Software Architecture

Remote Measurement, Monitoring and Control System: Phase 3 - Privacy analysis report

Professoren: Wouter Joossen,
Riccardo Scandariato,
Kim Wuyts

Maarten Allard - s0199048
Kristof Coninx - s0199831

May 14, 2012

Contents

1 Understanding the architecture

In this section a usage scenario in the provided ReMeS system will be explained by using the ReMeS components and client-server view diagrams. The scenario in question is the scenario where an alarm arrives at the ReMeS back-end and the actuator is activated.

When an alarm trame arrives at the ReMeS back-end, first of all the incoming communication component will translate the stream of bits to a NativeDataTrame. Then the same component will analyze that NativeDataTrame to find out what kind of trame it is. This analyzation will conclude that it is indeed an alarm trame.

Since the trame is an alarm trame, the incoming communication component will call the method receiveAlarmTrame in the alarm processor. The alarm processor will store this alarm in the database and will receive the alarm configuration data from the database. If this data includes a customer notification, it will call the notifyAlarm method of the outgoing communication component. This outgoing communication component will then make sure that the customer gets notified about the alarm.

If the alarm configuration data includes a valve actuation, the actuator controller will be called by the alarm processor. The actuator controller will then create an actuator message for the specific valve and call the correct method in the outgoing communication component. If the incoming communication component receives an acknowledgement, this data will be stored in the database. If the incoming communication component doesn't receive an acknowledgement trame, the actuator controller will make the outgoing communication component resend the control trame. The actuator controller will attempt to do this a certain amount of times. If there is still no acknowledgement received, the notifyIssue method will be called in the outgoing communication component. The customer will be notified about the issue.

2 Privacy analysis

2.1 Data Flow Diagram

The data flow diagrams (DFD) depicted in figures 1 and 2 are based on the client-server view of the ReMeS system.

