LINDDUN GO

DistriNet

CONTENTS

ABOUT

LINDDUN GO is designed to give you a quick start to privacy threat modeling. It is a threat modeling approach structured according to LIND(D)UN threat categories. It aims to provide structured, yet light-weight support for threat modeling.

LIND(D)UN stands for: Linkability, Identifiability, Non-repudiation, Detectability, Disclosure of information*, Unawareness, and Non-compliance.

* Disclosure of information is a security category. It is not included here, as LINDDUN GO focuses on privacy. We however advise to combine LINDDUN with security threat modeling [Shostack14, EoP], as privacy highly depends on security.

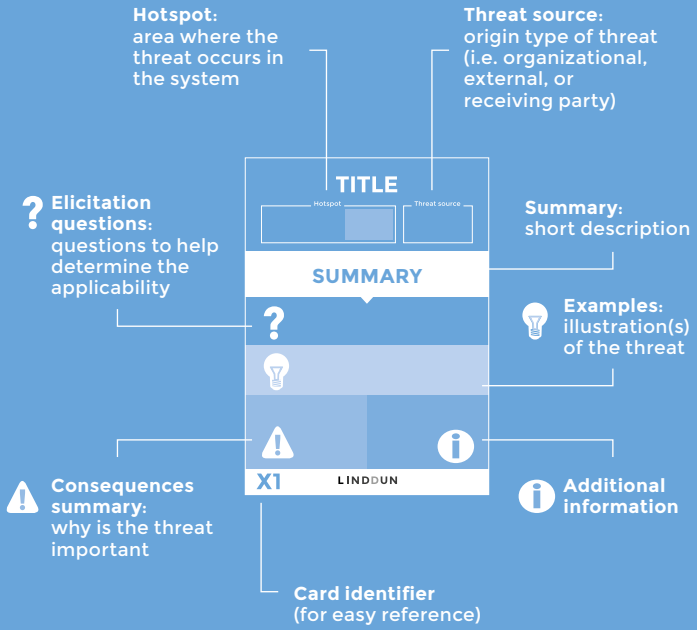
More information on each category can be found on the (bright-colored) LINDDUN GO threat category cards.

Visit our website to learn more about LINDDUN: www.linddun.org

LINDDUN GO

THREAT TYPE CARDS

Each threat type card consists of the following information



LINDDUN GO

INSTRUCTIONS

1 **Gather a group of 2-5 people who want to assess the privacy of a software architecture.**

2 **Draw a diagram of the system you want to threat model.** Make sure it contains at least elements that correspond to the hotspot types (see hotspots card) as you will need to iterate over each of these in the next step.

3 **Take turns picking a card.** For each drawn card, take turns to identify a relevant applicable threat.

- Read the drawn card.
- Systematically iterate over each corresponding hotspot on the system diagram and answer the two questions (if unsure, assume 'yes').
  - Q1 (could it be done?) helps to determine whether the prerequisites of the threat are fulfilled and the threat could occur.
  - Q2 (would it be a problem?) helps to assess whether the threat is actually applicable.
  - When you can answer 'yes' to both questions for one specific hotspot, you have found a threat. Great! Don't forget to document it.
- Continue iterating over the other applicable hotspots until no one can identify any new threat that corresponds to the card (i.e. you finished an entire round without newly identified threats).

4 **You are finished when all cards are examined.**

ALTERNATIVES

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

HOTSPOTS

A hotspot is an area of interest in the system where a specific threat can originate.

FLOWS TO/FROM SYSTEM

If unspecified, system can communicate both with external entities and (external) processes

INBOUND

OUTBOUND

IN/OUTBOUND

INBOUND FROM USER

OUTBOUND TO USER

IN/OUTBOUND WITH USER

DATA STORAGE

STORE

RETRIEVE

PROCESSING

PROCES

PROCESSING ON BEHALF OF USER

P indicates that **PERSONAL DATA** are involved
C indicates that **USER CREDENTIALS** are involved

E.G.: User sends personal data to system 

LINDDUN GO

THREAT SOURCES

In contrast to security threat modeling, privacy threats do not require an (external) attacker.

Three main threat sources are considered in LINDDUN GO:

- Organizational: Either the organization as a whole does not respect the data subject's privacy (i.e. by collecting, processing, storing or sharing personal data in a privacy-violating way) or an authorized employee/user (ab)uses personal data in a privacy-intrusive way. (whether it was intentional or not)
- External: misactor external to the system, who has gained access to (or can observe) communication or stored data (typically without authorized, unless specified otherwise).
- (future) receiving party: receiving end of the communication, or future receiving end (follow the interactions to see where the data can end up)

Note that all Linkability and Identifiability threats described for an organizational threat source, also apply to actors who have legitimate access to the system and to external actors when there is an information disclosure breach in the corresponding hotspot.

