Patient Community system - example Privacy analysis

Contents

1 Understanding the architecture

2 Privacy analysis

2.1 Data Flow Diagram

This DFD is based on the client-server view of the patient community architecture.

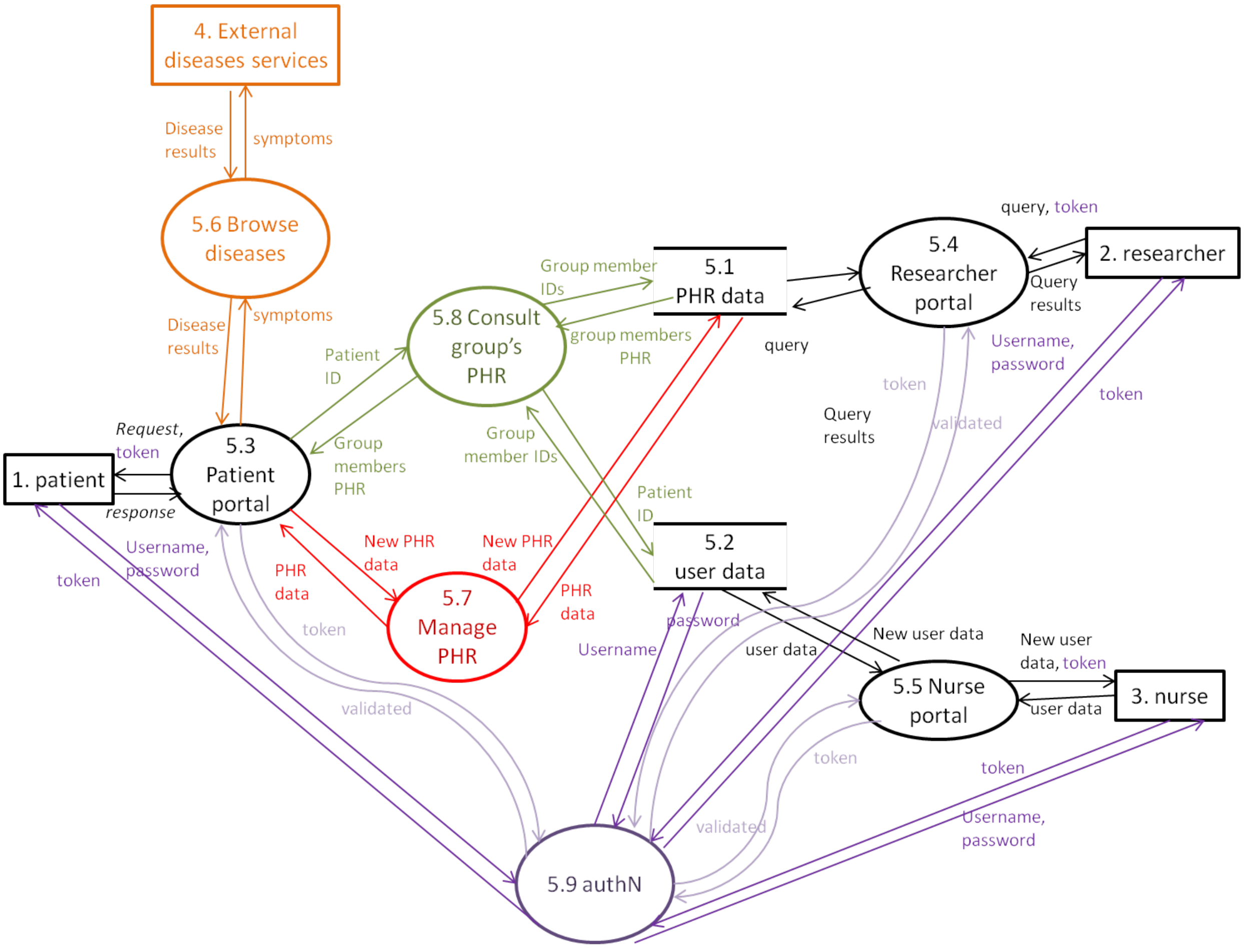

Figure 1: DFD representing the patient community system

The DFD slightly varies from the original client-server view, as the following decisions were made:

