Evaluating eHealth Scenarios for Adaptive Security in eHealth

Wolfgang Leister
Norsk Regnesentral
Oslo, Norway
wolfgang.leister@nr.no

Mohamed Hamdi
School of Communication Engineering
Tunisia
mmh@supcom.rnu.tn

Habtamu Abie
Norsk Regnesentral
Oslo, Norway
habtamu.abie@nr.no

Stefan Poslad
Queen Mary University
London, UK
stefan.poslad@qmul.ac.uk

~~Kashif Habib Sheikh~~
~~Norsk Regnesentral~~
~~Oslo, Norway~~
~~kashif.sheikh@nr.no~~

Arild Torjusen
Norsk Regnesentral
Oslo, Norway
arild.torjusen@nr.no

***Abstract*—We present a scenario and storyline that are part of a framework to evaluate adaptive security in the Internet of Things, also denoted as the IoT. The successful deployment of the IoT depends on ensuring security and privacy, which need to adapt to the processing capabilities and resource use of the IoT. We develop a scenario for the assessment and validation of context-aware adaptive security solutions for the IoT in eHealth. We first present the properties to be fulfilled by a scenario to assess the adaptive security solutions for eHealth. We then develop a home scenario for patients with chronic diseases using biomedical sensors. This scenario is then used to create a storyline for a chronic patient living at home. [tbd.: update]**

Keywords*—*Internet of Things; assessment scenarios; eHealth systems; adaptive security.

I. Introduction

Wireless Body Sensor Networks (WBSNs) improve the efficiency of eHealth applications by monitoring vital signs of a patient using low-rate communication media and constitute an important part of the Internet of Things (IoT) by bringing humans into the IoT. However, the successful deployment of the IoT depends on ensuring security and privacy, which need to adapt to the processing capabilities and resource use of the IoT. To evaluate such adaptive mechanisms we introduced evaluation scenarios specifically designed for applications in eHealth and proposed an evaluation framework [1]. This evaluation framework is extended here with a quantitative component that allows to put numbers on the quality of security solutions.

The "Adaptive Security for Smart Internet of Things in eHealth" (ASSET) project researches and develops risk-based adaptive security methods and mechanisms for IoT that will estimate and predict risk and future benefits using game theory and context awareness [2]. The security methods and mechanisms will adapt their security decisions based upon those estimates and predictions.

The main application area of ASSET is health and welfare. Health organisations may deploy IoT-based services to enhance traditional medical services and reduce delay for treatment of critical patients. A case study will evaluate the developed technologies for adaptive security using both simulation and implementation in a testbed based upon realistic cases. Blood pressure, electrocardiogram (ECG) and heart rate values will be gathered from patients and made anonymous. The sensor data will be stored in different biomedical sensor nodes that are capable of communicating with any of the following connectivity options ZigBee, Wi-Fi, 3G, GPRS, Bluetooth, and 802.15.4. For instance, a smartphone with a suitable transceiver could act as an access point between sensor nodes and a medical centre. For the evaluation in the case study, we developed a set of scenarios to assess the adaptive security models, techniques, and prototypes that will be introduced in ASSET. These scenarios describe the foreseeable interactions between the various actors and the patient monitoring system based on IoT.

In computing, a scenario is a narrative: it most commonly describes foreseeable interactions of user roles and the technical system, which usually includes computer hardware and software. A scenario has a goal, a time-frame, and scope. Alexander and Maiden [3] describe several types of scenarios, such as stories, situations (alternative worlds), simulations, story boards, sequences, and structures. Scenarios have interaction points and decision points where the technology under consideration can interact with the scenario. This means that the scenarios developed for a particular situation have to take into consideration the technologies used by the different actors. The importance of scenarios in the assessment of security solutions has been discussed in the literature [4], [5]. This work focuses on the development of scenarios that support the evaluation of adaptive security techniques for the IoT in eHealth.

[updated.] In this paper, we develop a framework for the assessment of adaptive security solutions on the basis of security and Quality of Service (QoS) requirements. In Section II the requirements and the proposed assessment framework are described including metrics that make this framework quantifiable in order to enable comparison of various situations. We define the properties that must be fulfilled by a scenario to assess adaptive security schemes for eHealth. We show the interaction between the scenarios, the threats, and the countermeasures in a global assessment framework for the ASSET project.

In Section III, we describe the extension of a previously developed generic system model, which is used for the struc-

ture of the scenarios in Section III-A with different QoS requirements, contexts and adaptive security methods and mechanisms. These scenarios, first proposed by Leister et al. [6], include a patient monitored at home, a hospital scenario, and an emergency scenario. These scenarios are reviewed and their adequacy to the evaluation of adaptive security techniques for the IoT is analysed. We propose a storyline that can support requirements analysis, as well as adaptive security design, implementation, evaluation, and testing.

Further, in Section IV, we present storylines for both the home monitoring scenario and the hospital scenario. These storylines are used in Section V to show how our framework can be applied to selected episodes of the home scenario and storyline. In Section VI we show how to use our framework in the context of adaptive security as defined by Abie and Balasingham [2]. Finally, Section VII offers concluding remarks and future prospects.

II. Adaptive Security Requirements

Designing the scenarios is of central significance for the ASSET project. They depict the operation of systems, here applied to IoT-based eHealth systems, in the form of actions and event sequences. In addition, scenarios facilitate the detection of threats and the identification of the solutions to cope with these threats. In a scenario-based assessment, a set of scenarios is developed to convey the design requirements. With regard to the specific objectives of IoT-based systems, the scenarios should capture two types of requirements:

1) *Security requirements:* Novel adaptive security and privacy mechanisms and methods are required that adapt to the dynamic context of the IoTs and changing threats to them. Thus, the scenarios should be generic enough to capture the security needs for the data processed and exchanged within a patient monitoring system. This is particularly challenging because this system encompasses multiple networking technologies, data, users, and applications, addressing varying processing capabilities and resource use.
2) *Quality of service requirements:* Unlike many traditional applications and services relying on communication networks, eHealth applications have stringent QoS requirements. Items such as the communication delay, the quality of the communication channels, and the lifetime of the self-powered sensor nodes are crucial context parameters that have significant impact on the safety of the patient. The scenarios should highlight the needs in terms of QoS requirements and illustrate the dynamic interplay between these needs and the security requirements. **[ato:tbd: Add example of how QoS and security requirements influence each other.]**

A. The ASSET Evaluation Framework

[updated.] The ASSET scenarios appear as a component of an assessment framework that will serve to improve the applicability of the security techniques proposed in the frame