PRIVACY TERMINOLOGY

- **Attributes:** a quality or characteristic of an entity or an action [PH2010]. Basic building blocks of personal data.
- **Credentials:** personal data used to authenticate a user (e.g. username-password combination)
- **Data subject:** person whose data are being collected and processed
- **De-identified (or anonymized) data:** personal data of which certain identifying properties are removed or minimized, which reduces the chance of identification
  (more on de-identification in [NIST8053])
- **Identifier:** sufficient (set of) attribute(s) to identify the data subject
- **IOI (item of interest) / data item:** see *personal (identifiable) data*
- **Non-personal data:** data not tied to any person. Facts. (e.g. the weather in New York, the current time in Brussels, etc.)
- **Personal (identifiable) data:** any information related to an identified or identifiable individual [GDPR]
- **(Personal) identified data:** personal information that is directly tied to the identity of a natural person
- **Quasi-identifier:** piece of information that, on its own, is not a unique identifier, but can be combined with other quasi-identifiers to create a unique identifier

REFERENCES

The following sources have been an inspiration for LINDDUN GO:

[DWS+11] Deng, M., Wuyts, K., Scandariato, R., Preneel, B., Joosen, W. (2011). A privacy threat analysis framework: supporting the elicitation and fulfillment of privacy requirements. In Requirements Engineering.

[EoP] Shostack, A. (2012). Elevation of privilege: Drawing Developers into Threat Modeling. white paper, Microsoft.

[GDPR] Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data, and repealing Directive 95/46/EC (General Data Protection Regulation)

[NIST8053] Garfinkel S.L., NIST. (2015). IR 8053, De-Identification of Personal Information, US Department of Commerce.

[PH2010] Pfitzmann, A., & Hansen, M. (2010). A terminology for talking about privacy by data minimization: Anonymity, unlinkability, undetectability, unobservability, pseudonymity, and identity management (v0.34)

[SHOSTACK14] Shostack, A. (2014). Threat modeling –designing for security, Wiley.

[STRIPED] Logmein (2018). STRIPED – Elevation of Privilege privacy extension

[TRIM] F-Secure (2018). Elevation of Privacy - Elevation of Privilege privacy extension

[WP29] Article 29 Data Protection Working Party (2014). Opinion 05/2014 on Anonymisation Techniques (0829/14/EN WP216)

[WSJ15] Wuyts, K., Scandariato, R., Joosen, W. (2014) LIND(D)UN privacy threat tree catalog, CW Reports CW675, Department of Computer Science, KU Leuven

LINKABILITY

What?

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

Tell me more!

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

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

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

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

So what?

Can result in:

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

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

Identifiability
Link data items to identity of data subject.

LINDDUN GO

LINKABILITY

FLOWS TO/FROM SYSTEM

INBOUND

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

OUTBOUND

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

DATA STORAGE

STORE

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

RETRIEVE

The retrieved data can be linked to other data items

LINDDUN GO

IDENTIFIABILITY

What?

Being able to sufficiently identify the subject within a set of subjects (i.e. the anonymity set). [PH2010]

Tell me more!

Data items can be linked to the identity of the data subject, with a certain probability.

Examples: identifying the reader of a web page, the sender of an email, the person to whom an entry in a database relates, etc.

So what?

When personal data can be identified, they require even stricter security measures. Identified data can also result in unawareness and non-compliance issues.

IDENTIFIABILITY

FLOWS TO/FROM SYSTEM

INBOUND

The system can identify personal data it receives

OUTBOUND

The receiving parties can identify the received personal data

DATA STORAGE

STORE

The system stores personal data that can be identified

RETRIEVE

The retrieved data can be identified

LINDDUN GO

NON-REPUDIATION

What?

A data subject cannot deny they know, have done or have said something.

Tell me more!

There is evidence that can link the data subject to a certain action.

Examples: unable to deny being a customer of a certain webshop, unable to deny having filed a complaint, a user of an online voting system is unable to deny whom they voted for, etc.

Identifiability (and linkability) threats will increase the risk of non-repudiation.

Note that non-repudiation is actually a security goal. This should however not result in any conflicts, as (parts of) a system that requires non-repudiation as a security goal, should not need plausible deniability for the same data.

So what?

Non repudiation leads to data subject accountability: when a person is not able to repudiate an action or piece of information, he can be held accountable (e.g. a whistleblower can be prosecuted).

LINDDUN GO

NON-REPUDIATION

FLOWS TO/FROM SYSTEM

INBOUND

The sending party cannot deny use of the system

OUTBOUND

The receiver cannot deny receipt of a message

DATA STORAGE

STORE

The data subject cannot deny storage of their data

RETRIEVE

The retrieved data cannot be denied by the data subject

LINDDUN GO

DETECTABILITY

What?

Being able to sufficiently distinguish whether an item of interest (IOI) exists or not. [PH2010]

Tell me more!

Without having access to the data, the threat actor knows it exists. Existence of data is sufficient to infer more (sensitive) information.

Examples: By detecting that a celebrity has a health record in a rehab facility, one can infer the celebrity has an addiction, even without having access to the actual record.

So what?

Detectability can lead to the deduction of personal data. This information can be used to extend a data subject's profile (linkability) and/or identify the data subject.