1. All frontend components were decomposed into an external entity and the actual process.
2. Although the session manager has an external interface, it refers to the "common" interface of the already created patient, nurse, and researcher entity. Therefore, the session manager is added as 1 process: authN.
3. The nurse frontend and patient manager component were combined to 1 process: nurse portal, because the additional process would not introduce any additional threats.
4. The researcher frontend and statistics processor component were combined to 1 process: researcher portal, because the additional process would not introduce any additional threats.

2.2 Mapping of threats to DFD

Table 1

	Threat target	L	I	N	D	D	U	N
Data Store	PHR data (5.1)	×	×	×	×	×		×
	user data (5.2)	×	×	×	×	×		×
Data Flow	patient - portal flow (1 – 5.3)	×	×	×	×	×		×
	portal - patient flow (5.3 – 1)	×	×	×	×	×		×
	researcher - portal flow (2 – 5.4)	×	×	×	×	×		×
	portal - researcher flow (5.4 – 2)	×	×	×	×	×		×
	nurse - portal flow (3 – 5.5)	×	×	×	×	×		×
	portal - nurse flow (5.5 – 3)	×	×	×	×	×		×
	diseases service - browse diseases flow (4 – 5.6)	×	×	×	×	×		×
	browse diseases- diseases service flow (5.6 – 4)	×	×	×	×	×		×
	patient portal - browse diseases flow (5.3 – 5.6)	×	×	×	×	×		×
	browse diseases data - patient portal flow (5.6 – 5.3)	×	×	×	×	×		×
	patient portal - manage PHR flow (5.3 – 5.7)	×	×	×	×	×		×
	manage PHR - patient portal flow (5.7 – 5.3)	×	×	×	×	×		×
	patient portal - consult group PHR flow (5.3 – 5.8)	×	×	×	×	×		×
	consult group PHR data - patient portal flow (5.8 – 5.3)	×	×	×	×	×		×
	researcher portal - PHR data flow (5.4 – 5.1)	×	×	×	×	×		×
	PHR data - researcher portal flow (5.1 – 5.4)	×	×	×	×	×		×
	nurse portal - user data flow (5.5 – 5.2)	×	×	×	×	×		×
	user data - nurse portal flow (5.2 – 5.5)	×	×	×	×	×		×
	manage PHR - PHR data flow (5.7 – 5.1)	×	×	×	×	×		×
	PHR data - manage PHR flow (5.7 – 5.1)	×	×	×	×	×		×
	consult group PHR - PHR data flow (5.8 – 5.1)	×	×	×	×	×		×
	PHR data - consult group PHR flow (5.1 – 5.8)	×	×	×	×	×		×
	consult group PHR - user data flow (5.8 – 5.2)	×	×	×	×	×		×
	user data - consult group PHR flow (5.2 – 5.8)	×	×	×	×	×		×
	patient - authN flow (1 – 5.9)	×	×	×	×	×		×
	authN - patient flow (5.9 – 1)	×	×	×	×	×		×
	researcher - authN flow (2 – 5.9)	×	×	×	×	×		×
	authN - researcher flow (5.9 – 2)	×	×	×	×	×		×
	nurse - authN flow (3 – 5.9)	×	×	×	×	×		×
	authN - nurse flow (5.9 – 3)	×	×	×	×	×		×
	user data - authN flow (5.2 – 5.9)	×	×	×	×	×		×
	authN - user data flow (5.9 – 5.2)	×	×	×	×	×		×
	patient portal - authN flow (5.3 – 5.9)	×	×	×	×	×		×
	authN - patient portal flow (5.9 – 5.3)	×	×	×	×	×		×
	researcher portal - authN flow (5.4 – 5.9)	×	×	×	×	×		×
	authN - researcher portal flow (5.9 – 5.4)	×	×	×	×	×		×
	nurse portal - authN flow (5.5 – 5.9)	×	×	×	×	×		×
	authN - nurse portal flow (5.9 – 5.5)	×	×	×	×	×		×
Process	patient portal (5.3)	×	×	×	×	×		×
	researcher portal (5.4)	×	×	×	×	×		×
	nurse portal (5.5)	×	×	×	×	×		×
	browse diseases (5.6)	×	×	×	×	×		×
	manage PHR (5.7)	×	×	×	×	×		×
	consult group PHR (5.8)	×	×	×	×	×		×
	authN (5.9)	×	×	×	×	×		×
Entity	patient (1)	×	×				×	
	researcher (2)	×	×				×	
	nurse (3)	×	×				×	
	diseases service (4)	×	×				×	

