LINDDUN: running example - social network 2.0 -

Based on
Mina Deng, Kim Wuyts, Riccardo Scandariato
Bart Preneel, and Wouter Joosen

A privacy threat analysis framework: supporting the elicitation and fulfillment of privacy requirements, Requirements Engineering Journal, volume 16, issue 1, pages 3-32, 2011

Abstract

This document summarizes the running example used in the LINDDUN paper. Be advised that the example is based on the original LINDDUN methodology and threat trees and thus not fully maps on the current LINDDUN methodology. Nevertheless, the general ideas remain the same and thus running example provides an interesting illustration of the overall LINDDUN methodology.

1 Introduction

This document contains a summary of the running example as used to illustrate the LINDDUN methodology. Note that the example is created based on the original methodology and uses the threat trees and methodology steps as described in the original LINDDUN paper [1], which is similar, but not the same as the trees and methodology described on the LINDDUN website [2].

2 Social Network 2.0

The example application used as illustration of LINDDUN was named *Social Network 2.0*. It is an abstract representation of a social network, where online users share personal information such as relationship status, pictures, and comments with their friends. In Social Network 2.0, Alice is a registered user of a social network. Each time Alice updates her friends list, she first connects to the social network's web portal. Accordingly, the portal communicates with the social network's server, and eventually, the friendship information of Alice and all other users of that social network is stored in a database.

Evidently, the goal of the LINDDUN analysis is to identify and mitigate potential privacy violations and create a privacy-friendly social network application.

3 Step 1. Creating a DFD

The system is graphically represented using a data flow diagram (DFD), with the following elements: data flows (i.e. communication data), data stores (i.e. logical data or concrete databases, files, and so on), processes (i.e. units of functionality or programs) and external entities (i.e. endpoints of the system like users, external services, and so on). For threat modeling, trust boundaries are also introduced to indicate the border between trustworthy and untrustworthy elements.

The social network DFD is shown in Figure 1. In the DFD, the user is represented as an entity to interact with the system. The Social Network 2.0 application contains two processes (the portal and the service) and one data store containing all the personal information of the users. The trust boundary shows that the processes, the data store, and the communication (data flows) between the two are assumed to be trustworthy in this particular setting.

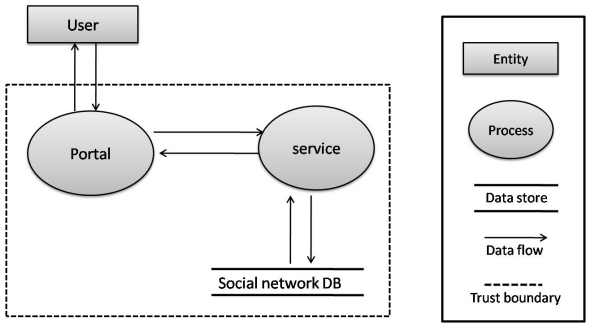

Figure 1. The Data Flow Diagram (DFD) of the Social Network 2.0 application

4 Step 2. Mapping DFD elements to threats

After the DFD elements are listed, we identify the privacy threat categories for each DFD element by following the LINDDUN mapping template. Each intersection marked with the symbol $\times$ indicates a potential privacy threat at a corresponding DFD element in the system.

Considering the Social Network 2.0 application, the list of generic privacy threats to the modeled system is depicted in Table 1. This is obtained by gathering the DFD elements and then determining the susceptible threats with the LINDDUN mapping template.