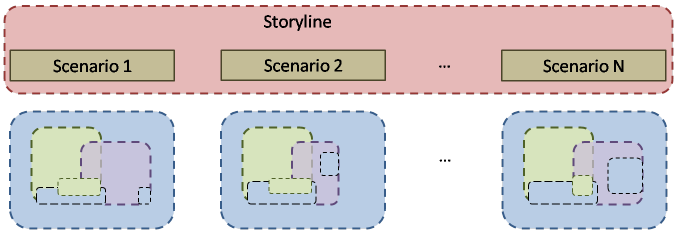


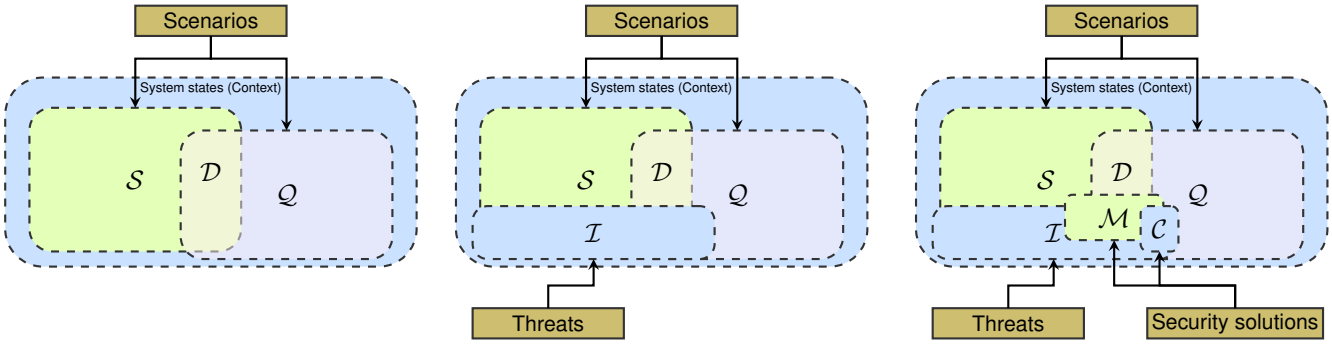
Fig. 2: Illustration of context changes during the execution of a storyline.

of the project. The other components of the assessment framework are (*i*) a set of threats describing the actions that violate the security requirements, (*ii*) a set of security solutions that mitigate the aforementioned threats, and (*iii*) a set of system states representing the dynamic context in which the patient monitoring system operates. Fig. 1 illustrates the ASSET assessment framework. The security and QoS requirements are the output of the scenario design activity. In other terms, the scenarios should give information about the set of reliable states from the security requirements, here denoted as $\mathcal{S}$, and the set of states where the QoS is acceptable, here denoted as $\mathcal{Q}$. The intersection of these sets is the set of desirable states, denoted in Fig. 1(a) by $\mathcal{D}$ (Desirable), where the security and QoS requirements are balanced.

One of the intrinsic features of the ASSET scenarios is that the sets of security requirements and QoS requirements could vary in time and space. This will make the threats and the security solutions also vary in time and space. Threats are viewed as potential events that may generate insecure system states while countermeasures are intended to thwart the effects of these threats. The realization of a threat reduces the set of secure states in the scenario of interest and affects the QoS requirements. This is represented by the region $\mathcal{I}$ (Impact) in Fig. 1(b). This region represents a set of states that will not fulfil the security or QoS requirements if a threat is realized. The countermeasures or *controls*[7] will reduce the likelihood of a threat being realized or the impact of a realized threat and hence the size of the set of potentially insecure states. Fig. 1(c) illustrates the effect of the countermeasures through the Region $\mathcal{M}$ (Mitigate). This region extends the set of secure states. Nonetheless, the countermeasures can have a negative effect on the QoS, represented by the region $\mathcal{C}$ (Cost), consisting of power, processing, memory, communication overhead, and cases where QoS requirements might not be fulfilled.

The elements of this representation will be used in the scenario based assessment of adaptive security schemes. The scenarios allow for evaluating the potential of controls to minimise the effect of threats in a given context.

For adaptive security solutions, the proposed protection techniques will vary in time and space according to the context. This is not conveyed by the scenario representation of Fig. 1. To overcome this issue, we derive a set of storylines from the ASSET scenarios. These can be viewed as a sequential application of the scenarios in a way that the selection of



(a) (b) (c)

Fig. 1: The ASSET assessment framework.

the appropriate countermeasures must take into consideration:

- *The space transition between scenarios.* Space encompasses much useful information that affect the security decision-making process. For instance, the location of the WBSN might increase/decrease its vulnerability. Moreover, mobility introduces significant challenges including horizontal and vertical handover management.
- *The time transitions between scenarios (with its implications on the context).* The time interplay between the threats and countermeasures has a substantial and dynamic impact on the environment where the patient monitoring system is deployed. The amount of energy, memory, and processing resources are crucial parameters from the QoS perspective and the security solutions have to adapt accordingly. In addition, the state of the communication channel and the proper temporal interplay in all these contexts are important in the selection of the appropriate security decisions.

Fig. 2 illustrates the evolution of the storyline and the underlying impact on the context. Of course, the sequence of scenarios forming a storyline should be consistent so that it translates a real-case situation.

B. Making the ASSET Framework Quantifiable

[new.] Assessing the qualities of a given system state can be done by means of subjective data from human assessors and by means of objective data from measurements. Our goal is to establish an estimation function that takes measured data as input and which is a preliminary to implement functionality for adaptive security. To establish such an estimation function the assessment from subjective data is used to calibrate a function that uses objective and measured data as input. Similar methodology has been used to estimate the quality of streamed video [8]. In the following we present how to assess a given system state by using human assessors.

To make the ASSET framework quantifiable we define a real function $0 \leq q(\text{system state}) \leq 1$ that shall express the degree of how well the requirements are fulfilled in the system state in question. A low value, below a given threshold, denotes that the system state in question is unacceptable, while a value close to 1 denotes that most requirements are well fulfilled.

The function q is composed of two types of inputs: *1)* security requirements that need to be fulfilled, expressed in the function q_S; *2)* degree of fulfilled QoS requirements and costs that occur due to mitigation costs for threats are expressed in the function q_Q. The function q is then composed of a product of all partial functions of $q_{i\in\{S,Q\}}$: $q = \prod_i {q_i}^{w_i}$. The weights are real numbers $0 \leq w_i < \infty$ and express the importance of a single q_i, large values indicating more importance. A weight $w_i = 1$ is considered neutral. The importance of each parameter is defined by the assessor according to the nature of the requirement before assessing the q_i values.

