LINDDUN analysis example: smart grid system

Contents

Introduction

This document describes an example privacy analysis using the LINDDUN privacy threat modeling methodology[1]. In this section, we briefly describe the application domain and this particular architecture.

This document was mainly used as baseline for the evaluation of a descriptive study, hence the focus of this report is the threat elicitation. For helping the reader understand the application, we however also provide a (simplified) component diagram and corresponding DFD.

Smart Grid application

The smart grid application analyzed in this document is *ReMeS, a smart grid remote measurement, monitoring and control system.*

A simplified component diagram can be found in 1. We refer the interested reader to the full architectural description[2][3] for more details.

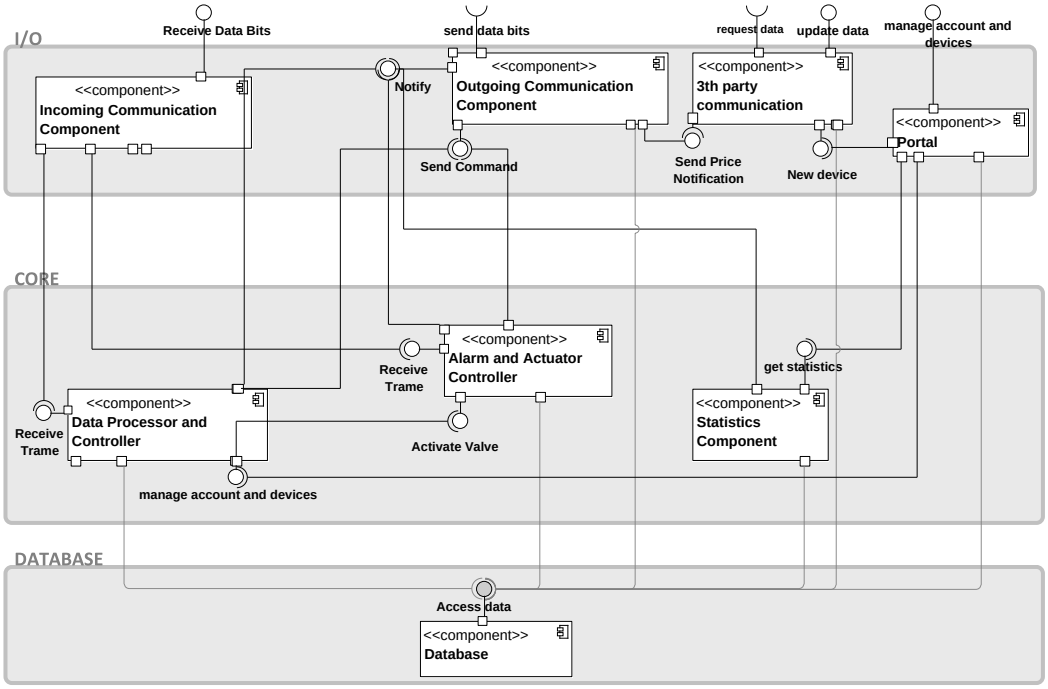

Figure 1: The (simplified) component diagram of the smart grid system

[1] Mina Deng, Kim Wuyts, Riccardo Scandariato, Bart Preneel, 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

[2] General ReMeS description: https://sites.google.com/site/linddunstudy/study2_system_description.pdf

[3] Architectural ReMeS description: https://sites.google.com/site/linddunstudy/study2_architecture_report.pdf

1 DFD

The DFD in Figure 2 clearly reflects the ReMeS component diagram (see Figure 1).

