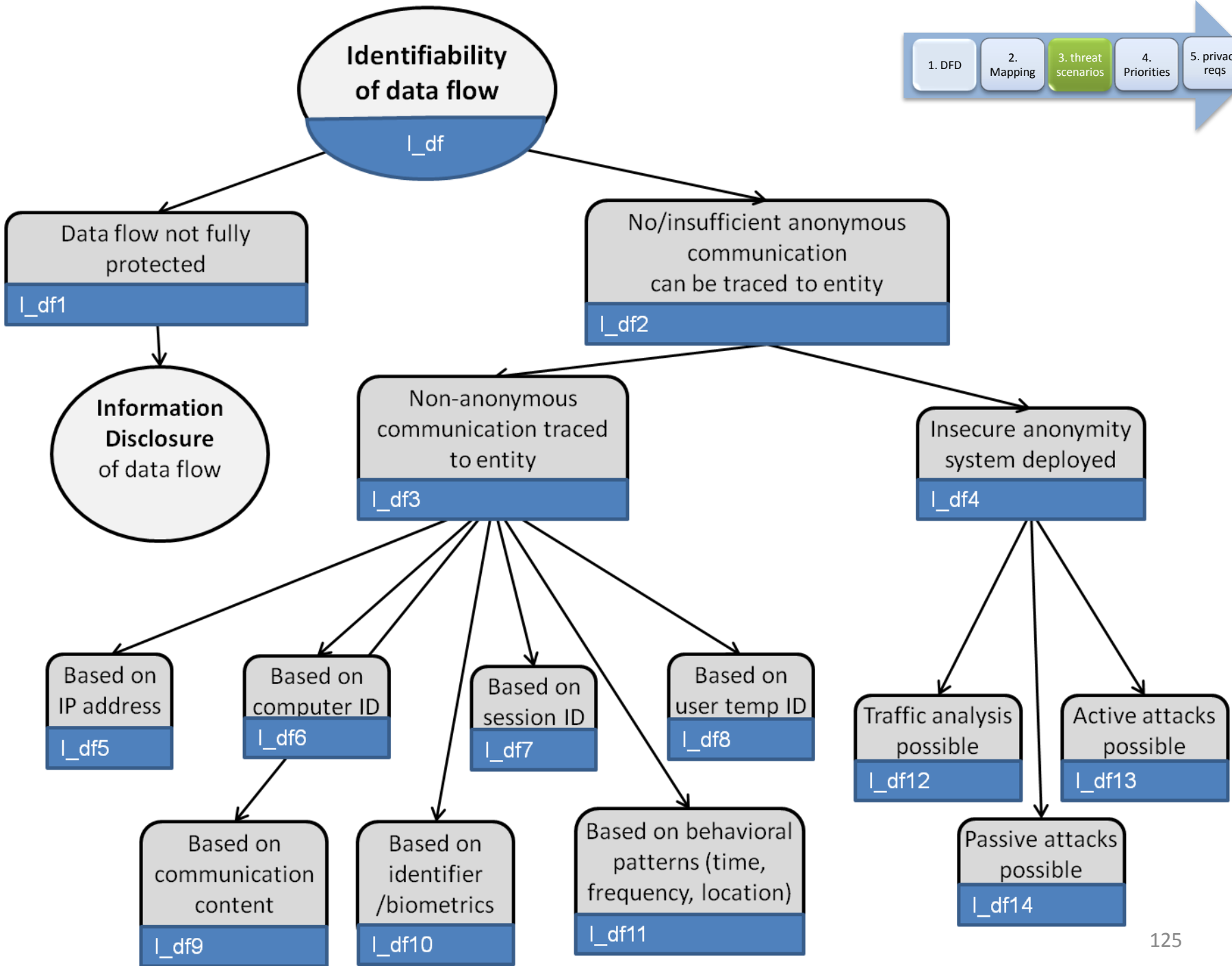
**DFD element(s):** 4. external disease service

This is **NOT** a **privacy** threat.