Table 1. Determining privacy threats for DFD elements within the Social Network 2.0 application (From left to right: L-Linkability, I-Identifiability, N-Non Repudiation, D-Detectability, D-Information Disclosure, U-Content Unawareness, N-Consent/policy Noncompliance)

	Threat target	L	I	N	D	D	U	N
Data Store	Social network DB	1	4	×	×	7		10
Data Flow	User data stream (user – portal)	2	5	×	×	8		10*
	Service data stream (portal – service)	×	×	×	×	×		10*
	DB data stream (service – DB)	×	×	×	×	×		10*
Process	Portal	×	×	×	×	×		10*
	Social network service	×	×	×	×	×		10*
Entity	User	3	6				9	

The intersections marked with × in Table 1 are potential threats that have been considered as irrelevant to the specific usage scenario. Each intersection that is indicated with a number (1 to 10) in Table 1 shows that there will be a privacy threat at the corresponding DFD element. These items marked with a number are the threats which we will actually consider. The number represents the ID of the threat scenario and will be used later for ease of reference.

Primarily, we assume that DFD elements within the trust boundary (marked as dashed line in Figure 1) are trustworthy. We trust the processes within the boundary, as well as all data flows in the trust boundary. Therefore, we will not discuss linkability, identifiability, and information disclosure threats on these elements. We however do not trust the user and its communication with the portal and we also want to protect the data store containing all the user's information.

Moreover, non-repudiation and detectability threats are considered irrelevant for social networks. Presumably, it depends on what privacy properties are required for a particular social network system. In case plausible deniability and undetectability would be desirable for a certain application, we should still consider these threats for each DFD element accordingly.

Following the above reasoning, ten threats will be examined in detail in Step 3, and they are numbered in Table 1. Note that some items are indicated with a $10*$. This means that the policy and consent noncompliance threat affects the system as a whole (including data flow, data store and process).

Note that this is a simplified representation of a social network application, and the assumptions made above are for demonstration purposes. Do not copy these assumptions unless you are sure they also apply to the system you are analyzing.

5 Step 3. Identifying threat scenarios

5.1 Eliciting threats using threat tree patterns

Threat tree patterns are used to detail the generic LINDDUN threat categories into specific threat instances that can occur in a system. In LINDDUN, these patterns are documented as privacy threat trees. This example uses the original LINDDUN trees as described in [1]. We refer the reader to the LINDDUN online website for the most recent threat tree catalog [2].

Each of the branches in the tree that corresponds to one of the 10 selected generic threats in the mapping table (see Table 1, are examined for potential privacy violations. Applicable threats are then documented using misuse cases.

5.2 Documenting privacy threats using misuse cases

A misuse case can be considered as a use case from the misactor's point of view. A misactor is someone who intentionally or unintentionally initiates the misuse case.

In our running example, we assume that communication and processes within the social network service provider are trustworthy (see the trust boundary in the DFD depicted in Figure 1). However, we want to protect the data store against information disclosure. The data controllers could be users, social network providers, and application providers.

To illustrate how to create a misuse case based on the threat tree patterns, consider the threat tree of linkability at the data store (see threat tree in [1]). The tree illustrates that in order to be susceptible to this threat, neither the data store is sufficiently protected against information disclosure nor sufficient data anonymization techniques are employed. These are the preconditions of the misuse case. To create the attack scenarios, it is clear that the attacker first needs to have access to the data store, and secondly, either the user (as the data subject) can be re-identified (as the basic flow) or the pseudonyms can be linkable (as the alternative flow).

MUC 1 – Linkability of social network database (data store)

Summary: Data entries can be linked to the same person (without necessarily revealing the persons identity)
Assets, stakeholders and threats: Personal Identifiable Information (PII) of the user.

- The user:
  - Data entries can be linked to each other which might reveal the persons identity
  - The misactor can build a profile of a user's online activities (interests, actives time, comments, updates, etc.)

Primary misactor: skilled insider / skilled outsider
Basic Flow:

1. The misactor gains access to the database
2. The misactor can link the data entries together and possibly re-identify the data subject from the data content

Alternative Flow:

1. The misactor gains access to the database
2. Each data entry is linked to a pseudonym
3. The misactor can link the different pseudonyms together (linkability of entity)
4. Based on the pseudonyms, the misactor can link the different data entries

Trigger: by misactor, can always happen.
Preconditions:

- no or insufficient protection of the data store
- no or insufficient data anonymization techniques or strong data mining applied

MUC 2: Linkability of of the user-portal data stream (data flow)

Summary: Data flows can be linked to the same person (without necessarily revealing the persons identity)
Asset: PII of the user

- The user:
  - data flow can be linked to each other which might reveal the persons identity
  - the attacker can build a profile of a user's online activities (interests, active time, comments, updates, etc.)