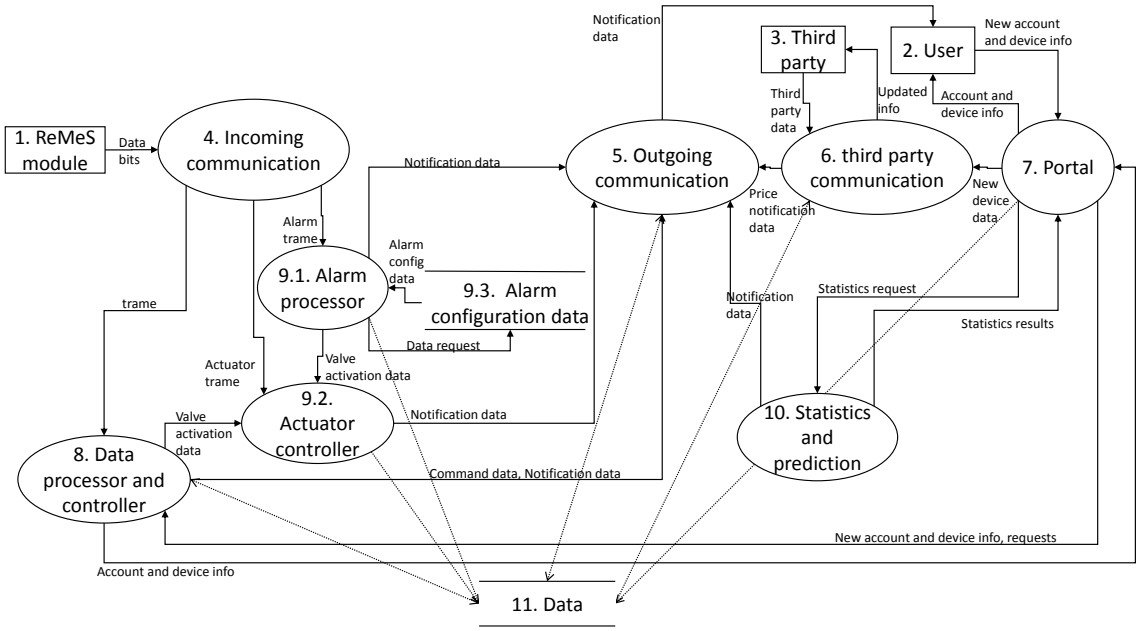

Figure 2: A sample DFD corresponding to the component-connector diagram

2 Mapping table

We refer the reader to the full architectural description of ReMeS[4]. The large client-server diagram was in fact used in a one-to-one mapping for the DFD in this baseline and the mapping table will hence be alike.

3 Threat elicitation

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

[4]Architectural ReMeS description: https://sites.google.com/site/linddunstudy/study2_architecture_report.pdf

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 only a threat to the data flow between ReMeS and the module. The privacy concerns of the rest of the 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 (customers, technicians, operators, researchers or external services) 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 ReMeS service is not considered an issue.

9. Identifiability of the data flow only poses a threat to the statistics data flows: as (re)identification of the anonymized statistics should be avoided

10. Linkability of the statistics data flows is the only linkability threat to data flows in the ReMeS system. Although less likely, when the identifiers are replaces by pseudonyms, linking the different statistics (of different searches) together can still result in an identifiability threat

11. Linkability of entities (customers, modules, ...) 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 ReMeS service is not considered an issue.

12. The external services are not authenticated to the back-end system

13. Linkability and identifiability do not pose a threat to the data flows between entities (customers, technicians, ...) and (portal) processes because of assumptions 8 and 11

14. 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 user's privacy. The user's privacy is only violated when the content of the communication is revealed (information disclosure threat)

15. Linkability and identifiability do not apply to internal processes as knowing that 2 actions belong to the same user does not violate the user's privacy. The user's privacy is only violated when the content of the action is revealed (information disclosure threat)

16. Identifiability and linkability are applicable to the data store(s)

17. Spoofing is a threats to all entities (modules, users and external services (UIS, billing)

18. Content unawareness only applies to the consumer, as he should be aware of the information he shares

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

20. 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

21. 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

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

3.2 Threats

The eliciting threats were identified based on the (original) LINDDUN threat trees[5]. We refer the reader to the LINDDUN website for the latest version of the trees[6].

T01 - Profiling ReMeS data (L DS)

Summary: A researcher or other insider with malicious intent links ReMeS 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 ReMeS data or user data store and retrieves very detailed results

bf2. The misactor links the results of the queries together (e.g. based on repeating patterns, or pseudo-identifiers like street and age)

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

Reference to threat tree node(s): L_ds2, L_e2

Parent threat tree(s): L_ds, I_ds

Remarks:

r1. This threat can be used as precondition for the identifiability threat at the data store (T03 - Identifying a user from his ReMeS data (I DS))

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 ReMeS data case, it also applies to the user data store (assumption 4)

T02 - Linking ReMeS data to user data (L DS)

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

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

Basic path:

bf1. The misactor retrieves information from both the ReMeS 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 personal identifiable information and especially poses a privacy threat when the misactor sells the information (e.g. advertisers, etc.)

[5]Catalog of original LINDDUN threat trees: http://people.cs.kuleuven.be/ kim.wuyts/LINDDUN/

[6]Official LINDDUN website containing the most recent description of the methodology and threat tree catalog: https://distrinet.cs.kuleuven.be/software/linddun

Reference to threat tree node(s): L_ds2, L_e6

Parent threat tree(s): L_ds, I_ds

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 user from his ReMeS data (I DS)

Summary: A user with malicious intent identifies a user in a set of ReMeS (or user) data (from the statistics results)

Primary mis-actor: unskilled insider

Basic path:

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

bf2. The misactor can extract the identity of the customer from each individual query result because of weak anonymization or he first links several results to each other (T01 - Profiling ReMeS data (L DS), T02 - Linking ReMeS data to user data (L DS)) which provides him with identifiable information