DETECTABILITY

FLOWS TO/FROM SYSTEM

INBOUND

OUTBOUND

An external party can detect in- or outbound communication

DATA STORAGE

STORE

Stored data can be detected

RETRIEVE

Query responses reveal existence of data

LINDDUN GO

UNAWARENESS

What?

A data subject is unaware of, or unable to intervene in, the collection and further processing of their personal data.

Tell me more!

Unawareness relates to data subject rights and therefore focuses on transparency (or predictability) and intervenability (or manageability) threats.

Lack of transparency: a data subject is not aware of collection and/or processing of personal data related to them.

Examples: no notice is provided before collection, data subject is not informed of 3rd party sharing, etc.

Lack of intervenability: a data subject cannot access or manage their own personal data (including managing access settings).

Examples: data subject cannot access own data or cannot request rectification of data, data subject cannot (easily) update privacy settings, etc.

So what?

Unawareness leads to a violation of fundamental data subject rights.

UNAWARENESS

FLOWS TO/FROM SYSTEM

INBOUND

There is a lack of transparency and intervenability provided to the data subject at collection time

DATA STORAGE

STORE

A data subject cannot sufficiently intervene in their stored data

PROCESS

PROCESS

There is a lack of transparency and intervenability provided to the data subject w.r.t. the processing of personal data

LINDDUN GO

NON-COMPLIANCE

What?

The system does not comply with data protection principles.

Tell me more!

Data protection processing principles include:

- purpose limitation
  only collect and process data for the pre-determined purpose
- Proportionality
  Only collect and process the minimal set of data required for the purpose
- Storage limitation,
  Only store data for as long as required for the purpose
- ...

Note that this category is mainly influenced by EU's GDPR, but the general principles apply independent of a specific region or legislation.

So what?

Data protection principles are designed to protect the data subjects' privacy. They should always be implemented.
In addition, violation of these legal obligations can result in large fines and reputation damage.

NON-COMPLIANCE

FLOWS TO/FROM SYSTEM

INBOUND

Data protection principles are violated at collection time

DATA STORAGE

STORE

Storage of data is not limited to its minimum requirements (duration + amount of data)

PROCESS

PROCESS

Processing activities lack lawful ground and/or purpose, or other data protection principles

LINDDUN GO

LINKABILITY OF CREDENTIALS

Hotspot

INBOUND
USER INTERACTION
SENDING CREDENTIALS
(AUTHENTICATED USER)

Threat source

ORGANIZATIONAL

Actions and data can be linked by re-using credentials (for multiple system interactions).

1. Is the system using the user credentials for tracking?
2. Is it a problem if the system tracks the user (i.e. should credentials only be used to gain access to the system)?

- An email address is used as login for multiple services.
- Rather than only using a customer's credentials to authenticate (and register a purchase), an e-shop links the user's credentials to his product page views and thereby builds a user profile.

- Linking multiple actions leads to profiling, which can impact the user (both negatively and positively).
- Linking also leads to identifiable personal data (e.g. types of purchases).

- Unless anonymous/ one-time credentials are used, credentials are always linkable.
- Relates to unawareness (U1) and non-compliance (Nc1).

LINKABLE USER ACTIONS

Hotspot

INBOUND USER INTERACTION (UNAUTHENTICATED USER)

Threat source

ORGANIZATIONAL

The requests to the system are linked based on the user's data and/or actions (who assumes he is anonymous).

1. Does an unauthenticated user interact with the system (assuming his actions are not linkable)?
2. Can the system link multiple requests (i.e. are actions or requests by the user sufficiently unique to link to another session) and is this a problem?

- Specific search queries (e.g. destination and date) can be linked to a previous session on a travel website (which can result in a higher price, other search results, ...).
- Even when a user is not logged in, his browsing pattern is sufficiently unique to link it to his (registered) profile.
- A review system for restaurants also links an authenticated user to (his visit to) the restaurant (to build a user profile).

- Linking might lead to identifiability (I2).
- Linking multiple actions can lead to profiling (of one person or of groups with similar habits).

- Profiling threats also apply to authenticated users.
- The more information, the more unique.

LINKABILITY OF INBOUND DATA

Hotspot

INBOUND FLOW CONTAINING **PERSONAL DATA**

Threat source

ORGANIZATIONAL

The data sent to the system are linked to already collected data of the same or other data subjects (from same or other source).

1. Does the flow contain personal data?
2. Does (or can) the system link these data (i.e. are data items sufficiently unique to link to each other) in a privacy-violating way?

- Data subject shares minimal set of information (e.g. city instead of full address), yet given the information already available (e.g. only 1 person of that city in the system), the data can be easily linked.

- Information can be deduced based on the linked data (inference).
- Threat depends on the knowledge of the organization.

- The data subject is not necessarily the sender of the data.
- Linkability of credentials (L1) and actions (L2) are subtypes of this threat.

L3

LINDDUN

LINKABILITY OF CONTEXT

Hotspot

INBOUND USER INTERACTION (UNAUTHENTICATED)

Threat source

ORGANIZATIONAL/ EXTERNAL

The contextual information (i.e. metadata) of the communication are linked (to create a user 'profile').