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

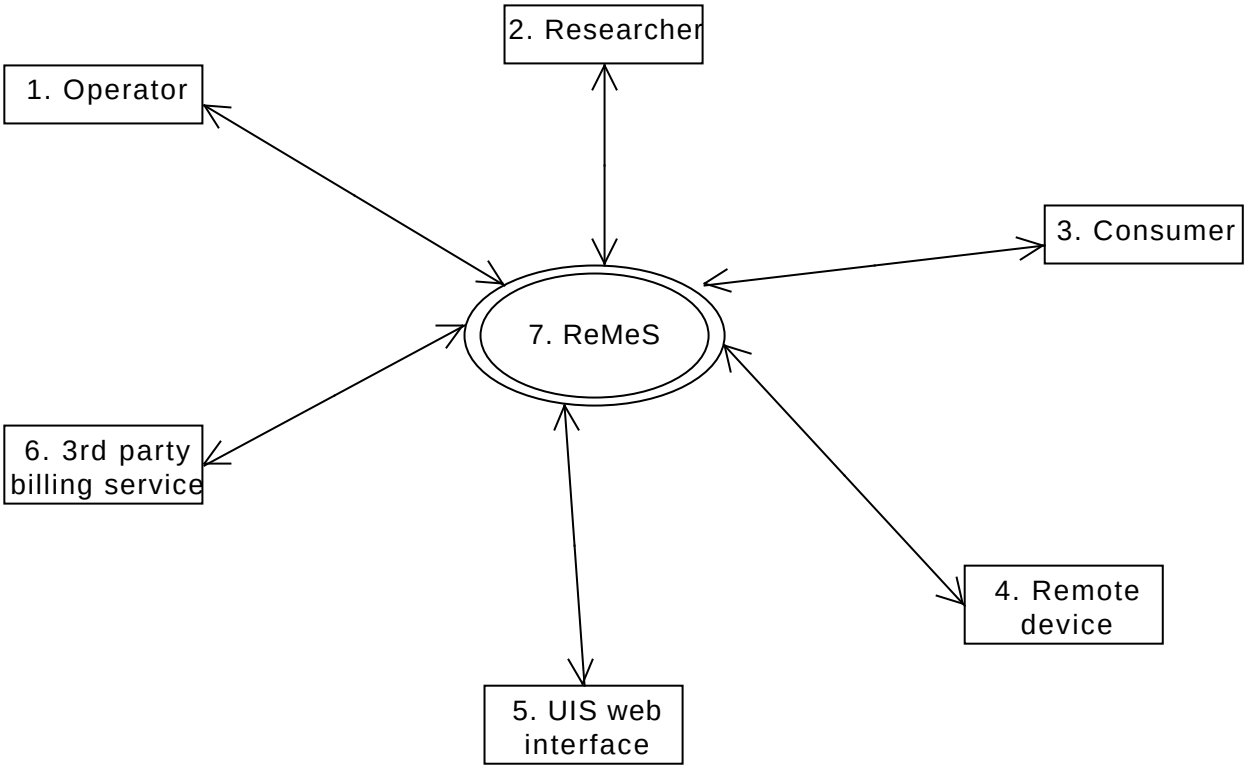

Figure 1: The Level 0 DFD diagram for ReMeS.

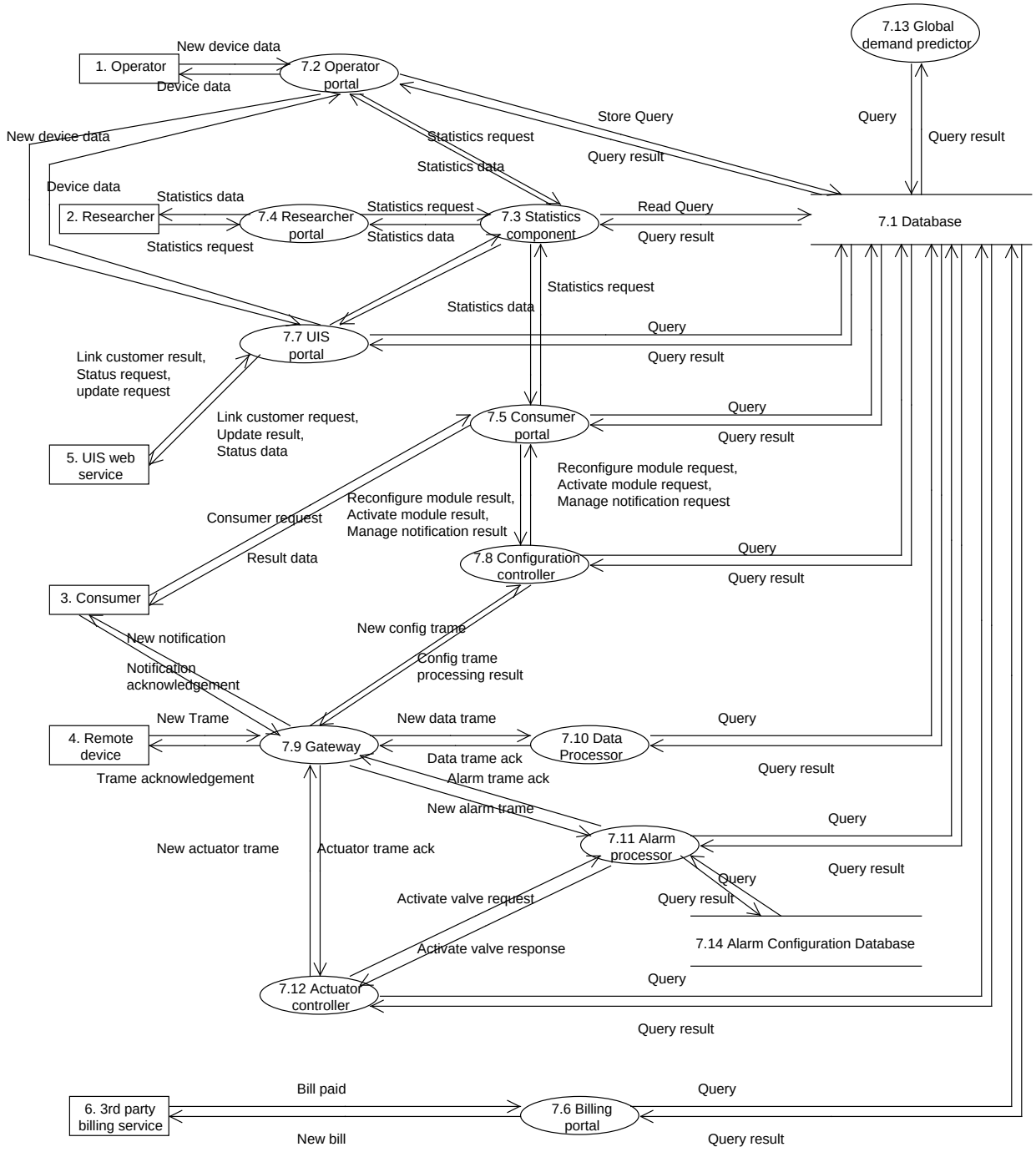

Figure 2: The Level 1 DFD diagram for ReMeS.