Primary misactor: skilled insider / skilled outsider
Basic Flow:

1. The misactor intercepts / eavesdrops two or more data flows
2. The misactor can link the data flows to each other and possibly link them (by combining this information) to the user / data subject

Trigger: by misactor, can happen whenever data is communicated
Preconditions:

- No anonymous communication system used
- Information disclosure of data flow possible

Prevention capture points:

- Use strong anonymous communication techniques
- Provide confidential channel

Prevention guarantee: Impossible to link data to each other

MUC 3: Linkability of the social network users (entity)

Summary: Entities (with different pseudonyms) can be linked to the same person (without necessarily revealing the persons identity)
Asset: PII of the user

- The user:
  - data can be linked to each other which might reveal the persons identity
  - attacker can build a profile of a user's online activities (interests, actives time, comments, updates, etc.)

Primary misactor: skilled insider / skilled outsider
Basic Flow:

1. The misactor intercepts or eavesdrops two or more pseudonyms
2. The misactor can link the pseudonyms to each other and possibly link (by combining this information) to the user / data subject

Trigger: by misactor, can happen whenever data is communicated
Preconditions:

- Information Disclosure of the data flow possible
- Different "pseudonyms" are linked to each other based on content of the data flow

Prevention capture points:

- protection of information such as user temporary ID, IP address, time and location, session ID, identifier and biometrics, computer ID, communication content, e.g. apply data obfuscation to protection this information (security)
- message and channel confidentiality provided

Prevention guarantee: Impossible to link data to each other

MUC 4: Identifiability at the social network database (data store)

Summary: The users identity is revealed
Asset: PII of the user

- The user: revealed identity

Primary misactor: skilled insider / skilled outsider
Basic Flow:

1. The misactor gains access to the database
2. The data is linked to a pseudonym
3. The misactor can link the pseudonym to the actual identity (identifiability of entity)
4. The misactor can link the data to the actual user's identity

Alternative Flow:

1. The misactor gains access to the database
2. The can link information from the database to other information (from another database or information which might be publicly accessible)
3. The misactor can re-identify the user based on the combined information

Trigger: by misactor, can always happen
Preconditions:

- no or insufficient protection of the data store
- no data anonymization techniques used

Prevention capture points:

- protection of the data store (security)
- apply data anonymization techniques

Prevention guarantee: hard-impossible to link data to identity (depending on applied technique)

MUC 5: Identifiability of user-portal data stream (data flow)

Summary: The users identity is revealed
Asset: PII of the user

- The user: revealed identity

Primary misactor: insider / outsider
Basic Flow:

1. The misactor gains access to the data flow
2. The data contains personal identifiable information about the user (user relationships, address, etc.)
3. The misactor is able to extract personal identifiable information from the user / data subject

Trigger: by misactor, can happen whenever data is communicated
Preconditions:

- no or weak anonymous communication system used
- Information disclosure of data flow possible

Prevention capture points:

- apply anonymous communication techniques
- Use confidential channel

Prevention guarantee: hard-impossible to link data to identity (depending on applied technique)

MUC 6: Identifiability of users of the social network system (entity)

Summary: The users identity is revealed
Asset: PII of the user

- The user: revealed identity

Primary misactor: skilled insider / skilled outsider
Basic Flow:

1. The misactor gains access to the data flow
2. The data contains the user's password
3. The misactor has access to the identity management database
4. The misactor can link the password to the user

Alternative Flow:

1. The misactor gains access to the data flow
2. The data contains the user's password

3. The misactor can link the user's password to the user's identity (password is initials followed by birthdate)

Trigger: by misactor, can happen whenever data is communicated and the user logs in using his "secret"
Preconditions:

- Insecure IDM system OR
- weak passwords used and information disclosure of data flow possible

Prevention capture points:

- Strong pseudonymity technique used (e.g. strong passwords)
- privacy-enhancing IDM system
- Data flow confidentiality

Prevention guarantee: hard(er) to link log-in to identity.