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

Reference to threat tree node(s): I_ds2

Parent threat tree(s): I_ds

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 ReMeS data (L DS) and T02 - Linking ReMeS data to user data (L DS) 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 ReMeS data case, it also applies to the user data store (assumption 4)

T04 - Information disclosure of ReMeS data (iD DS)

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

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 ReMeS entity by eavesdropping communication (S E), T05 - Spoofing a ReMeS entity by falsifying credentials (S E), T07 - Spoofing a ReMeS entity because of weak credential storage (S E)))

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

Consequence: customer data or UIS data are exposed to unauthorized users or outsiders

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

Parent threat tree(s): ID_ds

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 ReMeS entity by eavesdropping communication (S E), T05 - Spoofing a ReMeS entity by falsifying credentials (S E), T07 - Spoofing a ReMeS entity because of weak credential storage (S E)) 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 19)

T05 - Spoofing a ReMeS entity by falsifying credentials (S E)

Summary: The misactor obtains user credentials allowing him to log in and 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 user (e.g. the operator)

Consequence: Confidential customer or UIS data are exposed to outsiders (see threat T04 - Information disclosure of ReMeS data (iD DS))

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

Parent threat tree(s): ID_ds, S

Remarks:

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

r2. The authentication process is considered secure (assumption 22) 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 ReMeS entity because of weak credential storage (S E)

r4. Spoofing due weak transit is described by T06 - Spoofing a ReMeS entity by eavesdropping communication (S E)

r5. Spoofing applies to all entities (assumption 17, although spoofing a module will not result in privacy threats but will in integrity threats)

T06 - Spoofing a ReMeS entity by eavesdropping communication (S E)

Summary: The misactor obtains user credentials allowing him to log in and 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 (iD DF) and T09 - Disclosure of the transmitted session token (iD DF)) (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 user (e.g. an employee)

Consequence: Confidential customer or UIS data are exposed to outsiders (see threat T04 - Information disclosure of ReMeS data (iD DS))

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

Parent threat tree(s): I_ds, S

Remarks:

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

r2. The authentication process is considered secure (assumption 22) 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 (iD DF) and T09 - Disclosure of the transmitted session token (iD DF)

r4. Spoofing due to falsifying credentials is described in T05 - Spoofing a ReMeS entity by falsifying credentials (S E)

r5. Spoofing due to weak credential storage is described in T07 - Spoofing a ReMeS entity because of weak credential storage (S E)

r6. Spoofing applies to all entities (assumption 17)

T07 - Spoofing a ReMeS entity because of weak credential storage (S E)

Summary: The misactor obtains user credentials allowing him to log in and 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 ReMeS data (iD DS)) (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 customer or UIS data are exposed to outsiders (see threat T04 - Information disclosure of ReMeS data (iD DS))

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

Parent threat tree(s): ID_ds, S

Remarks:

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

r2. The authentication process is considered secure (assumption 22) 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 ReMeS entity by falsifying credentials (S E)

r4. Spoofing due to communication eavesdropping is described in T06 - Spoofing a ReMeS entity by eavesdropping communication (S E)

r5. Spoofing applies to all entities (assumption 17)

T08 - Disclosure of the transmitted log-in credentials (iD DF)

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

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 20)

r3. This threat only applies to the flows between the users and the portals, as other entities (UIS, billing, modules) currently do not authenticate

T09 - Disclosure of the transmitted session token (iD DF)

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

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 20)

r3. This threat only applies to the flows between the users and the portals, as other entities (UIS, billing, modules) currently do not authenticate

T10 - Disclosure of transmitted ReMeS/personal information (iD DF)

Summary: The misactor gains access to the transmitted customer/ReMeS information

Primary mis-actor: Skilled outsider

Basic path:

bf1. The misactor gains access to an external data flow (e.g. between the user and the portal)

bf2. The misactor intercepts the transmitted information

Consequence: The misactor has access to ReMeS or customer information

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

Parent threat tree(s): ID_df, S, ID_ds 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. Side channel attacks are not considered (assumption 20)

T11 - Linkability of statistics (L DF)

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 user searches ReMeS statistics on the portal

bf2. The misactor intercepts the dataflow (threat T10 - Disclosure of transmitted ReMeS/personal information (iD DF) or he is the user performing the queries

bf3. The misactor can link several requests to the same customer/UIS

Consequence: The misactor can build a profile of the customer/UIS

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

Parent threat tree(s): L_df

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 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 (user) whose identity should be protected, but the data subject (customer), who is not directly part of the data flow

r3. This threat applies to all data flows between a user and a portal that support statistical queries

T12 - Identifiability of statistics (I DF)