2.3 Threat elicitation

2.3.1 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

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.

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.

9. Identifiability of the data flow only poses a threat to one specific data flow: 5.6 $\rightarrow$ 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 $\rightarrow$ 4) is the only linkability threat to data flows in the patient community system. Although less likely, when the patient identifiers are replaces by pseudonyms, linking the different symptoms (of different searches) together can still result in an identifiability threat

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.

12. The information the external disease service passes back the the browse disease process does not contain any personal information and should thus not be protected against information disclosure threats

13. The external disease service is not authenticated (as shown in the architecture/DFD) to the back-end system

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

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)

17. Identifiability and linkability are applicable to both data stores, and will therefore be examined in a combined fashion

18. Only spoofing of users (patients, nurses, and researchers) of the portals are considered a privacy threat. Spoofing the external disease service cannot result in information disclosure as the external disease service has no access to the community data.

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

20. We assume that the data stores are sufficiently protected and that side-channel attacks, extra-monitor and bad storage management are not possible

21. Side channel attacks on data flows are not considered as they are highly-unlikely to occur because they take a lot of analysis and the extracted information is not in correspondence of the effort

22. Internal processes are not susceptible to corruption as we assume processes are implemented correctly and input is sufficiently validated, and memory access is dealt with as well

23. The authentication process is assumed to be well implemented and secure

2.3.2 Threats

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)

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

r3.

T03 - Identifying a patient from his PHR data

Summary: A researcher with malicious intent identifies a patient in a set of PHR (or user) data

Primary mis-actor: unskilled insider

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 can extract the identity of the patient from each individual query result because of weak anonymization or he first links several results to each other (T01 - Profiling PHR data (linking), T02 - Linking PHR data to user data) which provides him with identifiable information

Consequence: The misactor gains access to the patient's identity although this should have remained secret

Reference to threat tree node(s): I_ds2

Parent threat tree(s): I_ds

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

Remarks:

r1. This threat was inspired by I_ds2, however none of the leaf nodes from the entity identifiable tree seemed to match

r2. Threats T01 - Profiling PHR data (linking) and T02 - Linking PHR data to user data are part of the preconditions of this threat

r3. The (weak) access requirement (I_ds1) is fullfilled 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)

T04 - Information disclosure of patient community data

Summary: An authenticated user can access personal information of all patients

Primary mis-actor: Unskilled insider/ skilled outsider

Basic path:

bf1. The misactor authenticates himself (by using his own valid credentials or by spoofing a user (threats T06 - Spoofing a user of the social network system by eavesdropping communication, 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))

bf2. The misactor gains access to the PHR data and/or user data

Consequence: Confidential patient data (5.1) or user registration data (5.2) are exposed to unauthorized users or outsiders