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. The price rate notifier is not depicted in the client-server view, and is assumed to be part of the UIS web component.
3. The UIS web service entity represents the UIS component that actually uses the ReMeS interface to communicate and not the offered web service to the UIS component.

4. The authentication component is missing from the diagrams because it is assumed that the session token is sent from the users to the portal for each request.
5. The Data processor component and the anomaly detector component were combined to one process: Data processor, because the additional process would not introduce any more information about or threats to the system.
6. The *Store query* represents an insert request to the database of some sorts, while the *Read query* represents a retrieval query for the database. If just *Query* is used, it is assumed that the flow will contain both read and insert requests.

2.2 Mapping of threats to DFD

This section gives an overview of the different threats that exist for each DFD element. The DFD element names are represented in the DFD of the previous section! This table is split up in to different sections for data stores, data flows, processes and entities.

	Threat target	L	I	N	D	D	U	N
Data Store	Database (7.1)	×	×	×	×	×		×
	Alarm configuration DB (7.14)	×	×	×	×	×		×
Data Flow	Operator – Operator portal (1 - 7.2)	×	×	×	×	×		×
	Operator portal – Operator (7.2 - 1)	×	×	×	×	×		×
	Researcher – Reasearcher portal (2 - 7.4)	×	×	×	×	×		×
	Researcher portal – Reasearcher (7.4 - 2)	×	×	×	×	×		×
	Consumer – Consumer portal (3 - 7.5)	×	×	×	×	×		×
	Consumer portal – Consumer (7.5 - 3)	×	×	×	×	×		×
	Consumer – Gateway (3 - 7.9)	×	×	×	×	×		×
	Gateway – Consumer (7.9 - 3)	×	×	×	×	×		×
	Remote device – Gateway (4 - 7.9)	×	×	×	×	×		×
	Gateway – Remote device (7.9 - 4)	×	×	×	×	×		×
	UIS web service – UIS portal (5 - 7.7)	×	×	×	×	×		×
	UIS portal – UIS web service (7.7 - 5)	×	×	×	×	×		×
	3rd party billing service – Billing portal (6 - 7.6)	×	×	×	×	×		×
	Billing portal – 3rd party billing service (7.6 - 6)	×	×	×	×	×		×
	Operator portal – UIS Web service (7.2 - 7.7)	×	×	×	×	×		×
	UIS Web service – Operator portal (7.7 - 7.2)	×	×	×	×	×		×
	Operator portal – Database (7.2 - 7.1)	×	×	×	×	×		×
	Database – Operator portal (7.1 - 7.2)	×	×	×	×	×		×
	Operator portal – Statistics component (7.2 - 7.3)	×	×	×	×	×		×
	Statistics component – Operator portal (7.3 - 7.2)	×	×	×	×	×		×
	Researcher portal – Statistics component (7.4 - 7.3)	×	×	×	×	×		×
	Statistics component – Researcher portal (7.3 - 7.4)	×	×	×	×	×		×
	UIS portal – Statistics component (7.7 - 7.3)	×	×	×	×	×		×
	Statistics component – UIS portal (7.3 - 7.7)	×	×	×	×	×		×
	UIS portal – Database (7.7 - 7.1)	×	×	×	×	×		×
	Database – UIS portal (7.1 - 7.7)	×	×	×	×	×		×
	Consumer portal – Statistics component (7.5 - 7.3)	×	×	×	×	×		×
	Statistics component – Consumer portal (7.3 - 7.5)	×	×	×	×	×		×
	Consumer portal – Database (7.5 - 7.1)	×	×	×	×	×		×
	Database – Consumer portal (7.1 - 7.5)	×	×	×	×	×		×
	Statistics component – Database (7.3 - 7.1)	×	×	×	×	×		×
	Database – Statistics component (7.1 - 7.3)	×	×	×	×	×		×
	Configuration controller – Consumer portal (7.8 -7.5)	×	×	×	×	×		×
	Consumer portal – Configuration controller (7.5 -7.8)	×	×	×	×	×		×
	Configuration controller – Database (7.8 - 7.1)	×	×	×	×	×		×
	Database – Configuration controller (7.1 - 7.8)	×	×	×	×	×		×