1. Are there contextual data that can link accesses? (probably yes)
2. Is it a problem if accesses to the system can be linked (by the organization or by an observer)?

- Contextual information that can be used to link data includes: IP addresses, browser settings, acess times, etc.
- Contextual information can link multiple accesses to reveal a usage pattern (e.g. social media after the same tv show).

- Organizational: high likelihood as communication metadata are (usually) available.
- External: rather low impact and likelihood, unless there is a sensitive context.

- Organizational: linked actions can be treated differently (e.g. higher rates for recurring actions).
- External: requires detectability of communication metadata (D2,3) (always possible for regular (non-anonymous) communication).

LINKABILITY OF SHARED DATA

Hotspot

OUTBOUND FLOW CONTAINING **PERSONAL DATA** (RECEIVER IS NOT DATA SUBJECT)

Threat source

RECEIVING PARTY

Content communicated to external party can be linked by receiving party.

1. Are the shared data expected to be anonymous or unlinkable?
2. Can shared data be linked to previously obtained data? (if unknown, assume it is possible.)

A third party service is used as expert knowledge base. To easily forward asynchronous responses to the correct user, the system provides the user's internal identifier which allows the third party service to link all requests of the same user.

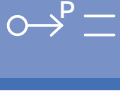
- Linkability can lead to profiling and identifiability (I4)
- Depends on knowledge of the receiving party.
- The more shared attributes, the higher the risk.

- When assuming data were fully de-identified, also non-compliance (Nc3) and unawareness (U1) threats will arise.
- If the shared data originate from a database, the threat can also be categorized as 'linkability of retrieved data (L7)'.

LINKABILITY OF STORED DATA

Hotspot

STORE PERSONAL DATA



Threat source

ORGANIZATIONAL

Personal data being stored are linkable (because they are insufficiently minimized before storage).

1. Are data stored with unique attributes?
2. Can (attributes of) the data item(s) be reduced (e.g. removed, de-identified, decentralized, ...)?

The system received a set of raw data. Only the aggregated set of data is required, yet they are stored per individual data subject.

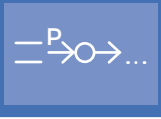
- Linkable data can lead to profiling, inference and identifiability.

- If all attributes are required for at least one process, the data can not be minimized/ de-identified. (but might be de-centralized).
- Closely related to minimization (Nc5).

LINKABILITY OF RETRIEVED DATA

Hotspot

RETRIEVE PERSONAL DATA (RECEIVING PARTY IS NOT DATA SUBJECT)



Threat source

(FUTURE) RECEIVING PARTY /ORGANIZATIONAL

Retrieved personal data are linkable to previously obtained data (possibly from a different source).

1. Are personal data being retrieved assumed to the be de-identified?
2. Can the receiving party link more information than they require? (if unknown, assume yes)

- While a database only allows queries on a limited number of attributes at a time, targeted queries can return linkable results (based on unique attributes).
- Sensor data are temporarily buffered before being sent to the back-end. Rather than sending an aggregated set, the back-end can retrieve the entire dataset.

- Can lead to identifiability (the more data, the more unique).
- Likelihood (mainly) depends on the knowledge of the receiving party.

- It is difficult to ensure unlinkability of query results.
- Quasi-identifiers can be sufficiently unique to link to other data.
- Related to minimization (Nc1,3,5).

L7 LINDDUN

IDENTIFYING CREDENTIALS

Hotspot

INBOUND
USER INTERACTION
SENDING CREDENTIALS
(AUTHENTICATED USER)

Threat source

ORGANIZATIONAL

The use of (non-anonymous) credentials allows identification of the user.

1. Do the credentials contain identifiable info?
   (e.g. e-ID, company email address, biometrics)
2. Is it a problem if the user is identified (i.e. should credentials only be used to gain access to the system)?

A user is required to register with his full name and address to access a newspaperwebsite allowing identification of webpage views.
Examples of identifying credentials include: email address with full name, e-ID, biometrics, too specific attributes of (anonymous) credentials, etc.

- When data are identified rather than identifiable, stronger security measures need to be in place.

- Relates to non-compliance (Nc1) and unawareness (U1).

ACTIONS IDENTIFY USER

Hotspot

INBOUND
(UNAUTHENTICATED)
USER INTERACTION

Threat source

ORGANIZATIONAL

The user is identified via his requests to the system.

1. Can requests (i.e. actions or data) be sufficiently unique to identify the user?
2. Is it a problem if the user is identified based on their actions?

- Extensive queries to a search engine can be used to identify the user that constructed the query.
- An anonymous user sends identifiable data about him/herself to the system.

- Likelihood depends on the previously obtained knowledge of the organization w.r.t. the user.

- Although the user is not identifying with credentials, their actions (and/or the data being sent) are sufficient to identify the user.
- Relates to non-compliance (Nc1) and unawareness (U1).

IDENTIFYING INBOUND DATA

Hotspot

INBOUND
FLOW CONTAINING
PERSONAL DATA

Threat source

ORGANIZATIONAL

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

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

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

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

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

IDENTIFYING CONTEXT

Hotspot

INBOUND USER INTERACTION (UNAUTHENTICATED/ ANONYMOUS)

Threat source

ORGANIZATIONAL/ EXTERNAL

The contextual information of the communication (i.e. metadata) can be identified, while the user assumes anonymous interaction.