Reference to threat tree node(s): ID_ds7, ID_ds2

Parent threat tree(s): ID_ds

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

Remarks:

r1. This threat is applicable to both data stores, as they are both designed in the same way and use the same authentication process (5.9)

r2. Spoofing a user (T06 - Spoofing a user of the social network system by eavesdropping communication, 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) is considered a precondition of this threat

r3. Assumption 4 states that no access control system is present

r4. We assume that the data store itself is sufficiently protected which eliminates unencrypted data, side channel attacks (ID_ds4), extra-monitor access (ID_ds3) and bad storage management (ID_ds5) (assumption 20)

T05 - Spoofing a user of the social network system by falsifying credentials

Summary: The misactor obtains user credentials allowing him to log in nd access the system

Primary mis-actor: skilled outsider

Basic path:

bf1. The misactor gains access to the credentials of a user (by stealing, guessing, phishing, etc.) (S_8, S_12, S_13)

bf2. The misactor uses the authentic credentials to log in to the system

bf3. The misactor receives all privileges of the spoofed employee

Consequence: Confidential data (patient health information, log-in credentials, etc.) are exposed to outsiders (see threat T04 - Information disclosure of patient community data)

Reference to threat tree node(s): S_8, S_12, S_13

Parent threat tree(s): ID_ds, S

DFD element(s): 1 patient, 2 researcher, 3 nurse

Remarks:

r1. An authentication system is present in the architecture, which rules out threat S_4

r2. The authentication process is considered secure (assumption 23) thus the tampering threat (leaf of S_3) does not hold, and it does not support null credentials (S_10) or equivalence (S_09), downgrade authentication (S_11) or weak change management (S_09). Also no key distribution storage is present (S_14)

r3. Spoofing due to weak server-side storage is described by T07 - Spoofing a user of the social network system because of weak credential storage

r4. Spoofing due weak transit is described by T06 - Spoofing a user of the social network system by eavesdropping communication

r5. Spoofing only applies to patients, nurses, and researchers (assumption 18)

T06 - Spoofing a user of the social network system by eavesdropping communication

Summary: The misactor obtains user credentials allowing him to log in nd access the system

Primary mis-actor: skilled outsider

Basic path:

bf1. The misactor gains access to the credentials of a user by eavesdropping the credential communication (threats T08 - Disclosure of the transmitted log-in credentials and T09 - Disclosure of the transmitted session token) (S_6, S_7)

bf2. The misactor uses the authentic credentials to log in to the system

bf3. The misactor receives all privileges of the spoofed employee

Consequence: Confidential data (patient health information, log-in credentials, etc.) are exposed to outsiders (see threat T04 - Information disclosure of patient community data)

Reference to threat tree node(s): S_6, S_7

Parent threat tree(s): I_ds, S

DFD element(s): 1 patient, 2 researcher, 3 nurse

Remarks:

r1. An authentication system is present in the architecture, which rules out threat S_4

r2. The authentication process is considered secure (assumption 23) thus the tampering threat (leaf of S_3) does not hold, and it does not support null credentials (S_10) or equivalence (S_09), downgrade authentication (S_11) or weak change management (S_09). Also no key distribution storage is present (S_14)

r3. Gaining access to the credentials in transit is described by threats T08 - Disclosure of the transmitted log-in credentials and T09 - Disclosure of the transmitted session token

r4. Spoofing due to falsifying credentials is described in T05 - Spoofing a user of the social network system by falsifying credentials r5. Spoofing due to weak credential storage is described in T07 - Spoofing a user of the social network system because of weak credential storage

r6. Spoofing only applies to patients, nurses, and researchers (assumption 18)

T07 - Spoofing a user of the social network system because of weak credential storage

Summary: The misactor obtains user credentials allowing him to log in nd access the system

Primary mis-actor: skilled outsider

Basic path:

bf1. The misactor gains access to the credentials of a user by weak credential storage at the server side (threat T04 - Information disclosure of patient community data) (S_15)

bf2. The misactor uses the authentic credentials to log in to the system

bf3. The misactor receives all privileges of the spoofed employee

Consequence: Confidential data (patient health information, log-in credentials, etc.) are exposed to outsiders (see threat T04 - Information disclosure of patient community data)