	Gateway – Configuration controller (7.9 - 7.8)	×	×	×	×	×	×
	Configuration controller – Gateway (7.8 - 7.9)	×	×	×	×	×	×
	Gateway – Data processor (7.9 - 7.10)	×	×	×	×	×	×
	Data processor – Gateway (7.10 - 7.9)	×	×	×	×	×	×
	Data processor – Database (7.10 - 7.1)	×	×	×	×	×	×
	Database – Data processor (7.1 - 7.10)	×	×	×	×	×	×
	Gateway – Alarm processor (7.9 - 7.11)	×	×	×	×	×	×
	Alarm processor – Gateway (7.11 - 7.9)	×	×	×	×	×	×
	Alarm processor – Alarm Configuration Database (7.11 - 7.14)	×	×	×	×	×	×
	Alarm Configuration Database – Alarm processor (7.14 - 7.11)	×	×	×	×	×	×
	Alarm processor – Database (7.11 - 7.1)	×	×	×	×	×	×
	Database – Alarm processor (7.1 - 7.11)	×	×	×	×	×	×
	Alarm processor – Actuator controller (7.11 - 7.12)	×	×	×	×	×	×
	Actuator controller – Alarm processor (7.12 - 7.11)	×	×	×	×	×	×
	Gateway – Actuator controller (7.9 - 7.12)	×	×	×	×	×	×
	Actuator controller – Gateway (7.12 - 7.9)	×	×	×	×	×	×
	Actuator controller – Database (7.12 - 7.1)	×	×	×	×	×	×
	Database – Actuator controller (7.1 - 7.12)	×	×	×	×	×	×
	Billing portal – Database (7.6 - 7.1)	×	×	×	×	×	×
	Database – Billing portal (7.1 - 7.6)	×	×	×	×	×	×
	Global demand predictor – Database (7.13 - 7.1)	×	×	×	×	×	×
	Database – Global demand predictor (7.1 - 7.13)	×	×	×	×	×	×
Process	Operator portal (7.2)	×	×	×	×	×	×
	Researcher portal (7.4)	×	×	×	×	×	×
	Actuator controller (7.12)	×	×	×	×	×	×
	Consumer portal (7.5)	×	×	×	×	×	×
	Billing portal (7.6)	×	×	×	×	×	×
	UIS portal (7.7)	×	×	×	×	×	×
	Statistics component (7.3)	×	×	×	×	×	×
	Alarm Processor (7.11)	×	×	×	×	×	×
	Data processor (7.10)	×	×	×	×	×	×
	Configuration controller (7.8)	×	×	×	×	×	×
	Global demand predictor (7.13)	×	×	×	×	×	×
Entity	Operator (1)	×	×			×	
	Researcher (2)	×	×			×	
	Consumer (3)	×	×			×	
	Remote Module (4)	×	×			×	
	UIS web service (5)	×	×			×	
	3rd party billing service (6)	×	×			×	

Table 1

After making different assumptions about the system and analysing the possible threats further, a lot of possible threats were ruled out. The final threat table can be seen in the following figure. In this table only the actually handled threats are represented.

	Threat target	L	I	N	D	D	U	N
Data Store	General Database (7.1)	×	×			×		×
Data Flow	Operator – Operator portal (1 - 7.2)							×
	Researcher – Reasearcher portal (2 - 7.4)							×
	Consumer – Consumer portal (3 - 7.5)							×
	Consumer – Gateway (3 - 7.9)							×
	Remote device – Gateway (4 - 7.9)							×
	UIS web service – UIS portal (5 - 7.7)	×	×					×
	3rd party billing service – Billing portal (6 - 7.6)							×
	General internal dataflow		×			×		×
Process	General internal process (7.2)							×
Entity	Operator (1)							
	Researcher (2)							
	Consumer (3)		×				×	
	Remote Module (4)		×					
	UIS web service (5)							
	3rd party billing service (6)							

Table 2

2.3 Threat elicitation

2.3.1 Assumptions

This section discusses the different assumptions that were made. 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 is also included.