It is a security threat (against integrity)  
And should not be included

# External disease service

- Linkability & Identifiability of data flow
  - NOT during transit
  - When arrived at external disease service
    - Always information disclosure



# T12 - Identifiability of data sent to external disease service

**Summary:** The misactor extracts the patient's identity from the request and links it to the symptoms

**Primary mis-actor:** unskilled insider/skilled outsider

**Basic path:**

- bf1. The patient searches diseases by providing his symptoms to the patient portal, which forwards the request (include the patient's identifiable information (e.g. SSN, address, etc.) to the external disease service
- bf2. The misactor intercepts the data flow (threat T10 – Information disclosure of transmitted medical or personal data) or is (or has access to) the external disease service

**Consequence:** The misactor knows which patient has which symptoms

**Reference to threat tree node(s):** I\_df1, I\_df8

**Parent threat tree(s):** I\_df

**DFD element(s):** data flow from browse service to external disease service (5.6 -> 4)

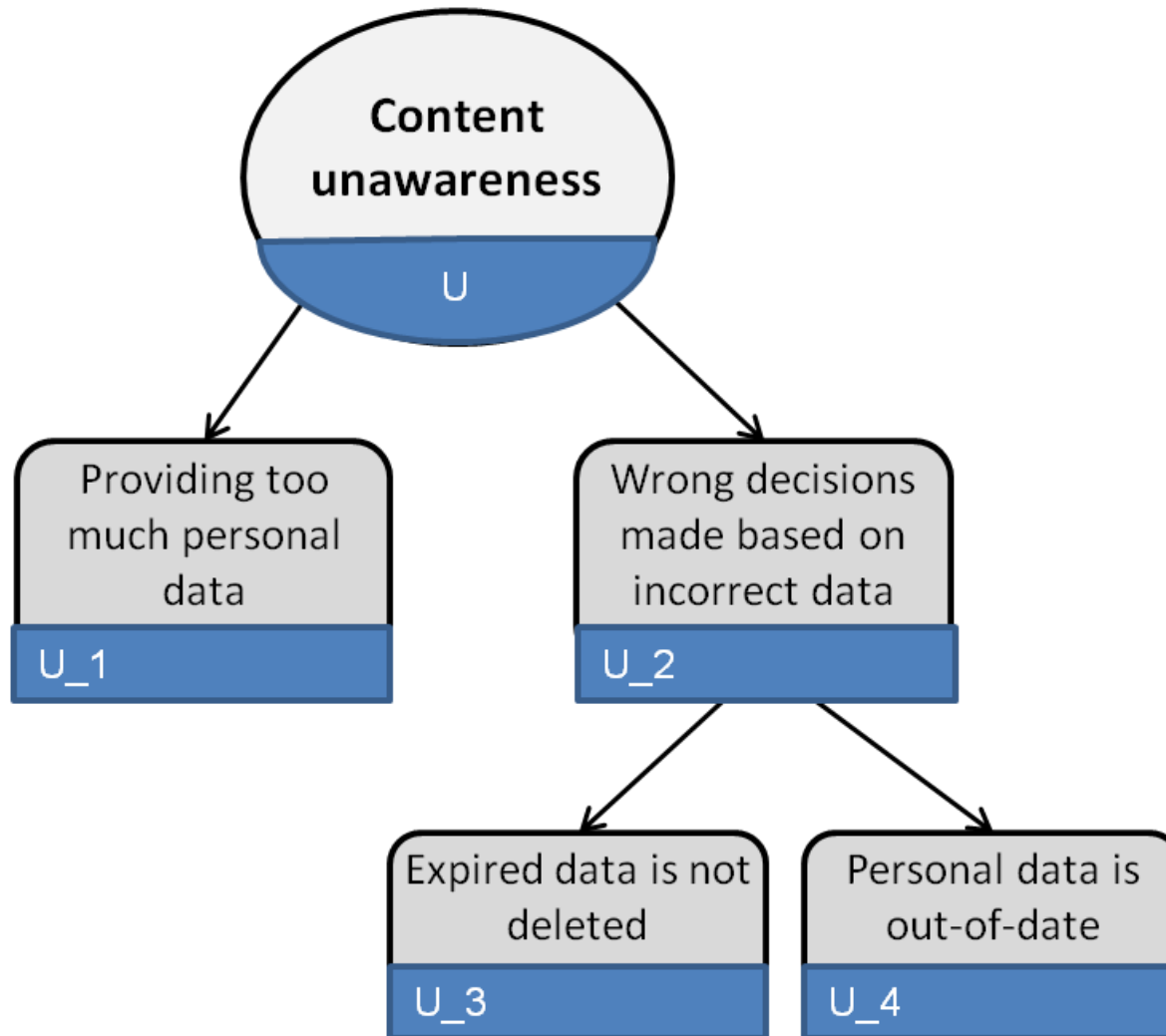
**Remarks:**

- r1. I\_df1 requires an unprotected data flow, which is currently present (assumption 3) and misactor is receiver, thus assumption always applies
- r2. The different requests are traced back based on the transmitted (temporary/internal) user ID (I\_df8)
- r3. The right branch of the tree (insecure anonymity system (I\_df4)) and the other leaf nodes of the non-anonymous communication branch (I\_df3) are not considered, as it is not the sender (browse service) whose identity should be protected, but the patient, who is not directly part of the data flow



# Soft privacy

- Non-compliance of employees
- Non-compliance of management
- Missing consent system
- Patient unawareness
- Content inaccuracy



# T19 - User unawareness

**Summary:** The user is unaware of the consequences of sharing information (e.g. by sharing too much information even anonymized data can reveal the user's identity)

**Primary mis-actor:** Management

**Basic path:**

bf1. The management fails to add as requirement the need of notifications and warnings when the patients intends to upload sensitive and/or identifiable content (e.g. picture of his broken arm which also shows his face)

bf2. The user adds information to the system which can easily identify him (e.g. a picture of himself) as he is unaware of the consequences