The above definition has the disadvantage that the resulting q is sensitive to the number k of factors q_i that are used to define it. To mitigate this we propose to replace the weights by $v_i = \frac{w_i}{\sum_{j=1}^{k} w_j}$ resulting in $\hat{q}_i = {q_i}^{\frac{w_i}{\sum_{j=1}^{k} w_j}}$. Thus, the value q is expressed by:

$$q = \prod_i \hat{q}_i = \prod_i {q_i}^{\frac{w_i}{\sum_{j=1}^{k} w_j}} \tag{1}$$

1) Security Requirements: Define $\mathcal{G}_\mathcal{S} = (\mathcal{S} \setminus \mathcal{I}) \cup \mathcal{M}$ as a set where all security requirements are fulfilled or threats mitigated. For security requirements j outside $\mathcal{G}_\mathcal{S}$ we define a deviation from the ideal requirements and a normalised distance $d_{S_j} : 0 \leq d_{S_j} \leq 1$ according to a suitable metric to denote how far the current requirement is from ideal fulfilment. We set $d_{S_j} = 1$ when deviations cannot be tolerated. Thus, we define the following function:

$$q_{S_j} = \begin{cases} 1 & \text{if requirement } \in \mathcal{G}_\mathcal{S} \\ 1 - d_{S_j} & \text{if requirement } \notin \mathcal{G}_\mathcal{S} \\ 0 & \text{if deviation intolerable} \end{cases}$$

2) QoS Requirements: Define $\mathcal{G}_\mathcal{Q} = \mathcal{Q} \setminus \mathcal{C}$ as a set where all QoS requirements are fulfilled and possible effects from the mitigation are tolerable. For QoS requirements j outside $\mathcal{G}_\mathcal{Q}$ we define a deviation from the ideal requirements and a normalised distance $d_{Q_j} : 0 \leq d_{Q_j} \leq 1$ according to a suitable metric to denote how far the current requirement is from ideal

fulfilment. We set $d_{Q_j} = 1$ when QoS requirements are not fulfilled (cf. availability) or costs cannot be tolerated. Thus, we define the following function:

$$q_{Q_j} = \begin{cases} 1 & \text{if requirement } \in \mathcal{G}_\mathcal{Q} \\ 1 - d_{Q_j} & \text{if requirement } \notin \mathcal{G}_\mathcal{Q} \\ 0 & \text{if QoS properties intolerable} \end{cases}$$

3) Mitigation Costs: Besides the effect on QoS there might be other costs implied by mitigation, e.g., real costs in payroll or material, changes to the environment, costs for the patient, virtual costs for lower Quality of Experience, and so on. Unacceptable costs are included in the area $\mathcal{C}$. For costs outside $\mathcal{C}$ we define relative costs on a normalised scale $d_C : 0 \leq d_C \leq 1$. We define the following function:

$$q_C = \begin{cases} 1 & \text{if costs neglectable} \\ 1 - d_C & \text{if costs } \notin \mathcal{C} \\ 0 & \text{if costs } \in \mathcal{C} \end{cases}$$

C. Assessment to define the q_i values

To aid human assessors in assessing the values for q_i (i.e. the value indicating how far a given requirement is from the ideal fulfilment) we propose to base the assessment on a set of questions based on a Likert scale [9]. A Likert scale is a psychometric scale commonly involved in research that employs questionnaires where the questions are to be answered from *best* to *worst* on a scale of n steps, where n is an odd integer number.

If the questionnaire to be filled out by an assessor is designed so that each q_i corresponds to one question on a Likert scale we propose to use a function e that takes the response $\tilde{q}_i \in \mathbb{N}$ for $0 \leq \tilde{q}_i \leq n-1$ as an argument. We use two approaches to express the q_i.

1) Linear Approach:

$$q_i = e_\alpha(\tilde{q}_i) = \frac{\tilde{q}_i}{n-1} \tag{2}$$

2) Logarithmic Approach:

$$q_i = e_\beta(\tilde{q}_i) = \log_n(\tilde{q}_i + 1) \tag{3}$$

Using the logarithmic approach leaves less impact of bad values than the linear approach. There are some caveats on using a logarithmic function for values on a Likert scale, as noted by Nevill and Lane [10]. Particularly, the values on the Likert scale should express a continuous and rather equidistant increase of quality.

3) Other Methods: In case the questionnaires are designed in a way that several independent questions result in one value for q_i, Bayesian networks developed by Perl and Russell [11] can be employed. However, we consider the design of the questionnaires and the use of Bayesian networks as future work. Note also that for Bayesian networks more data from an assessment are necessary than for the above mentioned methods.

While the Likert scale is useful for assessing opinions on a psychometric scale, i.e., subjective data, we need, as well, be able to assess objective data. In these cases, we set up a scale where discrete choices on a questionnaire are mapped to a similar scale as the Likert scale to reflect the quantity of data based on an objective value. This type of creating assessment data is quite common for assessments, such as in the estimation of the quality of software products in the OpenBRR [12].

When objective data are used as input, e.g., as the result of measurements, these data on a continuous scale can be mapped into the value range $0 \leq q_i \leq 1$ and used in Eq. 1. Note, however, that the mapping function not necessarily ought to be linear, and a specific assessment phase may be necessary to develop a suitable function that maps the values into the value range $0 \leq q_i \leq 1$.

4) Assessment by Subject Panels: For an assessment often several individuals are put into an assessment panel. These subjects perform the assessment individually while the results are put together into one assessment result. Further work needs to show whether it is more practicable to calculate individual q values and then calculate some mean value of these or whether to calculate mean values for each $\tilde{q}_i$.

D. Finding Useful Thresholds

[tbd.]

III. Extended Generic Model for eHealth Scenarios

In the following sections, we develop the scenarios of the ASSET project and show how storylines can be extracted. We also underline the role of the storyline in the assessment of adaptive security techniques for eHealth. Before delving into the details of scenario and storyline engineering, we highlight the major properties that a scenario should have in order to be useful for adaptive security.

Patient monitoring systems are a major data source in healthcare environments. During the last decade, the development of pervasive computing architectures based on the IoT has consistently improved the efficiency of such monitoring systems thereby introducing new use cases and requirements. It is important that these monitoring systems maintain a certain level of availability, QoS, and that they are secure and protect the privacy of the patient. Previously, we have analysed the security and privacy for patient monitoring systems with an emphasis on wireless sensor networks [13] and suggested a framework for providing privacy, security, adaptation, and QoS in patient monitoring systems [14]. We divided patient monitoring systems into four Generic Levels (GLs): (0) the patient; (I) the personal sensor network; (II) devices in the closer environment following several scenarios; and (III) the healthcare information system.