Summary: The misactor extracts the customer's/UIS identity from the request

Primary mis-actor: unskilled insider/skilled outsider

Basic path:

bf1. The user searches statistics on the portal

bf2. The misactor intercepts the dataflow or is the requesting user

Consequence: The misactor knows which customer has a certain consumption

Reference to threat tree node(s): I_df1, I_df8

Parent threat tree(s): I_df

Remarks:

r1. I_df1 requires an unprotected data flow, which is currently present (assumption 3) and mis-actor is receiver, thus assumption always applies

r2. 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 (user) whose identity should be protected, but the data subject (customer), who is not directly part of the data flow

r3. This threat applies to all data flows between a user and a portal that support statistical queries

T13 - Disclosure of internal transmitted information (iD DF internal)

Summary: The misactor gains access to the transmitted ReMeS information

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

Basic path:

bf1. The misactor has the required insider privileges gains access to the data flow between internal processes

bf2. The misactor intercepts the transmitted information

Consequence: The misactor has access to ReMeS or customer information

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

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

Remarks:

r1. This attack is possible because the attacker is an insider (assumption 2)

r2. Side channel attacks are not considered (assumption 20)

T14 - Information disclosure internal process (iD P internal)

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 ReMeS and user information

Reference to threat tree node(s): ID_p

Parent threat tree(s): ID_p

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 21)

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

T15 - Side channel information disclosure internal process (iD P internal)

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 ReMes and user information

Reference to threat tree node(s): ID_p2

Parent threat tree(s): ID_p

Remarks:

r1. The alternative spoofing attack is described in T14 - Information disclosure internal process (iD P internal)

r2. We assume processes are not corruptable (assumption 21)

T16 - Non-compliance of employees (NC)

Summary: The ReMeS service does not process user data in compliance with legislations or policies

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

Basic path:

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

Consequence: The customer's personal information (or sensitive UIS company information) is shared without his knowledge. When detected, the ReMeS system can get fined, and its trustworthy reputation is ruined

Reference to threat tree node(s): PN_2

Parent threat tree(s): PN

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 (NC)

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

T17 - Missing user consents (NC)

Summary: The system did not ask the customer's permission to share part of his (pseudonymized) ReMeS information

Primary mis-actor: Management

Basic path:

bf1. The management fails to require user 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 information is shared against his will

Reference to threat tree node(s): PN_3

Parent threat tree(s): PN

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 (NC) and T18 - Non-compliance management (NC)

T18 - Non-compliance management (NC)

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 customer data is not processed or collected in accordance to (privacy) legislation

Consequence: The customer's personal information (or UIS company information) is shared without his knowledge. When detected, the ReMeS system can get fined, and its trustworthy reputation is ruined

Reference to threat tree node(s): PN_2

Parent threat tree(s): PN

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 (NC)

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

T19 - User unawareness (U)

Summary: The customer 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 customer intends to upload sensitive and/or identifiable content (e.g. to integrate habits in the anomaly detector)

bf2. The customer adds information to the system which can identify him as he is unaware of the consequences

Consequence: When authenticated users retrieve information, the identifiable information is returned. The customer'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

Remarks:

r1. This threat only applies to the customer (assumption 18)

r2. The threat concerning inaccurate user information is described in T20 - content inaccuracy (U) and expired data in T21 - content unawareness - expired data (U)

T20 - content inaccuracy (U)

Summary: The customer failed to update his 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 personal information or fails to update old information

Consequence: The system uses inaccurate information in its calculations (e.g. wrong demand predictions, anomaly checks, billing addresses)

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

Parent threat tree(s): U

Remarks:

r1. This threat only applies to the customer (assumption 18)

r2. The threat concerning users providing too much information is described in T19 - User unawareness (U) and expired data in T21 - content unawareness - expired data (U)

T21 - content unawareness - expired data (U)

Summary: Expired customer's data is not removed

Primary mis-actor: Management

Basic path:

bf1. The management fails to indicate the need the removal of outdated information (e.g. customers who stopped using ReMeS)

bf2. Expired information stays available in the system

Consequence: The customer's privacy is violated, as he assumes that the old data is destroyed.

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

Parent threat tree(s): U

Remarks:

r1. This threat only applies to the customer (assumption 18)

r2. The threat concerning users providing too much information is described in T19 - User unawareness (U) and inaccurate user information in T20 - content inaccuracy (U)

T22 - Detectability of module flows (D DF)

Summary: An message is sent by the module on an unexpected time, revealing an anomaly situation

Primary mis-actor: Skilled outsider

Basic path:

bf1. The module detects an anomaly/error and sends an alarm message to ReMeS

bf2. The misactor is eavesdropping the module communication flow

bf3. The misactor notices a message sent on an unexpected time (no dummy traffic) and knows an emergency situation exists

Consequence: The customer's privacy is violated, as outsiders can determine whether or not an emergency situation occurs.

Reference to threat tree node(s): D_df4, D_df9

Parent threat tree(s): D