MUC 7: Information Disclosure at the social network database (data store)

Summary: Data is exposed to unauthorized users
Asset: PII of the user

- The user: revealed sensitive data

Primary misactor: skilled insider / skilled outsider
Basic Flow:

1. The misactor gains access to the database
2. The misactor retrieves data to which he should not have access

Trigger: by misactor, can always happen
Preconditions:

- no or insufficient internal access policies

Prevention capture points:

- strong access control policies (security). For example, rule-based access control based on friendships in the social network

Prevention guarantee: hard-impossible to obtain data without having the necessary permissions

MUC 8: Information Disclosure of communication between the user and the social network (data flow)

Summary: The communication is exposed to unauthorized users
Asset: PII of the user

- The user: revealed sensitive data

Primary misactor: skilled insider / skilled outsider
Basic Flow:

1. The misactor gains access to the data flow
2. The misactor retrieves data to which he should not have access

Trigger: by misactor, can happen whenever messages are being sent
Preconditions:

- communication goes through insecure public network

Prevention capture points:

- messages sent between user and social network web client is encrypted and secure communication channel is ensured

Prevention guarantee: hard-impossible to gain access to the data flow without having the right permissions

Note that formulating soft privacy threats is less straightforward and requires some out-of-the-box thinking for suitable (non-)technical solutions, as illustrated in misuse cases 9 and 10.

MUC 9: Content unawareness

Summary: User is unaware that his or her anonymity is at risk due to the fact that too much personal identifiable information is released
Asset: PII of the user

- The user: revealed identity

Primary misactor: skilled insider / skilled outsider
Basic Flow:

1. The misactor gain access to user's online comments
2. The misactor profiles the user's data and can identify the user

Trigger: by misactor, can always happen
Preconditions:

- User provides too much personal data

Prevention capture points:

- User provides only minimal set of required information

Prevention guarantee: user will be informed about potential privacy risks

MUC 10: Policy and consent noncompliance

Summary: The social network provider doesn't process user's personal data in compliance with user consent, e.g., disclose the database to third parties for secondary use
Asset: PII of the user

- The user: revealed identity and personal information
- The system / company: negative impact on reputation

Primary misactor: Insider
Basic Flow:

1. The misactor gains access to social network database
2. The misactor discloses the data to a third party

Trigger: by misactor, can always happen
Preconditions:

- misactor can tamper with privacy policies and makes consents inconsistent OR
- policies not managed correctly (not updated according to user's requests)

Prevention capture points:

- Design system in compliance with legal guidelines for privacy and data protection and keep internal policies consistent with policies communicated to user
- Legal enforcement: user can sue the social network provider whenever his or her personal data is processed without consents
- Employee contracts: employees who share information with 3th parties will be penalized (fired, pay fine, etc.)

Prevention guarantee: Legal enforcement will lower the threat of an insider leaking information but it will still be possible to breach user's privacy

6 Step 4. Prioritization/ risk assessment

The LINDDUN framework is independent from specific risk assessment techniques. This step is therefore not included in the running example.

7 Step 5.Elicit privacy requirements

Misuse cases describe the relevant threat scenarios for the system. The preconditions are based on the threat tree patterns and the basic and alternative flows are inspired by the system's use cases.