In this work, we extend the generic model presented by Leister et al. [14] by the definition of three new levels related to the monitoring of chronic diseases, the communication between multiple healthcare providers, and the communication between healthcare providers and medical research institutions, respectively. Consequently, the extended generic model is composed of five levels numbered from (0) to (IV)

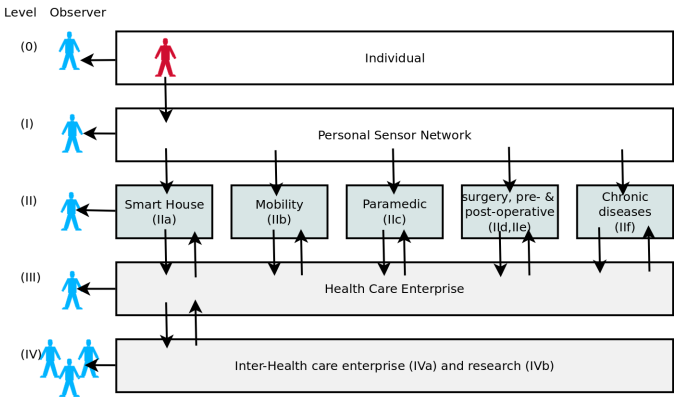


Fig. 3: Generic eHealth framework indicating the use cases in five levels (Extended from [13]).

depending on the logical distance to the patient to whom Level (0) is assigned. Multiple types are considered at Level (II). Note that only one of these types applies at a time. However, it must be possible to switch between the types in Level (II) depending on the activity of the patient. To this purpose, the communication between Levels (II) and (III) is two-way. The key levels of our extended generic model are as follows, as shown in Fig. 3:

(0) **Patient.** This is the actual patient.

(I) **Personal sensor network.** The personal sensor network denotes the patient and the sensors measuring the medical data. These sensors are connected to each other in a WBSN. While this sensor network can be connected randomly, in most cases one special WBSN node is appointed to be a Personal Cluster Head (PCH), which forwards the collected data outside the range of the WBSN.

(IIa) **Smart home.** The patient is in a smart-home environment where the personal sensor network interacts with various networks and applications within this environment. The smart home infrastructure might be connected to a healthcare enterprise infrastructure using long-distance data communication.

(IIb) **Mobility.** The patient is mobile, e.g., using public or personal transportation facilities. The personal sensor network of the patient is connected to the infrastructure of a healthcare enterprise via a mobile device, e.g., a mobile Internet connection.

(IIc) **Paramedic.** The WBSN is connected to the medical devices of an ambulance (car, plane, and helicopter) via the PCH. The devices of the ambulance can work autonomously, showing the patient status locally. Alternatively, the devices of the ambulance can communicate with an external healthcare infrastructure, e.g., at a hospital.

(IId) **Intensive care/surgery.** During an operation the sensor data are transferred to the PCH or directly to the hospital infrastructure over a relatively short distance. The sensors are in a very controlled environment, but some sensors might be very resource limited due to their size, so extra transport nodes close to the sensors might be needed.

(IIe) **Pre- and postoperative.** During pre- and postoperative phases of a treatment, and for use in hospital bedrooms, the sensor data are transferred from the sensor network to the PCH and then to the healthcare information system.

(IIf) **Chronic disease treatment.** The WBSN data are used by healthcare personnel in non-emergency treatment of individual patients with a chronic disease.

(III) **Healthcare information system.** This is considered a trusted environment. It consists of the hospital network, the computing facilities, databases, and access terminals in the hospital.

(IVa) **Inter-healthcare provider.** Information is shared between different healthcare providers concerning medical information of an individual patient.

(IVb) **Healthcare provider and research.** Information is shared between healthcare providers and medical research organisations for the purposes of research, new solutions development, etc.

A. *The Structure of the Scenarios*

Through the potential interactions between these levels, notice that the model can support the elaboration of multiple scenarios where the actors interact by switching from a level to another. The scenarios in healthcare using biomedical sensor networks are quite complex. Therefore, they need to be efficiently structured. We consider three main scenarios (hereafter denoted as *overall scenarios*) and we decompose them into sub-scenarios (hereafter denoted as *core scenarios*). A particular interest is given to the transitions between the core scenarios since these transitions constitute substantial sources of threats. For ASSET, we consider a home scenario (A) shown in Fig. 4, a hospital scenario (B) shown in Fig. 6, as well as an emergency scenario (C).

Each of these overall scenarios contain a set of core scenarios which are denoted by the scenario identifier A, B, or C, followed by a dash and the core scenario numbering in roman number minuscules. The transitions between these core scenarios model the interaction between the various components of the patient monitoring system. In this paper, we focus mostly on the Home Scenario (A) where the patient is supposed to be monitored outside the hospital while performing normal daily actions. However, to extract useful technical cases for the evaluation phase we need to structure the scenario according to the patient's actions and situation.

TABLE I shows a list of core scenarios used in our work, which overall scenario they belong to, and which transitions are useful. Note that other transitions are theoretically possible, but these are either unlikely or can be achieved by combining a series of transitions, e.g., taking the Core Scenario iii as an intermediate for Overall Scenario A. Omitting unlikely transitions helps to reduce the number of states when modelling

TABLE I: Overview of core scenarios. • indicates that this core scenario is included in the overall scenario. ○ indicates that this core scenario is related to the overall scenario.

core scenario & name		scenario A	B	C	transition to core scenario
i	home monitoring	•			iii, xv
ii	home diabetes	•			i, iii
iii	moving	•			i, iv, v, ix, vii, vi
iv	public transport	•			iii
v	vehicle transport	•		○	iii
vi	shop	•			iii
vii	café	•			iii
viii	doctor's office	•			iii, xv
ix	waiting room	•	•		viii, x, iii
x	diagnosis		•	•	xi, xii, xiii, iii
xi	operation		•		xii
xii	intensive care		•		xiii
xiii	observation		•		iii, xii, x
xiv	accident			•	xv
xv	ambulance	○	○	•	x

the scenarios.

B. The Structure of the Home Scenario

The Home Scenario (A) envisages that a monitored patient can be in various contexts performing normal daily actions. For example, for a patient with diabetes the following situations apply:

- The patient is at home or a nursing home using monitoring equipment.
- The patient uses sensors and communicates electronically with the doctor's office.
- The patient uses specific monitoring equipment for diabetes.
- The patient visits the doctor's office regularly and uses public transport or a car to get there.
- At the waiting room the patient can communicate data to the health care infrastructure of the doctor's office.
- The patient regularly takes walking or jogging trips.
- The patient regularly visits a café with friends; this includes walking or commuting with public transport.
- In case of an emergency or planned surgery, the patient may be sent to a hospital with an ambulance.

This list of situations is not yet a useful narrative. It needs to be structured and enriched with the specific context information, such as the necessary devices of the IoT, the communication channels, and actions of the involved actors. This is done in the core scenarios that describe a specific part of an overall scenario; e.g., a situation a patient experiences. Each core scenarios can be part of several overall scenarios.

1) Home Situation (monitored at home) (A-i): Biomedical sensors are employed in an environment where the patient is at home or in a nursing home. The patient is monitored by a WBSN, and the sensor data and alarms can be transmitted to medical centres and emergency dispatch units.