Reference to threat tree node(s): S_8, S_12, S_13

Parent threat tree(s): ID_ds, S

DFD element(s): 1 patient, 2 researcher, 3 nurse

Remarks:

r1. An authentication system is present in the architecture, which rules out threat S_4

r2. The authentication process is considered secure (assumption 23) thus the tampering threat (leaf of S_3) does not hold, and it does not support null credentials (S_10) or equivalence (S_09), downgrade authentication (S_11) or weak change management (S_09). Also no key distribution storage is present (S_14)

r3. Spoofing due to falsifying credentials is described in T05 - Spoofing a user of the social network system by falsifying credentials

r4. Spoofing due to communication eavesdropping is described in T06 - Spoofing a user of the social network system by eavesdropping communication

r5. Spoofing only applies to patients, nurses, and researchers (assumption 18)

T08 - Disclosure of the transmitted log-in credentials

Summary: The misactor gains access to the data flow that contains the credentials used for log-in

Primary mis-actor: Skilled outsider

Basic path:

bf1. The misactor gains access to the data flow between the user and the authentication process

bf2. The misactor intercepts the credentials (username, password) of the user

Consequence: The misactor now has access to the user's log-in information and can from now on spoof the user

Reference to threat tree node(s): ID_df4, ID_df7

Parent threat tree(s): ID_df, S, ID_ds

DFD element(s): patient-authN (1-5.9), nurse-authN (2-5.9), researcher-authN (3-5.9)

Remarks:

r1. This threat is possible as the data flow between the entities and the system is considered insecure (assumption 3)

r2. Side channel attacks are not considered (assumption 21)

T09 - Disclosure of the transmitted session token

Summary: The misactor gains access to the data flow that contains the session token (which authenticates the user during the entire session)

Primary mis-actor: Skilled outsider

Basic path:

bf1. The misactor gains access to the data flow between the the authentication process and the user, or between the user and the portal

bf2. The misactor intercepts the session token of the user

Consequence: The misactor can use the session token to spoof the user during the current session

Reference to threat tree node(s): ID_df4, ID_df7

Parent threat tree(s): ID_df, S, ID_ds

DFD element(s): patient-portal (1-5.3), nurse-portal (2-5.3), researcher-portal (3-5.3), authN-patient (5.9-1), authN-nurse (5.9-2), authN-researcher(5.9-3)

Remarks:

r1. This threat is possible as the data flow between the entities and the system is considered insecure (assumption 3)

r2. Side channel attacks are not considered (assumption 21)

T10 - Disclosure of transmitted medical/personal information

Summary: The misactor gains access to the transmitted patient information

Primary mis-actor: Skilled outsider

Basic path:

bf1. The misactor gains access to the data flow between the user and the portal

bf2. The misactor intercepts the transmitted personal information

Consequence: The misactor has access to sensitive health or personal information

Reference to threat tree node(s): ID_df4, ID_df7

Parent threat tree(s): ID_df, S, ID_ds

DFD element(s): patient-portal(1-5.3), nurse-portal(3-5.5), portal-patient(5.3-1), portal-nurse(5.5-3), researcher-portal(2-5.4), portal-researcher (5.4-2), browse diseases-disease service (5.6-4)

Remarks:

r1. This threat is possible as the data flow between the entities and the system is considered insecure (assumption 3)

r2. We do not consider the response of the external disease service as it does not contain personal information (assumption 12)

r3. Side channel attacks are not considered (assumption 21)

T11 - Linkability of symptoms sent to external disease service

Summary: The misactor links several requests to the same user and creates a profile of this user

Primary mis-actor: unskilled insider (external disease service) /skilled outsider