1. Are there contextual data available that can be identified or can be linked to identified data?
2. It is a problem if the user's communication is identified (by the organization or by someone external)?

- An e-shop tracks a user's access. John Doe accesses the website every Monday around 10PM (but only sporadically purchases something). Even when John is not logged in, the shop can identify John based on his contextual data (with a certain likelihood).
- An external misactor want to identify who of his neighbors accesses a certain service with sensitive content (he can verify who is home at that time, etc.).

- likelihood depends on previous knowledge.
- Organizational: User can be identified while assuming anonymity.
- External: Low impact, unless sensitive context.

- Organizational: Relates to unawareness (U1), and non-compliance (Nc1).
- External: Without access to content, attacker can identify communication (requires detectability of channel (D2,3)).

IDENTIFYING SHARED DATA

Hotspot

OUTBOUND FLOW CONTAINING **PERSONAL DATA** (RECEIVER IS NOT DATA SUBJECT.)

Threat source

RECEIVING PARTY

Communicated content can be used by receiving party to identify individuals (although data were expected to be anonymous).

1. Are the shared data expected to be anonymous/ de-identified?
2. Is it possible to (re-)identify the shared data by linking with identified data or by combining (seemingly non-identifying) attributes? (if unknown, assume it is possible)

When sharing a dataset with an external party, full name is removed and address is reduced to city. However, quasi-identifiers are available which, when combined, are sufficiently unique to identify the individuals in the dataset.
Example quasi-identifier combinations include: gender, birthdate, postal code; gender, age, municipality and occupation.

- When sharing identified data (especially when not assumed to), the data subject's privacy is violated.

- Combining seemingly non-identifying attributes (quasi-identifiers) can identify a person.
- Results in non-compliance (Nc3) and unawareness (U1) threats.
- If the data originate from a database, the threat also corresponds to 'identifiability of retrieved data (I7)'.

IDENTIFYING STORED DATA

Hotspot

STORE PERSONAL DATA

Threat source

ORGANIZATIONAL

Personal data being stored can be identified (because they are insufficiently minimized/de-identified before storage).

1. Are data stored with identifiable attributes? (i.e. do the data contain identifiers, quasi-identifiers, or links to identified data?)
2. Can identifying data item(s) be minimized (e.g. removed, de-identified, decentralized)?

- The data are being de-identified by replacing identifying attributes (e.g. name, address) by an internal identifier. A link to the actual identity is however being kept, which still allows identifiability.
- Data are being stored with username, email address or SSN as (internal) identifier [TRIM].

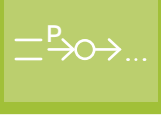
- Identified data, when they are meant to be anonymous and/or when they do not have to be identified, cause a serious privacy violation.

- If data cannot be de-identified (because required in the system), they might be de-centralized.
- Closely related to minimization (Nc5).

IDENTIFYING RETRIEVED DATA

Hotspot

RETRIEVE PERSONAL DATA (RECEIVING PARTY IS NOT DATA SUBJECT)



Threat source

(FUTURE) RECEIVING PARTY /ORGANIZATIONAL

Personal data being retrieved from persistent storage can be used to identify the data subject

(because they contain an identifier, or because they contain sufficient attributes (that combine to a quasi-identifier), or because they can be linked with previously identified data).

1. Are identified data being retrieved or does the receiving party have more data on the data subjects (possibly publicly available (identified) info)? (if unknown, assume it is)
2. Is it a problem if the receiving party can identify data?

The database returns a unique attribute (e.g. email address, birth date, etc.) that the receiving party can use to identify the data subject.

- Quasi-identifiers can be sufficient to identify the data.
- Likelihood (and impact) depends on previous knowledge.

- Ensuring anonymity of data query results is difficult.
- The more information is tied to a profile, the more unique, which can result in identifiability.
- Relates to minimization (Nc3,5).

CREDENTIALS NON-REPUDIATION

Hotspot

INBOUND FLOW CONTAINING CREDENTIALS (AUTHENTICATED USER INTERACTION)

Threat source

EXTERNAL (WITH ACCESS TO DATA)

Person cannot deny having authenticated to a service

1. Does the system require identifiable credentials?
2. Is it a problem if a user can be tied to the system (when credentials or access logs are leaked)? (This threat is not likely to be applicable. Only when use of the system is considered 'sensitive')

A user registers himself with his company email address on an obscure site. When breached, the user account leads directly to the user.

Note: a personal email address issued by the government or an employer is much more difficult to repudiate than a self registered email address (e.g. gmail).

- Impact depends on how easily the credentials can be linked to the natural person.

- Applies when the system requires authentication, but the user needs plausible deniability of using the system (less likely to occur).
- To ensure plausible deniability of access, ideally no (or anonymous) credentials are used.

NON-REPUDIATION OF SENDING

Hotspot

INBOUND
USER INTERACTION

Threat source

ORGANIZATIONAL

The user cannot deny having sent a message.