Here, the sensors might not be monitoring or transmitting the physiological patient data continuously in order to reduce

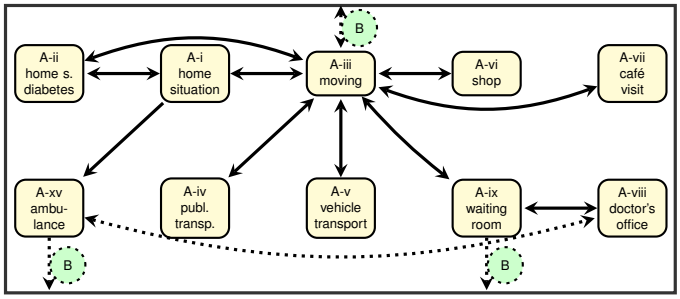


Fig. 4: The Home Scenario with the underlying core scenarios and their transitions.

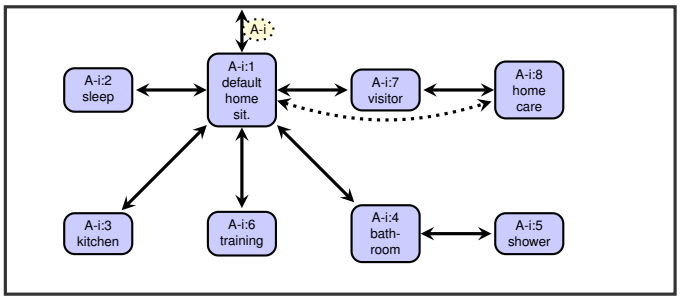


Fig. 5: The detail-scenarios of the home-situation.

battery power consumption. Depending on a predefined algorithm, abnormal sensor data from certain sensors may be used to activate other sensors autonomously before an alarm is triggered, and sent to a central monitoring unit. In this scenario, the following characteristics are given:

1) Ease of use and non-intrusiveness are important issues.
2) Very low power consumption, enabling a long life span of the batteries, is required.
3) A network infrastructure is available, such as access to the Internet via LAN, WLAN, or mobile networks.
4) Limited mobility, handoff is possible, but infrequent.

Core Scenario A-i could be split up into several sub-scenarios, if necessary, depending on the patient's activities, time of the day, etc. These sub-scenarios may include sleeping, watching TV, kitchen work, or other household activities.

We created a specialised scenario for patients living at home with diabetes monitoring (A-ii). The patient uses a smartphone with a health-diary software that also implements personal health records (PHR) and stores measurements. The measurements are performed using special devices that communicate with a smartphone using Bluetooth. **[does not fit:]** ~~Note that such specialisations also could be described as a part of the storyline of a separate core scenario.~~

On a regular basis, the patient transmits measurements to the doctor's office, thus synchronising the PHR with the hospital information system; the patient also has an audio-/video-conversation where medical questions are discussed. During these sessions the patient might take pictures with the smart phone camera or perform other measurements.

2) Moving (Walking and Jogging) Scenario (A-iii): The patient does daily training, i.e., jogs in the nearby park, or does shorter walks from the home to the public transport, to the café, shop, or doctor's office. A common feature in these situations is that the patient needs to use a smartphone as a device that collects sensor data, using the mobile networks to transmit the data. When walking or jogging in the park many other people and their devices might interfere with the communication of the smartphone.

When walking in the woods, there might be several spots which are not covered by a mobile network. In this case, the signal is so weak that only emergency calls from another provider can be done. While data traffic is not possible, SMS messages can be used to send data with very low bandwidth, possibly after several retries. For an average walking trip, this outage may last for some minutes.

3) Transport Scenarios: Core Scenario A-iv presents a situation where a patient commutes to a doctor's office or to a café using public transport. Here, the patient needs to use a smartphone as a device that collects sensor data, using the mobile networks to transmit the data. Blind spots without connectivity to a mobile network, roaming, varying data transmission quality, etc., are parts of this scenario. This scenario can be applied to long-distance trains, planes, etc.

Core Scenario A-v represents the scenario where a patient uses his own or another's (private) car to commute to a shop, a café, or the doctor's office. Here, the patient needs to use a smartphone as a device that collects sensor data, using the mobile networks or networks installed or used in the car to transmit the data. Blind spots without connectivity to a mobile network, roaming, varying data transmission quality, etc., are parts of this scenario.

4) Café Scenario (A-vii): The patient visits a café. Here, the patient needs to use a smartphone as a device that collects sensor data, using mobile networks or café's WLAN zone for data transfer. Switching between the WLAN and mobile networks may occur, the WLAN might be of varying quality, many other café visitors may interfere, or the WLAN might not actually be connected to the Internet.

5) Doctor's Office Scenario (A-viii): The patient is in the doctor's office, usually after some time in a waiting room (A-ix). Here, the patient can have extra sensors attached. These extra sensors, as well as the existing sensors, can communicate with the doctor's infrastructure either through the smartphone of the patient, or directly, depending on the needs. A doctor can change a sensor's characteristics, which requires the possibility to re-program the sensor devices.

6) Waiting Room Scenario (A-ix): The patient is in a waiting room at a doctor's office or a hospital. Patients that are known to the healthcare system can be connected from their smartphone to the healthcare network; here, specific actions for collecting data from the device or other preparations can be performed. Once the patient is in the range of the waiting room, the smartphone can transfer large amounts of stored patient data directly to the infrastructure of the medical centre via short-range communication, instead of using long-range mobile communication.

7) Other scenarios: In the scenario structure we foresee that the patient can undergo a transition to other core scenarios in a different overall scenario in order to cover situations that else would be outside the scenario structure. For instance, a patient could get ill and be brought to a hospital in an ambulance (B-xv) or an emergency situation happens (Scenario C). Note that the use of devices in the IoT could be different in Scenarios A, B, and C: as an example, in an emergency situation the use of one of the patient's own sensors would not be possible in all cases.

C. The Structure of the Hospital Scenario

In Scenario B the biomedical sensors are used in a hospital environment. Here, the patient is located in an operating room (OR) or intensive care unit (ICU) while undergoing intensive monitoring of vital physiological parameters. Additional sensors might be required during this procedure to monitor other physiological parameters. The patient may be moved between different rooms during the treatment, e.g., from the OR to the ICU, but monitoring must continue uninfluenced by this. The sensor data may need to be transferred over different wireless networks. The system should be able to cope with breakdown in sensor nodes, new software updates, wireless network traffic congestion, and interferences with other wireless networks and biomedical devices.

In Scenario B a fixed network infrastructure is available between Levels (II) and (III) which can be accessed by the sink nodes of the biomedical sensor network. The scenario includes a complex communication environment. Interference from co-existing wireless networks, mobile networks, and various medical facilities is possible; this may reduce the performance of the transmission. While the network topology in this scenario is fixed, changes to the network topology may happen while patients are moving or being moved from one place to another, possibly causing handoffs to other gateways. On the other hand, roaming to other networks is not part of this scenario in order to stay within the hospital domain.

Note that scenarios that seem to be similar in Scenario B and in Scenario A might have differences that might not be obvious. Thus, one cannot use reasoning performed in one scenario in another uncritically, without checking the context and other conditions. For instance, A-viii (doctor's office) could be different from a rather similar situation in a hospital (B-x) since the hospital is connected to a different kind of network infrastructure. Usually, the primary healthcare points (doctor's office) and hospitals have different security requirements and regimes.