These numbered assumptions will also be referenced to quite a lot in the threat elicitation section.

1. All internal processes can only be compromised by internal threats. We consider the back-end capable of protecting these internal processes from outsider threats. Therefor we will consider only one process, representing all internal processes, since the same threats apply to all of them.
2. Likewise to the previous assumption, all data flows between the internal processes are also considered as one data flow, since those threats apply to all of them. Like the previous assumption, data flows between internal processes are only vulnerable to internal threats.
3. Other dataflows (not between internal processes) are not grouped to one dataflow, since different threats may apply. Since these flows are not only between internal processes, the back-end cannot guarantee protection of these flows.
4. We assume that the data stores are encrypted and have a layer of access control installed. This leads us to trusting the data stores and as such, we will only consider one data store to represent all the stores. The data stores also have access control installed. This access control ensures that certain processes/entities only have access to the bare minimum amount of information needed for that process/entity. Queries requesting more information than a process or entity is allowed to have are blocked by this control. Since the data stores are encrypted very well and there is access control installed, identifiability and linkability are not an issue with our data stores (except for the administrator who has all access rights).
5. No non-repudiation threats exist in our system. Our system stores utility usages and creates invoices based upon these usages. This means our system components do not need plausible deniability.
6. Detectability also is not a pressing concern in our 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 in our system. However, this threat is not specific for a component of our system, but poses to the system as a whole. We will therefor not make a distinction between the different DFD elements for this threat.
8. The only dataflow between entities and internal processes that is susceptible to linkability and identifiability threats is the data flow between the external UIS service and the UIS portal process. Linking the company contacted with internal data flows might reveal personal information of a customer such as his utility provider. Since we allready assumed that the internal components are shielded off from the outside world and their threats, we can assume that linkability and identifiability are not an issue for the internal data flows of our system.
9. We assume that the data flows between external entities and internal processes are SSL-encrypted. We will also assume that trames sent via sms/gprs are also using an encrypted channel, provided by the service provider.
10. The only entities that directly add data to the system are the consumer and the remote device. Therefor we can assume that content unawareness is not a threat to the other entities.
11. The remote devices are preprogrammed to only send useful data. We can assume that content unawareness is not a threat for the remote device entity.

12. The identifiability of the entities *consumer* is considered to be a threat. The other entities all use a unique identifier and have no possible need to hide their identities.
13. Information disclosure of data not meant to be accessed by certain internal users is not an issue because of the access control to the data stores, mentioned in assumption 4. Every user is able to access only specific views of the data store needed to execute their function.
14. We assume that the portals for employees are only accessible from inside the company network and not via the internet. This limits the threats to unauthorized access to customer or researcher functions from outside the system.
15. The authentication system is assume to be well implemented and secure.
16. The authentication credentials are also assumed to be stored securely on the server side.
17. Internal processes are not susceptible to corruption as we assume processes are implemented correctly and input is suficiently validated, and memory access is dealt with as well.
18. 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.

2.3.2 Threats

This section documents the threats which were uncovered in the mapping section. Each threat description strictly follows the provided template.

T01 - Linking Alarm configuration data to user data

Summary: The administrator or another insider with administrator rights is able to access both the alarm configuration database and the general database and will be able to link these two together. Access control to both these databases limit the type of requests a user can issue on any database but administrator rights are transitive to all other types of users.

Primary mis-actor: Moderately skilled insider who is able to execute and manipulate his own access rights.

Basic path:

bf1. The misactor invokes the rights of a user with valid access to the alarm configuration database

bf2. The misactor retrieves information from the alarm configuration database

bf3. The misactor invokes the rights of a user with valid access to the general database

bf4. The misactor retrieves information from the general database

bf5. The misactor links both sets of data (e.g. based on a shared foreign key)

Consequence: The combined sets of data contain possibly sensitive personal data such as emergency notification telephone numbers. This poses an actual privacy threat when the misactor sells this information to interested parties, such as criminal organisations.

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

Parent threat tree(s): L_ds, L_e.

DFD element(s): 7.14 Alarm configuration database, 7.1 Database

Remarks:

r1. The L_ds1 requirement of weak access is only fulfilled when the misactor has the access rights of the root of the access right hierarchy. In all other instances this precondition is not met due to the installed access control for regular users. These root users will have the ability to circumvent the installed access control in some particular situations.

r2. The linkability of entity leaf node L_e6, indicating linkability based on a device's temporary ID, inspired to this data store linkability threat.