1. Is the origin of incoming communication known and traceable to the sender? (e.g. sender logged, digital signature,...)
2. Is it a problem if a trace of this information is kept (i.e. does the sender require deniability afterwards)? (This threat is not likely to be applicable as it only applies when sensitive actions or data are being communicated that require deniability)

An employee shares gossip among his co-workers via a digitally signed email.. When his boss received the forwarded message, it is difficult for the employee to deny having spread the gossip.
(level of deniability depends on the likelihood of spoofing the message).

- Mainly applies when the receiving end requires a proof of authenticity during communication, but the sender wants to be able to deny to external parties (afterwards).

- Not only applies to messages, but also to 'requests' to the system (e.g. logging of access to a process, logging of database queries, etc.).
- Credential non-repudiation (Nr1) is a subtype of this threat.

Nr2

LINDDUN

NON-REPUDIATION OF RECEIPT

Hotspot

OUTBOUND FLOW TO **USER**

Threat source

ORGANIZATIONAL

User is not able to deny having received a message.

1. Is an acknowledgement of message receipt (automatically) sent by the receiver?
2. Is it a problem if the system knows that the user received the message? (This threat is not likely to occur.)

Messaging services (e.g. Whatsapp and Messenger) reveal to the sender of a message when their message was received.

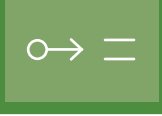
- Since this acknowledgement is often implicit, it is easy to miss. Likelihood is thus rather high.

- A user should be able to decide on whether or not they want to acknowledge receiving a message.
- Related to unawareness (U1).

NON-REPUTABLE STORAGE

Hotspot

STORE
SENSITIVE DATA



Threat source

ORGANIZATIONAL

The data in storage cannot be denied

(e.g., because its authenticity was verified and logged, because the data cannot be altered, etc.).

1. Are (sensitive) data stored in an unreputable way?
2. Do the data require repudiation? (probably no, as this threat is very unlikely to be applicable)

- Data in the blockchain cannot be changed, therefore deniability is not possible.
- (Advanced) No deniable encryption is used and therefore it can be proven that the data are encrypted (and can be encrypted to a certain plain text).

- Impact: mainly applies to sensitive data of which a data subject wants to remove all ties to himself.

- For security, non-repudiation is often a requirement, rather than a threat.
- Closely relates to non-repudiation of sending (Nr2).

NON-REPUDIATION OF RETRIEVED DATA

Hotspot

RETRIEVE
PERSONAL DATA
(DATA SUBJECT IS NOT RECEIVER)

Threat source

(FUTURE)
RECEIVING PARTY

The retrieved data contains undeniable information.

1. Is the retrieved information unreputable personal data of a data subject (who is not the receiver)?
2. Is it a problem if the data can be tied to the data subject? (e.g. log files)

System administrators have access to full log files and can tie each access to an employee (rather than a pseudonym). An employee will thus not be able to deny that he has used the company's ethical complaints system (to file a complaint), although it should have been anonymous.

- Impact is higher when the retrieved information is identifiable (I7).

- If non-repudiation of certain data is required, it is important that this info is not accessible by default (requires access control and/or de-identification at retrieval time).
- Relates to non-reputable storage (Nr4).

DETECTABLE CREDENTIALS

Hotspot

INBOUND
USER INTERACTION
SENDING **CREDENTIALS**
(AUTHENTICATED USER)

Threat source

EXTERNAL

Response of a request allows detection of existence of a user (without actually accessing any data).

1. Does the system provide feedback w.r.t. credentials (wrong password, forgot password, ...)?
2. Would it be a problem for a user if his use of the system is known? (i.e. does the system have a sensitive context?)

When signing in to a service, it is possible to detect that a user exists (i.e. error message of wrong password) or does not exist (i.e. error message of invalid user ID).

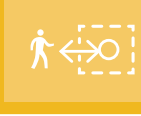
- Detecting user accounts also results in security threats (information disclosure/spoofing).

- Often easy to fix by making the responses more privacy-friendly.

DETECTABLE COMMUNICATION

Hotspot

IN/OUTBOUND FLOW WITH **USER**



Threat source

EXTERNAL

Communication between the user and the service can be observed.

1. Is there a mechanism to hide that communication takes place? (e.g. anonymous communication is missing)
2. Would it be a problem if an external party could see that the user communicates with the system? (This threat is unlikely to be applicable, unless the system has a sensitive context and usage is to be undetectable)

By detecting communication between a person and a service, it can be inferred that the person is a user of the service (e.g. adult website, forum for certain disease, etc).

- Only applicable when the system has a sensitive context.

- Solutions include: anonymous communication networks such as Tor.

DETECTABLE OUTLIERS

Hotspot

IN/OUTBOUND FLOW

Threat source

EXTERNAL

By detecting communication that behaves differently, more information can be deduced about the flow.

1. Can additional (personal) information be deduced from the communication behavior (e.g. different time, different size, etc.)?
2. Is it a problem if an external misactor can observe outlier communication? (i.e. can there be much deduced from this observation?)