1) Hospital Diagnosis Scenario (B-x): The patient is examined; extra sensors are attached, and existing sensors on the patient might be accessed both directly and via the patient's smartphone. In addition, NFC tags are used to identify objects. The medical personnel can re-configure and re-program the sensors during diagnosis.

2) Hospital Operation Scenario (B-xi): The patient is under surgery; extra sensors are attached, and existing sensors on

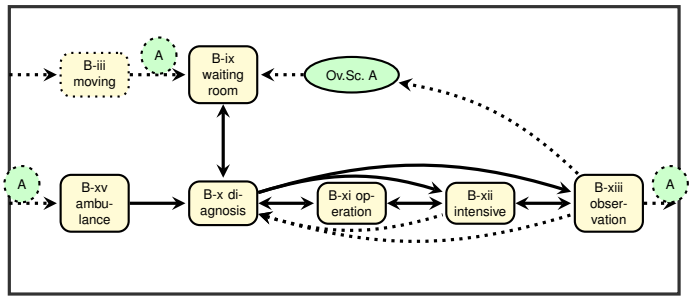


Fig. 6: The Hospital Scenario with the underlying core scenarios and their transitions.

the patient are accessed directly by the hospital system rather than through the smartphone of the patient. In this scenario, the QoS is set very high, while security-wise the sensors are in a protected zone. The medical personnel can re-program the sensors during the operation.

3) Hospital Intensive Care Scenario (B-xii): The patient is in intensive care after an operation. Extra sensors are attached, and existing sensors on the patient might be accessed both through the patient's smartphone, and directly through the hospital infrastructure. In addition, NFC tags are used to identify objects. In most cases, the smartphone will be used as PCH. The medical personnel can re-program the sensors during intensive care.

4) Hospital Observation Scenario (B-xiii): The patient is in a room under "normal" observation; in contrast to the home situation, the patient's smartphone has direct access to the hospital systems and will deliver data directly with higher QoS through the secured hospital systems.

D. The Structure of the Emergency Scenario

The Emergency Scenario (C) presents an emergency situation where victims are provided with sensors, patients are transported with an ambulance (car, helicopter, plane) and delivered to the emergency reception at a hospital. In Scenario C the use of sensors is not planned beforehand, health personnel must improvise, the identity of the patient might be unknown, and the infrastructure might be partially unavailable. Despite of this, the expectation is that severely injured patients are stabilised and survive the transport to the emergency reception in the best condition possible.

We include the first scenario of the Hospital Scenario, the diagnosis phase when the patient arrives in Core Scenario C-x. Here, the rather unplanned interventions at the emergency site are adapted to the routines at the hospital.

1) Accident Site Scenario (C-xiv): This scenario is a disaster and accident response scenario where biomedical sensors are deployed to measure values like blood pressure, temperature, pulse and ECG in an ad-hoc network at the site of an accident. Wired or wireless communications infrastructures may be damaged or unavailable, and a large number of severely injured people might overwhelm the emergency field personnel. This could prevent them from providing efficient and effective emergency rescue. Biomedical sensor networks can be quickly deployed to monitor vital signs. A large number of injured can be monitored simultaneously.

In this scenario, the following characteristics are given:

1) The sensor network must operate autonomously, and needs a high degree of self-organisation. The network topology is highly dynamic. Therefore, the sensor nodes should be able to discover each other and setup a sensor network autonomously.
2) A fixed network infrastructure is not available; data transferred from Level (II) to Level (III) must use a mobile network or other specific wireless network, such as microwave, or digital trunk communication.
3) The radio link might be unstable and the radio link quality might vary. Additionally, the communication environment is rather complex, since many sensor nodes may be deployed in a small area, possibly causing severe channel competition.
4) High degree of mobility. Handoffs are possible and might be frequent.
5) Blue-light functionality. That is, being able to re-use sensors on short notice with high flexibility (short-cutting some of the usual procedures).

2) Ambulance Scenario (C-xv): The patient is in an ambulance. The sensors on the patient are connected to the ambulance's information system, which is connected to a hospital infrastructure via a mobile network connection. The communication between the patient's sensors is either directly to the ambulance infrastructure, or via the mobile phone. The ambulance and the patient's mobile phone might use different carriers. Some properties in this scenario are common with Scenario v (vehicle transport).

Note that once the patient is inside the ambulance, sensors should communicate with devices in the ambulance without involving the mobile carrier.

IV. Storylines for the Scenarios

The set of overall scenarios, core scenarios, and transitions can be used to create *storylines* that can be used as case studies in ASSET. We present the storylines developed for the Scenarios A and B. Parts of these storylines will be used in the following analysis to evaluate the diverse functions in the IoT. We have not yet developed a storyline for Scenario C.

A. Storyline for the Home Scenario

We developed the storyline for the home scenario as follows: Petra has both a heart condition and diabetes. In a hospital, she had two sensors placed in her body: one heart sensor and one blood sugar sensor. In addition, she uses external sensors to measure blood pressure, heart beat, inertial sensors, etc., as well as a camera. Petra is living in her home that has been prepared for the monitoring system and is commissioned with the necessary data connections so that her vital signs can be periodically reported to the healthcare personnel in levels (II) (nurse or doctor) or (III) (patient records) as introduced in Fig. 3; several technologies can be applied to achieve this.

The patient monitoring system is set up so that the sensor data are transmitted wirelessly (several transmission technologies are possible) to a smartphone that acts as PCH. The PCH communicates with the hospital infrastructure (Level (III)).

1. Petra is now being monitored at home but data is acquired remotely (A-i); the following requirements are important:
   a. Petra wants her data to remain confidential from neighbours, i.e., people close-by, but outside her home;
   b. Petra wants her data to remain confidential from visitors, i.e., people inside her home.
2. Petra takes a bath in her home (planned sensor acquisition disruption; A-i);
   a. the sensors are water-proof; the PCH is close enough to receive signals;
   b. the sensors need to be removed;
      i. a change in the values implicitly indicates the sensor removal; or
      ii. patient must notify the PCH about the sensors going off-line;
3. Petra is sleeping and sensors fall off (unplanned sensor acquisition disruption; A-i).
4. Petra leaves her home for training outdoors or a stroll in the park nearby (A-iii);
   a. she is walking alone with her sensors communicating to the PCH;
   b. she meets an acquaintance, Linda who has similar sensor equipment; note that Petra's sensors could communicate through Linda's sensor network; they continue walking together;
   c. when they walk further, Petra looses the communication channel to the health care institution because of the terrain; should she connect through the open, mobile WLAN-zones that are offered or should she use Linda's PCH as communication channel?
5. Petra leaves her home to visit her friends in a café (A-vii, A-iii, A-iv, A-v).
6. Petra visits her regular doctor for a check-up; the doctor's office is in walking distance from her home (A-iii, A-viii, A-ix).
7. Petra becomes ill and is transported by an emergency ambulance to the hospital (B-xv); transition to the Overall Hospital Scenario B.