T02 - Information disclosure of customer usage history

Summary: An authenticated internal user can access personal usage history of any customer he wants.

Primary mis-actor: Unskilled insider

Basic path:

bf1. The misactor authenticates himself (by using his own credentials or by spoofing another valid user).

bf2. The misactor gains indirect access to the database and is able to perform queries about certain certain contents.

Consequence: Confidential usage history data and personal data is exposed to the authenticated user (researcher or operator). This way an unauthorised user can access information that is not supposed to be available to said user.

Reference to threat tree node(s): ID_ds9, ID_ds2

Parent threat tree(s): ID_ds

DFD element(s): 7.1 Database

Remarks:

r1. This threat is only applicable to the general database (7.1) because the alarm configuration database is not accessible via non automated entities.

r2. Spoofing a user is considered a precondition of this threat. By spoofing another user, different contents in the database is made accessible to the user.

r3. Although access control is installed for the data stores as explained in assumption 4 and that only internal users (e.g.employees) have access to the data stores (assumption 14, the protection scheme can be circumvented as specified in ID_ds9 by internal employees spoofing other types of employees and thus gaining other access rights. See threat T03.

r4. We assume 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 4).

T03 - Spoofing an internal user of ReMeS by falsifying credentials

Summary: The misactor obtains user credentials allowing him to log in and access the system as a user other than himself.

Primary mis-actor: Skilled insider

Basic path:

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

bf2. The misactor uses the credentials to log in to the system as another type of user.

bf3. The misactor receives all priveleges of the spoofed employee

Consequence: Confidential data can possibly be viewed by users that are normally not able to view this data. This misactor could possibly expose sensitive data to the outside.

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

Parent threat tree(s): ID_ds, S

DFD element(s): 1. Operator, 2. Researcher

Remarks:

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

r2. The authentication process is considered secure (assumption 15) 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 (S_15) is not possible because of assumption 16.

r4. Spoofing due to weak transit is not possible due to the strong ssl encryption of the communication between entities and portals (assumption 9).

r5. Spoofing only applies to operators and researchers (assumption 14).

r6. Spoofing due to weak credential storage on client-side is described in T04 - Spoofing a user of ReMeS because of weak credential storage. .

T04 - Spoofing a user of ReMeS because of weak credential storage.

Summary: The misactor obtains user credentials from a client side system allowing him to log in and access the system.

Primary mis-actor: Skilled insider or skilled outsider

Basic path:

bf1. The misactor gains access to the credentials of a user by weak credential storage at the client side (e.g. unprotected text file for easy recall of credentials)(S_13).

bf2. The misactor uses the authentic credentials to log in to the system as an other user than himself.

bf3. The misactor receives all privileges of the spoofed employee or customer

Consequence: Confidential data is possibly exposed to outsiders.

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

Parent threat tree(s): ID_ds, S

DFD element(s): 1. Operator, 2. Researcher, 3.Consumer

Remarks:

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

r2. The authentication process is considered secure (assumption 15) 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 crednetials is described in T03 - Spoofing an internal user of ReMeS by falsifying credentials.

r4. This form of spoofing can apply to outside users (consumers) or inside users (operators and researchers), but spoofing outside users does not affect the inside entities or vice versa.

T05 - Linkability of requests sent to external UIS

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

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

Basic path:

bf1. A bill is being made for a certain customer. Requests are sent to the correct UIS (there exist different companies, requests need to be sent to the UIS of the company who has the customer).

bf2. The misactor intercepts the data flow.

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

Consequence: The misactor can build a profile of the patient. The misactor knows the utility company of the customer.

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

Parent threat tree(s): L_df

DFD element(s): data flow from UIS portal to UIS web service (7.7 - 5).

Remarks:

r1. The misactor doesn't have to know about the content being sent, only which UIS is being consulted.

r2. To link the different requests, the misactor has to know for which customer a bill is being made, which makes this threat very unlikely.

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.

T06 - 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): All internal processes (7.2 - 7.13)

Remarks:

r1. This threat especially applies to administrators of our system. Our databases have access control installed, but administrators will still have full access to all the data (assumption 4).

r2. 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).

r3. We assume processes are not corruptable (assumption 17).

r4. The side channel attack is described in T07 - Side channel information disclosure internal process.