Communication is detected at an irregular time (between a service and a user), e.g. smart home sends updates at regular intervals, only in case of emergency (fire, burglary) a notification is sent immediately (which can be detected).

- Detectability can lead to inference of (personal) information by observing communication.
- Impact depends on sensitivity of data and context involved.

- Typically the communication is detected between the system and a user, or a process acting in their behalf (e.g. smartphone, sensor, etc.).
- Solutions include dummy traffic and steganography.

DETECTABLE AT STORAGE

Hotspot

STORE PERSONAL DATA

Threat source

EXTERNAL (WITH ACCESS TO SYSTEM)

The misactor can detect that there are (more) data stored in the database.

1. Can storage actions reveal more information?
   (e.g. through acknowledgements)
2. Is it a problem if existence of data can be deduced?

- When storing data, an out of memory error reveals the existence of other data in the database.
- A political party provides the possibility to register a home address to receive a flyer. The 'address already registered' message allows to detect addresses of people who support the political party.

- Impact depends on the type of information stored in the database (i.e. what can be deduced from detecting existence).

- Storage actions should not leak information about previously stored data.

DETECTABLE AT RETRIEVAL

Hotspot

RETRIEVE
PERSONAL DATA

Threat source

(FUTURE)
RECEIVING PARTY

Query response reveals existence of data (without providing access).

1. Can retrieval requests reveal more information about the content of the database (e.g. presence of a specific file, number of matching data items for a query)?
2. Would it be a problem if this information is revealed?
   (i.e. does this concern sensitive information, or can sensitive information be deduced from merely the presence of the personal data)

Query results metadata reveals more than required (e.g. access control prevents access to actual data/files, but query response indicates that results have been found).

- Often knowing data exists can reveal already some (additional) information, even without actually having access to the specific data item(s).

- Mainly concerns meta-information that can be extracted by the receiving party.

NO TRANSPARENCY

Hotspot

INBOUND FLOW/ ...
PROCESS WITH
PERSONAL DATA

Threat source

ORGANIZATIONAL

The data subject is insufficiently informed about the collection and further processing of their personal data.

1. Are personal data being collected and/or processed?
2. Is the data subject insufficiently informed about this collection or further processing activities?

- It is unclear to the data subject with which third parties their data will be shared because no notice is provided.
- The data subject was not informed at collection time about the purpose or the retention period of their personal data.
- The notice provided to the data subject was not written in clear and plain language.

- Transparency (notice) is a data subject right [GDPR].
- This threat can be triggered at collection time, but applies to all further processing activities.

- Both collection directly from the data subject and collection from a third party should be communicated to the data subject.

NO USER-FRIENDLY PRIVACY CONTROL

Hotspot

INBOUND FLOW
BY **USER** WITH
PERSONAL DATA

Threat source

ORGANIZATIONAL

The system does not provide user-friendly privacy control.

(e.g. default settings, feedback & awareness tools, user-friendly privacy preferences support)

1. Does the system process personal data?
2. Are there no privacy-preserving default settings and/or is there no user-friendly support for the data subject to set privacy preferences or provide awareness information?

- When visiting a website for the first time, it requires navigation through several tabs and slide several switches to set the cookie settings and other privacy preferences (no privacy by default, no user-friendliness).
- When posting on social media, the post is made public by default (no privacy by default, no feedback and awareness tools to educate the data subject on the consequences of these privacy settings).

- Mainly relevant for systems directly collecting personal data from users (or indirectly through communication metadata) and systems targeted at sharing personal data (e.g. social media).

- Privacy-friendly settings should be the default.
- The data subject should be able to easily control his privacy settings.
- Raising privacy awareness can nudge the data subject into a more privacy-aware behavior.

NO ACCESS OR PORTABILITY

Hotspot

STORE PERSONAL DATA

Threat source

ORGANIZATIONAL

The data subject does not have access to their personal data or is not able to port personal data to another platform/vendor/...

1. Are personal data being stored?
2. Is a process lacking that can extract data (in both a human understandable and computer interpretable format) for an individual data subject?

- A wearable device's sensor data are sent to a lifestyle tracking app, but the user is unable to access the statistics and deduced information based on his data that the app has collected and processed.
- A data subject does not have the means to request their data, neither directly through the system, or indirectly (e.g. a request to a helpdesk which generates the requested data set and forwards it to the data subject.).

- Access and data portability is a data subject right [GDPR].
- Does not apply to data that infringes other data subjects' privacy, corporate secrets, etc.

- This access can also exist outside of the system. (e.g. a helpdesk request)
- Data portability only involves personal data that was provided directly by the data subject.

NO ERASURE OR RECTIFICATION

Hotspot

STORE PERSONAL DATA

Threat source

ORGANIZATIONAL

The data subject cannot request erasure or rectification of personal data.

1. Are personal data being stored?
2. Is a process lacking that can delete and rectify (a subset of) data related to a specific data subject?

- A data subject requests deletion of his social media data, but only his account is revoked, the actual data remain.
- The data subject moved and wants to update their address in the system, but is unable to.