B. Storyline for the Hospital Scenario

We developed the storyline for the hospital scenario as follows: Petra has both a heart condition and diabetes. One year ago, she had two sensors placed in her body: one heart sensor and one blood sugar sensor that both communicate wirelessly. In addition, she uses external sensors to measure blood pressure, heart beat, inertial sensors, etc., as well as a camera. Petra suddenly gets ill while being at home. This is detected by the patient monitoring system installed at her home.

1. Petra is taken in an ambulance to the hospital (B-xv). In addition to the sensors she is using, the paramedics use EEG and ECG sensors. The information from all sensors is available in the ambulance from three possible sources:
   a. information received directly from the sensors, available on the displays in the ambulance;
   b. information received from the PCH that Petra is using;
   c. information received from the healthcare records.
2. After the ambulance arrives at the hospital, Petra is moved to a room where diagnosis of her condition is performed (B-x). Different sensors are used to find out her condition. These sensors are removed after diagnosis.
3. It becomes clear that Petra needs to undergo surgery (B-xi). During surgery sensors are used to measure certain biomedical values. However, the medical procedure also creates electromagnetic noise in the same band as the data transmission between sensors is ongoing.
4. After the surgery, Petra is moved to intensive care (B-xii) where a variety of sensors are used to observe her biomedical values.
5. After two days, Petra is moved to a recovery room with three other patients to allow time for her surgery wound to heal and for observation (B-xiii). In addition to the heart and blood sugar sensors, two additional sensors are now used, but these will be removed after the observation phase is over. The two other patients in the same room are using the same kind of sensors.
   a. The sensors Petra is using transmit their readings to her PCH.
   b. The additional sensors Petra is using transmit their readings to a base station in the patients' room, while her ordinary sensors are reporting to her PCH.
6. Petra is discharged from hospital; transition to Overall Scenario A.

C. Applying the Storylines

[tbd. – note: needs to be adjusted in the light of new research presented in this paper.] To conduct an efficient threat analysis of these storylines, we apply security objectives introduced by Savola and Abie [15] and Savola et al. [16], who stated that adaptive security decision-making should adapt requirements for privacy and data confidentiality based on the data processing needs, roles of stakeholders, regulations and legislation, and the privacy level of data indicated by privacy metrics. For example, the security requirement pointed out in Step 1.a of the storyline is related to confidentiality and privacy, which are often emphasised in healthcare. Strong confidentiality algorithms, key distribution, associated processes, and compliance to appropriate privacy legislation and regulations are crucial.

V. Evaluating the Home Scenario

[new.] We use selected parts of Scenario A to illustrate with some examples how to use the ASSET framework. We go through the scenario description, and comment on the use of the framework. Note, however, that the numerical values are for illustration purposes. These values are based on rough

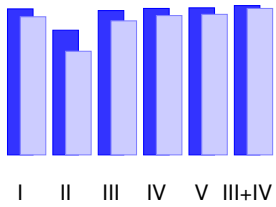


Fig. 7: Visualising the result for confidentiality and observability. The dark blue bars represent the results using the logarithmic function e_β while the light blue bars represent the results using the linear function e_α.

estimates instead of a careful assessment. Different methods for assessment were proposed above in Section II-C, but applying and evaluating the different methods reamin future work.

A. Confidentiality and Observability

In the storyline of the Home Scenario Petra is monitored at home with the requirement that she wants her data to be confidential for people inside and outside her home. Let us assume that the properties of data observability and data confidentiality are essential in this first case, i.e., are in $\mathcal{S}$.

Here, data observability means that a third party can observe the signal sent from a device and, thus, deduct the existence of this device and some meta-data. For instance, neighbours of Petra might observe the signals from her sensors and make assumptions about her health conditions from this. As countermeasures the apartment could be shielded or the signal strength of the sensors could be reduced. While shielding the apartment is too expensive, reducing the signal strength, however, could have an impact on the data availability since some corners in Petra's apartment wound not be covered.

Data confidentiality means that a third party cannot interpret the received signals. Cryptographic methods and authentication are often used to assure data confidentiality. Countermeasures when threats occur could be the use of a different cryptographic method or authentication protocol. However, using a different cryptographic method could have a negative impact on the performance or battery consumption.

For a numeric example we use the following variables: q_{S_1} is the value for observability inside the apartment; q_{S_2} is the value for observability outside the apartment; q_{S_3} is the value for confidentiality; q_{S_4} is the value for availability; q_{Q_1} is the value for bandwidth; q_{Q_2} is the value for battery consumption; and q_C are other mitigation costs. recall that the value of q_i indicates how far a given requirement is from the ideal fulfilment, where 1 is complete fulfilment of the requirement. We use the following cases: *I*) the base case, i.e., the apartment is not shielded, rather simple encryption algorithms and authentication protocols are used, and sensors transmit at normal power; *II*) shielding the apartment; *III*) reducing transmission power; *IV*) using different encryption algorithm; and *V*) using different authentication protocol.

As outlined in in Section II-B, for objective assessment we need to establish a scale using n steps similarly to the Likert scale. For an example, we present a possible scale for the requirement $\tilde{q}_{S_2}$ (observability outside apartment) on a scale with 11 values in TABLE III. The value of $\tilde{q}_{S_2} = 0$ is marked as not applicable to indicate that for observability outside the appartment no situation is considered totally inacceptable. Note that marking $\tilde{q}_{S_2} = 0$ implies $q = 0$ for this alternative.

TABLE III: The 11-value scale for $\tilde{q}_{S_2}$ of Example 1

$\tilde{q}_{S_2}$	Description
10	not observable outside apartment
9	barely observable in adjacent apartments; cannot be interpreted
8	barely observable in adjacent apartments; need advanced equipment to interpret
7	observable in parts of adjacent apartments, but not beyond
6	well observable in adjacent apartments, but not beyond
5	observable in range $>$ 30m; on street
4	observable in range $>$ 50m on street
3	observable in range $>$ 100m on street
2	observable on street from running car
1	observable through wide-range network
0	n/a

In an experiment, we assessed the values for $\tilde{q}_{S_{i=1\ldots4}}$, $\tilde{q}_{Q_{i=1\ldots2}}$, and $\tilde{q}_{Q_C}$ by using a rough estimate. We also assigned values for the weights w_i using intuition; we are aware that these values need to be assessed more thoroughly at a later stage. The assessment values, weights, and results for $\hat{q}_i$ and q_{total} are shown in TABLE II for the logarithmic approach from Eq. 3. We also applied the linear approach from Eq. 2 to the same data. Both results for q_{total} are visualised in Fig. 7.