Table 2. Privacy objectives based on LINDDUN threat types (E-Entity, DF-Data Flow, DS-Data Store, P-Process)

LINDDUN threats	Elementary privacy objectives
Linkability of (E,E)	Unlinkability of (E,E)
Linkability of (DF,DF)	Unlinkability of (DF,DF)
Linkability of (DS,DS)	Unlinkability of (DS,DS)
Linkability of (P,P)	Unlinkability of (P,P)
Identifiability of (E,E)	Anonymity / pseudonymity of (E,E)
Identifiability of (E,DF)	Anonymity / pseudonymity of (E,DF)
Identifiability of (E,DS)	Anonymity / pseudonymity of (E,DS)
Identifiability of (E,P)	Anonymity / pseudonymity of (E,P)
Non-repudiation of (E,DF)	Plausible deniability of (E,DF)
Non-repudiation of (E,DS)	Plausible deniability of (E,DS)
Non-repudiation of (E,P)	Plausible deniability of (E,P)
Detectability of DF	Undetectability of DF
Detectability of DS	Undetectability of DS
Detectability of P	Undetectability of P
Information Disclosure of DF	Confidentiality of DF
Information Disclosure of DS	Confidentiality of DS
Information Disclosure of P	Confidentiality of P
Content Unawareness of E	Content awareness of E
Policy and consent Non-compliance of the system	Policy and consent compliance of the system

As a next step, the system's (positive) requirements can be extracted from the misuse cases. To this aim, the specification of the privacy requirements is facilitated by Table 2, which maps the types of threats scenarios to types of privacy requirements.

Note that this table is rather straight-forward. In practice, also more detailed requirements can be extracted. We refer the reader to the LINDDUN website [2] which describes the updated LINDDUN methodology steps that aid in identifying mitigation strategies and corresponding requirements and solutions.

8 Step 6. From privacy requirements to privacy enhancing solutions (PETs)

Table 3 summarizes the selection of PETs based on the privacy requirements elicited in our running example. It is possible that a more business oriented example would suggest different mitigation strategies. Nevertheless, we hope

the example depicted in this section can illustrate how the proposed framework can be applied in real life applications.

In an attempt to make the running example more accessible to the reader, the system model, the misuse cases, and the mitigation techniques of the Social Network 2.0 are largely simplified due to the assumption that the social network providers are semi-trustworthy (i.e., the adversary model consists of external parties, data holder, honest insiders who make errors, and corrupt insiders). If different assumptions would hold, different misuse cases should be identified with a distinct mitigation approach. For instance, if we apply a smaller trust boundary and assume that the social network provider is totally untrustworthy, then extra privacy requirements and a stronger threat model would be considered. One possible misuse case would be that the malicious social network provider, as an attacker, takes advantage of profiling user's personal data for its own benefits. In that scenario, one solution could be building a security agriculture out of smart clients and an untrusted central server to removes the need for faith in network operators and gives users control of their privacy [8]. Another solution could be using encryption to enforce access control for users' personal information based on their privacy preferences [9, 10].

References

[1] M. Deng, K. Wuyts, R. Scandariato, B. Preneel, and W. Joosen, "A privacy threat analysis framework: supporting the elicitation and fulfillment of privacy requirements," *Requirements Engineering Journal*, vol. 16, no. 1, pp. 3–32, 2011.

[2] "Linddun privacy threat modeling - official website." https://distrinet.cs.kuleuven.be/software/linddun/index.php.

[3] L. Sweeney, "Achieving k-anonymity privacy protection using generalization and suppression," *Int. J. Uncertain. Fuzziness Knowl.-Based Syst.*, vol. 10, no. 5, 2002.

[4] B. Carminati and E. Ferrari, "Privacy-aware collaborative access control in web-based social networks," in *Proc. of the 22nd IFIP WG 11.3 Working Conference on Data and Applications Security (DBSEC2008)*, 2008.

[5] R. Dingledine, N. Mathewson, and P. Syverson, "Tor: The second-generation onion router," in *Proceedings of the 13th USENIX Security Symposium*, August 2004.

[6] M. Hansen, P. Berlich, J. Camenisch, S. Clauß, A. Pfitzmann, and M. Waidner, "Privacy-enhancing identity management," *Information Security Technical Report (ISTR)*, vol. 9, no. 1, pp. 35–44, 2004. http://dx.doi.org/10.1016/S1363-4127(04)00014-7.