bf3. Group members retrieve information and can still identify the pseudonymized user

**Consequence:** When group members retrieve information, the identifiable information. The user's privacy is violated as he assumes that his information stays confidential and his identity will not be revealed

**Reference to threat tree node(s):** U 1

**Parent threat tree(s):** U

**DFD element(s):** 1 patient

**Remarks:**

r1. This threat only applies to the patient (assumption 19)

r2. The threat concerning inaccurate user information is described in T20 - content inaccuracy





# LINDDUN Methodology

- Step 1
  - Create the DFD diagram (assets)
- Step 2
  - Map LINDDUN to DFD element types
- Step 3
  - Refine threats via threat tree patterns
  - Document assumptions
  - Document the threats with template
- **Step 4**
  - **Assign priorities**
- Step 5
  - Extract privacy requirements

Information disclosure and identifiability of stored data violate privacy more than disclosure of “partial” transmitted data

# Priorities

## High

- T04 - Information disclosure of patient community data
- T03 - Identifying a patient from his PHR data
- T08 - Disclosure of the transmitted log-in credentials
- T09 - Disclosure of the transmitted session token
- T10 - Disclosure of transmitted medical/personal information
- T05 - Spoofing a user of the social network system by falsifying credentials
- T07 - Spoofing a user of the social network system because of weak credential storage
- T06 - Spoofing a user of the social network system by eavesdropping communication

Spoofing leads to information disclosure which is a high risk threat

Data in system is purely informative, and not used for important decisions, thus impact of threat is low

## Low

- T16 - Non-compliance of employees
- T20 - content inaccuracy
- T14 - Information disclosure internal process
- T13 - Disclosure of internal transmitted medical/personal information
- T15 - Side channel information disclosure internal process

There is a trust relationship with the employees, thus likelihood of threats is low

## Medium

- T12 - Identifiability of data sent to external disease service
- T11 - Linkability of symptoms sent to external disease service
- T01 - Profiling PHR data (linking)
- T02 - Linking PHR data to user data
- T18 - Non-compliance management
- T17 - Missing user consents
- T19 - User unawareness