T07 - 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 obtains process information.

Reference to threat tree node(s): ID_p2

Parent threat tree(s): ID_p

DFD element(s): All internal processes (7.2 - 7.13)

Remarks:

r1. The alternative spoofing attack is described in T06 - Information disclosure internal process.

r2. We assume processes are not corruptable (assumption 17).

T08 - Non-compliance of employees

Summary: The ReMeS operators don't process the customer data in compliance with legislations or policies.

Primary mis-actor: insider (operators, ...).

Basic path:

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

Consequence: The customer's personal information is shared without his knowledge. When detected, ReMeS 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 (assumption 7).

r2. A similar threat which is posed by the developer is described in T10 - Non-compliance management.

r3. A specific non-compliance threat concerning cnsents is described in T09 - Missing user consents.

T09 - Missing user consents

Summary: The system did not ask the customer's permission to share part of his (pseudonymized) personal information with 3rd parties.

Primary mis-actor: Management

Basic path:

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

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

Consequence: The customer's personal information will be shared with 3rd parties against his will.

Reference to threat tree node(s): PN_3

Parent threat tree(s): PN

DFD element(s): entire system (except 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 T08 - Non-compliance of employees and T10 - Non-compliance management.

T10 - 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 customer data is not processed or collected in accordance to (privacy) legislation.

Consequence: The customer's personal information is shared without his knowledge. When detected, ReMeS 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 T08 - Non-compliance of employees.

r3. A specific non-compliance threat concerning cnsents is described in T09 - Missing user consents.

T11 - 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.

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.

Consequence: When ReMeS processes retreive 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): 3. consumer

Remarks:

r1. This threat only applies to the consumer (assumption 10 and 11).

r2. The threat concerning inaccurate user information is described in T12 - content inaccuracy.

T12 - content inaccuracy

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 customer provides inaccurate or incomplete administrative information or fails to update old information.

Consequence: The customer himself or ReMeS processes consult the customer's inaccurate administrative information and create incorrect data.

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

Parent threat tree(s): U

DFD element(s): 3. consumer

Remarks:

r1. This threat only applies to the customer (assumption 10 and 11).

r2. The threat concerning users providing too much information is described in T11 - User unawareness.

2.4 Prioritization of threats

This section provides a list of the threats (ID + title) of the previous section. The order is based on the threat's risk (likelihood * impact). The distinction was made between high, medium, and low risk and, within each category, the threats are also ordered according to their risk. Finally, an explanation will be given of why the threats were ordered in this particular way.

2.4.1 High priority

The threat that was given the highest priority is T02 - Information disclosure of customer usage history. The main reason for this choice is the fact that is one of the more significant threats to the privacy of the customers. This threat is also very difficult to deal with. Other threats that were labeled as high priority threats include the threats about spoofing an internal user of ReMeS. Motivated attackers wishing to exploit this threat could cause ReMeS harm in name and function. This should, evidently, be avoided at all cost.

- T02 - Information disclosure of customer usage history
- T03 - Spoofing an internal user of ReMeS by falsifying credentials
- T04 - Spoofing a user of ReMeS because of weak credential storage.

2.4.2 Medium priority

The threats that were labeled as being of medium priority are placed in this category because of the fact that some form of trust has been put in the employees of ReMeS. Misuse of this trust will have serious consequences for the misactors and this should be incentive enough to mitigate the threat for these specific cases. Other than that, the medium priority threats could be mitigated further or avoided altogether without too much trouble from the ReMeS side.

- T11 - User unawareness
- T09 - Missing user consents
- T01 - Linking Alarm configuration data to user data
- T10 - Non-compliance management
- T12 - content inaccuracy

2.4.3 Low priority

Due to the fact that some level of trust is put in our employees, some threats are of a low priority. The list below contains threats that are just rather unlikely to occur because of the nature of the consequences for the misactors or the fact that the trouble that a misactor has to go through to exploit such a threat is not worth the merit of the exploit. (e.g. side channel information disclosure of internal processes).

- T08 - Non-compliance of employees
- T07 - Side channel information disclosure internal process
- T06 - Information disclosure internal process
- T05 - Linkability of requests sent to external UIS