- Request of erasure and rectification is a data subject right (under certain conditions) [GDPR].
- Deletion can only be requested 'within reason'.

- The request can also be made outside of the system (e.g. helpdesk), it however should always be technically feasible to delete the data.
- A data subject can only request rectification of data to increase accuracy.

INSUFFICIENT CONSENT SUPPORT

Hotspot

STORE
CONSENT

Threat source

ORGANIZATIONAL

Data subject consents are are not properly taken into account by the relevant processes and data are still being processed with a missing or withdrawn consent.

1. Does the system require user consent to process personal data? Does the system fail to take the consent into account?
2. Are means lacking for the data subject to explicitly provide or withdraw consent or are the consents not taken into account for processing operations (e.g. access control)?

Wearables data are being used for a research study, but

- The data subject has never given his consent
- The data subject decides to revoke his consent, but there is no technical revocation support
- The system only stops collecting new data but continues its analysis with the previously collected data.

- A consent should always be freely given and thus also be revocable. The system should thus support the consequences of a newly obtained or revoked consent.

- This can be a feature directly available to the data subject or it can be done indirectly (e.g. helpdesk). In both cases, an internal process should be in place to support this.

DISPROPORTIONATE COLLECTION

Hotspot

INBOUND FLOW WITH **PERSONAL DATA**

Threat source

ORGANIZATIONAL

More personal data are being collected than required for the purpose.

1. Are personal data being collected?
2. Are not all attributes strictly required for the processing purpose? (e.g. would an aggregated data set suffice? Is real-time information not strictly required?)

- Data are collected before purposes for collection and processing have been documented.
- Audit logs register every personal data activity (but not required) [TRIM].
- Geolocation data collected is too accurate, only the city is required for the purpose [TRIM].

- Disproportionate collection violates data protection principles [GDPR].

- Systems often tend to collect and process more (raw) data than required.
- Relates to linkability and identifiability.
- Also known as 'minimization at collection time'.

Nc1

LINDDUN

UNLAWFUL PROCESSING

Hotspot

INBOUND FLOW WITH **PERSONAL DATA**

Threat source

ORGANIZATIONAL

There is no lawful ground for the collection or further processing and storage of personal data.

1. Are personal data being processed in the system?
2. Did the data subject not consent to the processing and is there no other lawful ground?

A smart tv collects viewing history of its users and sends it periodically to the back-end, without any lawful grounds (nor consent).

- A lawful ground is required for each processing activity. (Consent is just one of them!)

- Lawful ground includes: vital, legitimate or public interest,legal obligation, contractual necessity and consent.
- Triggered by inbound flows, but applies to all subsequent processing activities in the system.

Nc2

LINDDUN

DISPROPORTIONATE PROCESSING

Hotspot

PROCESS (...→P)
PERSONAL DATA

Threat source

ORGANIZATIONAL

More personal data are being processed than required for the purpose.

1. Are personal data being processed?
2. Are personal data being processed that are not strictly required for the processing purpose(s) or that were collected for an incompatible purpose?

- Personal data are being used as testing data or as machine learning training sets [TRIM].
- Access logs are used to check at what time employees were at work, rather than using these files only in case of (security) violations.
- IoT data (e.g. location data) are being collected by a wearable to track lifestyle. When shared in a different context (e.g. on a social platform), a different purpose is required.

- According to data protection processing principles, personal data can only be processed if they are strictly required for the processing purpose. [GDPR]

- A contextual change often requires a different purpose.
- Data should be minimized as much as possible.
- Relates to linkability and identifiability.

Nc3 LINDDUN

AUTOMATED DECISION MAKING

Hotspot

PROCESS PERSONAL DATA FOR **AUTOMATED DECISION** MAKING

Threat source

ORGANIZATIONAL

A decision is made based solely on automated processing of personal data which significantly affects the data subject.

1. Does the process make decisions that directly affect the data subject without human interference/verification?
2. Is there legitimate ground missing to do so (e.g. explicit consent or contract)? Is the data subject unable to contest the decision?

- A loan was rejected based on automated decision making. The data subject was not able to obtain human intervention or review the decision.
- Neural network makes customer-related decisions, but nobody can explain to the customer what the model is based on [TRIM].

- Automated decision making is generally prohibited (unless required for a contract, authorized by law, or with an explicit consent) [GDPR].

- Relates to unawareness threats of the data subject (U1+3).
- Additional data subject rights apply as well.

Nc4 LINDDUN

DISPROPORTIONATE STORAGE

Hotspot

STORE PERSONAL DATA

Threat source

ORGANIZATIONAL

More personal data are being stored than required for the purpose.

1. Are personal data being stored?
2. Is the database storing more than only the information that is strictly required or for a longer period than required for the purpose?

The system stores all collected personal data because “we might need them in the future”, while an aggregated data set will be sufficient.

- There is no lawful ground to store more than strictly required for the purpose(s) or to keep it for a longer period of time.

- Data should be minimized as much as possible.
- When personal data are required, measures should be taken to minimize L and I threats.
- Relates to retention and purpose limitation [GDPR].


LINDDUN GO