Only partial data and patient deniability

Linkability can lead to identifiability

Non-compliance can still have “part” in place + reputation

# LINDDUN Methodology

- Step 1
  - Create the DFD diagram (assets)
- Step 2
  - Map LINDDUN to DFD element types
- Step 3
  - Refine threats via threat tree patterns
  - Document assumptions
  - Document the threats with template
- Step 4
  - Assign priorities
- **Step 5**
  - **Extract privacy requirements**

# Threats to requirements

## T01 - Profiling PHR data

- A researcher or other insider with malicious intent links PHR data or user data
  - e.g. based on medication which is usually combined, medical conditions which occur together, or pseudo-identifiers like street and age

Threats (misuse cases)	Caused by (leaf nodes)	Mitigated by (requirements)
Profiling PHR data	Weak data anonymity (in the data store)	Apply strong data anonymization techniques in the database (for storage)
	PII linked (after retrieval)	Apply data anonymization techniques on query results (for information retrieval)

# Documenting requirements

Requirements	Threats
Apply strong data anonymization techniques in the database (for storage)	T01-Profiling PHR data (weak data anonymity in the data store), T03- identifying a patient from his PHR data
Apply data anonymization techniques on query results (for information retrieval)	T01-Profiling PHR data (PII linked after retrieval)
...	...

LINDDUN - Privacy threat analysis

# PROJECT

<http://people.cs.kuleuven.be/~kim.wuyts/ERISE>

# Questionnaires

- Entry questionnaire
  - **Before** you start the working on the assignment
  - Understand your background
- Exit questionnaire
  - **After** you have turned in your report
  - Getting your feedback
- You can stay anonymous if so desired
- Please, fill in per student (not per team)
- Links are provided in the instructions



# Online threat tree catalog

• [home](#)