[7] S. Clauß, A. Pfitzmann, M. Hansen, and E. V. Herreweghen, "Privacy-enhancing identity management." The IPTS Report 67, 8-16, September 2002.

[8] J. Anderson, C. Diaz, J. Bonneau, and F. Stajano, "Privacy-enabling social networking over untrusted networks," in *WOSN '09: Proceedings of the 2nd ACM workshop on Online social networks*, 2009.

[9] F. Beato, M. Kohlweiss, , and K. Wouters, "Enforcing access control in social networks." HotPets 2009, 2009. http://www.cosic.esat.kuleuven.be/publications/article-1240.pdf.

[10] PrimeLife, "The european primelife research project – privacy and identity management in europe for life." http://www.primelife.eu/.

Table 3. Social Network 2.0 example: from misuse cases to privacy requirements and suggested mitigation strategies and techniques

No.	Misuse cases	Privacy requirements	Suggested mitigation strategies and techniques
1	Linkability of social network data store	Unlinkability of data entries within the social network database	Apply data anonymization techniques, such as k-anonymity [3].
		Protection of data store	Enforce data protection by means of relationship-based access control [4]
2	Linkability of data flow of the user data stream (user-portal)	Unlinkability of messages of user-portal communication; channel confidentiality	Deploy anonymity system, such as TOR [5].
3	Linkability of entities the social network users	Unlinkability of different pseudonyms (user IDs) of social network users; channel confidentiality.	1) Technical enforcement: deploy anonymity system, such as TOR [5], for communication between user and social network web portal; 2) User privacy awareness: inform users that revealing too much information online can be privacy invasive.
4	Identifiability at the social network data store	Anonymity of social network users such that the user will not be identified from social network database entries	Protection of the data store, by applying data anonymization techniques, such as k-anonymity [3].
		Protection of data store	Enforce data protection by means of relationship-based access control [4]
5	Identifiability at data flow of user data stream (user-portal)	Anonymity of social network users such that the user will not be identified from user-portal communication by content; channel confidentiality	Deploy anonymity system, such as TOR [5], for communication between user and social network web portal.
6	Identifiability of the social network users	Pseudonymize users IDs	1) Apply secure pseudonymization techniques to issue pseudonyms as user IDs; 2) User privacy awareness: inform users using real ID has a risk for privacy violation.
		Use identity management to ensure unlinkability is sufficiently preserved (as seen by an attacker) between the partial identities of an individual person required by the applications	Employ privacy preserving identity management, e.g. proposed in [6], together with user-controlled identity management system [7] to ensure user-controlled linkability of personal data. System supports the user in making an informed choice of pseudonyms, representing his or her partial identities. Make the flow of this user's identity attributes explicit to the user and gives its user a large degree of control.
		Confidentiality of data flow in user-portal communication	Deploy anonymity system such as TOR [5].
7	Information disclosure at the social network data store	Release of the social network data store should be controlled according to user's privacy preference	Apply access control at the social network databases, e.g. privacy aware collaborative access control based on relationships [4]
8	Information disclosure of communication between the user and the social network	Confidentiality of communication between the user and the social network should be ensured	Employ a secure communication channel and deploy anonymity system such as TOR [5].
9	Content unawareness of user	Users need to be aware that they only need to provide minimal set of required personal data (the data minimization principle)	Use feedback tools to raise user's privacy awareness.
10	Policy and consent noncompliance of the whole social network system	Design system in compliance with legal guidelines for privacy and data protection	1) Hire employee who is responsible for making the policies compliant OR hire external company for compliancy auditing 2) Ensure training obligations for employees.
		Ensure user aware that in case of violation, user is legitimated to take legal actions	E.g., user can sue the social network provider whenever users personal data is not processed according to what is consented.
		Employee contracts clearly specify do's and don'ts according to legal guidance	1) Ensure training obligations for employees; 2) Employees who disclose users information will be penalized (get fired, pay fine, etc.).