Basic path:

bf1. The patient searches diseases by providing his symptoms to the patient portal, which forwards the request (including the patient's pseudonym) to the external disease service

bf2. The misactor intercepts the dataflow (threat T10 - Disclosure of transmitted medical/personal information or is (or has access to) the external disease service

bf3. The misactor can link several requests to the same patient

Consequence: The misactor can build a profile of the patient

Reference to threat tree node(s): L_df1, L_df8

Parent threat tree(s): L_df

DFD element(s): data flow from browse service to external disease service (5.6 $\rightarrow$ 4)

Remarks:

r1. L_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 linked, based on the transmitted (temporary/internal) user ID (L_df8)

r3. The right branch of the tree (insecure anonymity system (L_df4)) and the other leaf nodes of the non-anonymous communication branch (L_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

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 dataflow 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 $\rightarrow$ 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

T13 - Disclosure of internal transmitted medical/personal information

Summary: The misactor gains access to the transmitted patient information

Primary mis-actor: Skilled insider (e.g. admin)

Basic path:

bf1. The misactor gains access to the data flow between the user and the authentication process

bf2. The misactor intercepts the transmitted personal information

Consequence: The misactor has access to sensitive health or personal information

Reference to threat tree node(s): ID_df4, ID_df7

Parent threat tree(s): ID_df, S, ID_ds

DFD element(s): patient-portal(1-5.3), nurse-portal(2-5.3), portal-patient(5.3-1), nurse-patient(2-5.3)

Remarks:

r1. This threat is possible as the data flow between the entities and the system is considered insecure (assumption 3)

r2. Side channel attacks are not considered (assumption 21)

T14 - Information disclosure internal process

Summary: The misactor gains access to one of the internal processes

Primary mis-actor: authorized insider

Basic path:

bf1. The misactor has the required privileges to access to processes

bf2. The misactor uses his privileges to access information outside the scope of his job

Consequence: The misactor has access to (possibly sensitive) personal identifiable information

Reference to threat tree node(s): ID_p

Parent threat tree(s): ID_p

DFD element(s): patient portal (5.3), researcher portal (5.4), nurse portal (5.5), browse diseases (5.6), manage PHR (5.7), consult group PHR (5.8), authN (5.9)

Remarks:

r1. This threat is inspired by "spoofing an entity" leaf threat, however, when an insider has to much privileges, this threat applies as well. Spoofing entities with access to internal processes is not considered, as we assume the system is physically protected (assumption 1)

r2. We assume processes are not corruptable (assumption 22)

r3. The side channel attack is described in T15 - Side channel information disclosure internal process

T15 - Side channel information disclosure internal process

Summary: The misactor gains access to one of the internal processes

Primary mis-actor: skilled insider

Basic path:

bf1. The misactor performs a side channel attack on one of the internal processes

bf2. The misactor obtains process information

Consequence: The misactor has access to (possibly sensitive) personal identifiable information

Reference to threat tree node(s): ID_p2

Parent threat tree(s): ID_p

DFD element(s): patient portal (5.3), researcher portal (5.4), nurse portal (5.5), browse diseases (5.6), manage PHR (5.7), consult group PHR (5.8), authN (5.9)

Remarks:

r1. The alternative spoofing attack is described in T14 - Information disclosure internal process

r2. We assume processes are not corruptable (assumption 22)

T16 - Non-compliance of employees

Summary: The community service does not process patient data in compliance with legislations or policies

Primary mis-actor: insider (employee: admin, nurse, etc.)

Basic path:

bf1. The misactor fails to comply with the community's policy or legislation (e.g. the patient's data is revealed to third parties)

Consequence: The patient's personal information is shared without his knowledge. When detected, the community service can get fined, and its trustworthy reputation is ruined

Reference to threat tree node(s): PN_2

Parent threat tree(s): PN

DFD element(s): all (except entities)

Remarks:

r1. This threat applies to the entire system, as no individual DFD element is specifically targetted

r2. A similar threat which is posed by the developer is described in T18 - Non-compliance management

r3. A specific non-compliance threat concerning cnsents is described in T17 - Missing user consents

T17 - Missing user consents

Summary: The system did not ask the patient's permission to share part of his (pseudonymized) medical information with his group members