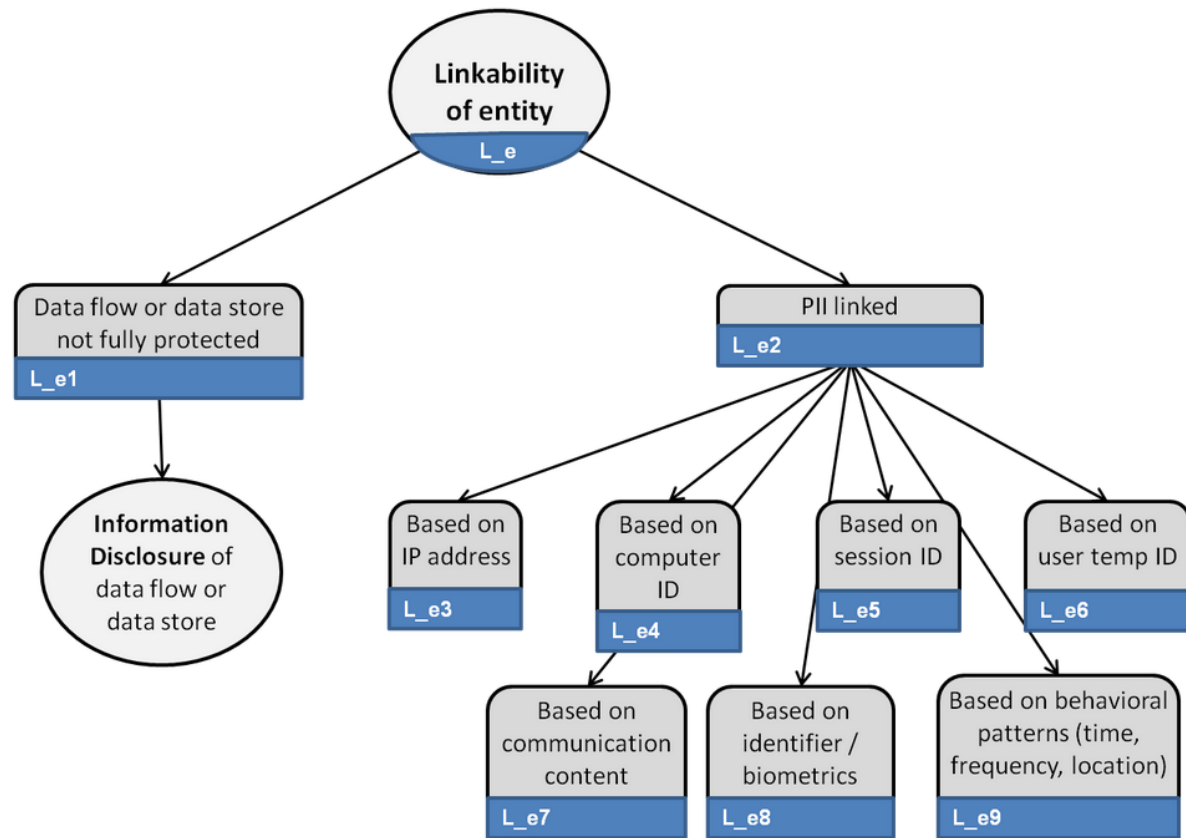
## Linkability of an entity

### LINDDUN threats

- Entity
  - [Linkability of entity](#)
  - [identifiability of entity](#)
  - [content unawareness of entity](#)
- Data flow
  - [Linkability of data flow](#)
  - [identifiability of data flow](#)
  - [non-repudiation of data flow](#)
  - [detectability of data flow](#)
  - [information disclosure of data flow](#)
  - [policy and consent non-compliance](#)
- Data store
  - [Linkability of data store](#)
  - [identifiability of data store](#)
  - [non-repudiation of data store](#)
  - [detectability of data store](#)
  - [information disclosure of data store](#)
  - [policy and consent non-compliance](#)
- Process
  - [Linkability of process](#)
  - [identifiability of process](#)
  - [non-repudiation of process](#)
  - [detectability of process](#)
  - [information disclosure of process](#)
  - [policy and consent non-compliance](#)

### STRIDE threats

- Entity
  - [Spoofing an entity](#)
- Data flow
  - [information disclosure of data flow](#)
  - [tampering with a data flow](#)
- Data store
  - [information disclosure of data store](#)
  - [tampering with a data store](#)
- Process
  - [information disclosure of process](#)
  - [tampering with a process](#)
  - [elevation of privilege of a process](#)



Linkability of entity refers to an attacker who can sufficiently distinguish whether two or more entities are related or not within the system. This implies that different pseudonyms can be linked to each other. One precondition is that data flow or data store is not fully protected (e.g. unencrypted), which leads to the Information Disclosure threat of data flow and data store. The second precondition is that Personal Identifiable Information (PII) can be linked, e.g. based on user temporary ID, IP address, behavioral patterns such as time, frequency and location, session ID, identifier and biometrics, computer ID, communication content or any combination of these factors. The aforementioned data store refers to the identity management system's database or any other database which contains personal identifiers of users. Having accessed such a data store, the attacker could easily link different pseudonyms to the same user.

# eRISE - Report structure

## 1. TARGET OF EVALUATION

This section should describe the part of the use case that you have analyzed and the assumptions you have made during the analysis.

## 2. METHOD APPLICATION

This section should document how you have followed the steps of the security requirements and risk methods.

## 3. SUMMARY OF RESULTS

This section should summarize for each assets, the threats and the security/privacy requirements that mitigates the threats.

ASSET	THREAT	SECURITY/PRIVACY REQUIREMENT

- Scope use case (if applicable)
- list all assumptions made

1. DFD
2. mapping table (if possible with reference to threats)
3. threats (following template)
4. prioritization
5. requirements (table with link to threats)

link to assumptions

*Framework for augmented interaction in UCARL: in Proceedings of the 16th Annual ACM Symposium on User Interface Software and Technology (Vancouver, Canada, November 02 - 05, 2003). UIST'03. ACM, New York, NY, 1-10. DOI= <http://doi.acm.org/10.1145/964696.964697>.*