Software architecture - Phase 3: Privacy analysis report

Contents

1 Understanding the architecture

2 Privacy analysis

2.1 Data Flow Diagram

This section should contain the DFD diagram + an explanation of the decisions you made.

2.2 Mapping of threats to DFD

This section should give an overview of the different threats that exist for each DFD element. The DFD element names should be represented in the DFD of the previous section!

To create this table, you can use the provided template.

Table 1

	Threat target	L	I	N	D	D	U	N
Data Store	Social network DB	×	×	×	×	×		×
Data Flow	User data stream (user – portal)	×	×	×	×	×		×
	Service data stream (portal – service)	×	×	×	×	×		×
	DB data stream (service – DB)	×	×	×	×	×		×
Process	Portal	×	×	×	×	×		×
	Social network service	×	×	×	×	×		×
Entity	User	×	×				×	

2.3 Threat elicitation

2.3.1 Assumptions

This section should discuss the different assumptions you make. This includes general assumptions about the system (e.g. the data flow between X and Y is considered encrypted), and decisions and observations (e.g. non-repudiation is not considered a threat for this system). The reasoning behind each assumption and decision should also be included.

This section should be a numbered list to make it easier to refer to it from other sections (from the "remarks" part of each threat description). This section will be critical for the evaluation of the elicited threats, as the assumptions will explain why a certain threat was (or was not) included.

2.3.2 Threats

This section should document the threats which were uncovered in the mapping section. Each threat description should strictly follow the provided template.

ID + title*

Summary*:

Primary mis-actor*:

Basic path*:

bf1.

bf2.

bf3.

Consequence*:

Reference to threat tree node(s)*:

Parent threat tree(s)*:

DFD element(s)*:

Remarks:

r1.

r2.

2.4 Prioritization of threats

This section provides an list of the threats (ID + title) of the previous section. The order is based on the threat's risk (likelihood * impact). You should make a distinction between high, medium, and low risk and, if possible, within each category also order the threats according to their risk. Also, you should briefly explain why you ordered the threats in this particular order.