Primary mis-actor: Management

Basic path:

bf1. The management fails to require patient consents to be included in the user flow

bf2. The user is unable to state his preferences concerning personal data sharing

Consequence: The user's medical information (although pseudonymized), will be shared with the patient's group against his will

Reference to threat tree node(s): PN_3

Parent threat tree(s): PN

DFD element(s): entire (back-end) system (excluding entities)

Remarks:

r1. This threat applies to the entire system (assumption 7)

r2. Two general threats which correspond to general non-compliance are described in T16 - Non-compliance of employees and T18 - Non-compliance management

T18 - Non-compliance management

Summary: The management fails to request a design and implementation of the system in compliance with legislation

Primary mis-actor: Management

Basic path:

bf1. The misactor fails to require a system that is legally compliant (either he is unaware of the legislation or he consciously decides to ignore it)

bf2. The patient data is not processed or collected in accordance to (privacy) legislation

Consequence: The patient's personal information is shared without his knowledge. When detected, the community service can get fined, and its trustworthy reputation is ruined

Reference to threat tree node(s): PN_2

Parent threat tree(s): PN

DFD element(s): all (except entities)

Remarks:

r1. This threat applies to the entire system, as no individual DFD element is specifically targetted

r2. A similar threat which is posed by the employees when the system is up-and-running is described in T16 - Non-compliance of employees

r3. A specific non-compliance threat concerning cnsents is described in T17 - Missing user consents

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 is returned. The user's privacy is thus 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

T20 - content inaccuracy

Summary: The user failed to update his medical information or administrative information

Primary mis-actor: Management

Basic path:

bf1. The management fails to indicate the need of a notification that warns the user of the importance of up-to-date and accurate information

bf2. The user provides inaccurate or incomplete medical information or fails to update old information

Consequence: The user himself or users from his group consult the user's inaccurate medical information and deduce the wrong conclusion (e.g. user claims he got better by taking medication X, while he actually took medication Y)

Reference to threat tree node(s): U_3, U_4

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 users providing too much information is described in T19 - User unawareness

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.

2.4.1 High priority

- 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

Information disclosure of data (both medication data and patient data) is the most important threat as it violates the patient's privacy the most (the patient uses this system under the assumption that his information is kept confidential).

Also identifiability of stored PHR data has high priority as it should be assured that only the patient himself can access his own identifiable information and group members should not be able to identify the patient from his shared, de-identified medical data.

Information disclosure of transmitted data also poses a high risk, but less than information disclosure of the data store, as the data flow only reveals part of the information.

Finally, spoofing is considered high-priority. Even though spoofing is security threat, it can result in information disclosure of stored information, which has the highest risk.

2.4.2 Medium priority

- 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

Linkability and identifiability of the symptoms sent to the external disease service can violate the patient's privacy as they can reveal a certain disease. However, the threats are only considered medium risk as there is still some plausible deniability (as the patient might have been looking up a disease for a friend or relative).

Linking PHR data (to other PHR data or th user data) only poses a real threat when the linking actual leads to identification. Therefore, linkability on its own is only considered medium risk.

Non-compliance of the system in general, and missing consents and user unawareness specifically, will result in a violation of the patients' privacy. However, the management are considered knowledgeable and at least aware of the consequences of ignoring legislation. Also, even though officially a system is non-compliant, it is still possible that the general legislation concepts are present.

2.4.3 Low priority

- 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

Information inaccuracy is considered low risk, as inaccurate data can indeed lead to false conclusions, the patient community system is mainly focused on peer-information and in practice, no important decisions will be made based on these data.

The internal process and data flow threats are considered low priority as there is a trust relation with the employees. Most likely there is also a non-disclosure agreement in their contract with associated consequences (fine, fired, etc.) Non-compliance of employees is considered low risk for the same reason as the internal processes and data flows. Given the trust relationship between the employees and the company, it is less likely that they will violate the rules.