In our example we see that the logarithmic approach and the linear approach show similar behaviour with respect to ranking the alternatives. However, the logarithmic approach results in higher values and less differences the values in-between. In this particular example, a combination of cases IV and V gives the best result while case II delivers the lowest result, which is reasonable.

B. Assessment of Changes in Time

As a second example we use the part of the storyline where Petra is taking a stroll in the park. We assume that her sensors are connected wirelessly to her smartphone in its function as a PCH, and the PCH is communicating through a wireless network with the health care infrastructure through a public wireless network offered by a telephony provider. Further, we assume that her smartphone can connect using WLAN.

In this example, we use different definitions for q_{S_1} and q_{S_1} by using the observability of the sensors and the PCH, respectively. We take into account effects for long-range networks that indicate that battery consumption is higher when the signal strength from the base station is weak or the connection is lost.

For a numeric example we use the following variables: q_{S_1} is the value for observability of the sensors; q_{S_2} is the value for observability of the PCH; q_{S_3} is the value for confidentiality; q_{S_4} is the value for availability; q_{Q_1} is the value for bandwidth; q_{Q_2} is the value for battery consumption; and q_C are other mitigation costs. We use the following cases from the storyline of Scenario A: *I*) walking alone in the park; *II*) meeting Linda;

TABLE II: Example for applying the ASSET framework using the logarithmic approach from Eq. 3

	S_1		S_2		S_3		S_4		Q_1		Q_2		C		q_{total}
w_i	0.4		0.8		2.0		1.0		1.0		1.5		1.0		$\sum = 7.4$
	$\tilde{q}$	$\hat{q}$	$\tilde{q}$	$\hat{q}$	$\tilde{q}$	$\hat{q}$	$\tilde{q}$	$\hat{q}$	$\tilde{q}$	$\hat{q}$	$\tilde{q}$	$\hat{q}$	$\tilde{q}$	$\hat{q}$	q_{total}
Case I	6	0.997	8	0.991	8	0.977	10	1.000	10	1.000	10	1.000	10	1.000	0.965
Case II	6	0.997	10	1.000	8	0.977	10	1.000	10	1.000	10	1.000	1	0.846	0.824
Case III	7	0.998	9	0.996	8	0.977	9	0.995	8	0.988	10	1.000	10	1.000	0.954
Case IV	6	0.997	8	0.991	10	1.000	10	1.000	8	0.988	9	0.992	10	1.000	0.968
Case V	6	0.997	8	0.991	9	0.989	10	1.000	9	0.995	10	1.000	10	1.000	0.972
Case III+IV	6	0.997	9	0.996	10	1.000	10	1.000	9	0.995	10	1.000	10	1.000	0.987

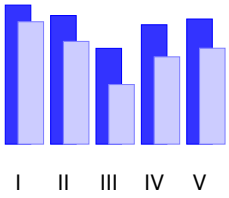


Fig. 8: Visualising the result for Example 2. The dark blue bars represent the results using the logarithmic function e_β while the light blue bars represent the results using the linear function e_α.

TABLE IV: Example 2 for applying the ASSET framework using the logarithmic approach from Eq. 3

q_i	S_1	S_2	S_3	S_4	Q_1	Q_2	C	q_{total}
w_i	1	1	2	1	1	1.5	1	$\sum = 8.4$
Case I	7	6	8	9	8	9	10	0.919
Case II	7	6	4	9	8	9	9	0.850
Case III	7	5	4	1	1	8	9	0.633
Case IV	7	5	3	9	7	7	8	0.789
Case V	7	6	4	9	6	8	8	0.827

III) loosing connection; *IV*) connect to open, mobile WLAN; and *V*) using Linda's PCH as communication channel.

In an experiment, as above, we assessed the values for $\tilde{q}_{S_{i=1\ldots4}}$, $\tilde{q}_{Q_{i=1\ldots2}}$, and $\tilde{q}_C$ by using a rough estimate and assigned values for the weights w_i using intuition. The assessment values $\tilde{q}_i$, weights, and q_{total} are shown in TABLE IV for the logarithmic approach from Eq. 3. We also applied the linear approach from Eq. 2 to the same data. Both results for q_{total} are visualised in Fig. 8.

In this example we see how the security situation changes due to changes of the context (I–II–III), i.e., when Petra meets Linda or Petra looses connection. This example also shows that the assessment can give a hint which one of two possible actions (IV or V) would promise a better security situation.

VI. Applying the Framework to Adaptive Security

[new.] Abie and Balasingham [2] define the term *adaptive security* as "*a security solution that learns, and adapts to changing environment dynamically, and anticipates unknown threats without sacrificing too much of the efficiency, flexibility, reliability, and security of the IoT system*". Abie and Balasingham present the *Adaptive Risk MAnagement* (ARM) framework that is based on a feedback loop known from cybernetics [17] with the five measures (*i*) identify, (*ii*) analyse, (*iii*) plan, (*iv*) track, and (*v*) control. This results in four steps in the adaptation loop, aligned to ISO/IEC 27005:2008 [7] and the *Plan–Do–Check–Act* (PDCA) model of ISO/IEC 27001:2005 [18].

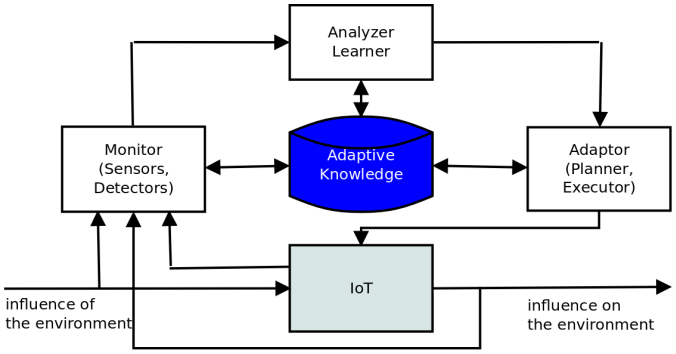


Fig. 9: The Adaptive Security concept, adapted for the IoT by Abie [19].

Abie [19] presented a functional description on the concept of adaptive security for a message-oriented infrastructure; he adapted this concept to the IoT, as shown in Fig. 9, and identified the following functionality to be essential for adaptive security to be implemented: *a*) being self-aware using a feedback loop and a history database; *b*) being context-aware using sensors and feedback from other nodes in the IoT; *c*) using security metrics to process the data from the sensors and the other nodes; *d*) using risk and threat estimation and prediction; *e*) using security metrics as defined by Savola et al. [16]; *f*) using methods such as Bayesian networks [20], game theory, Markov chains, etc. to support the threat estimation and prediction; *g*) using a decision making module to enforce appropriate security and privacy level; and *h*) communicating data to other nodes in the IoT.

In the adaptive security concept, the Monitor receives data from sensors and other sources that are further used in the Analyzer/Learner to make adaptive decisions. In this context, the ASSET Evaluation framework can be used to provide the ground truth data *a*) to train the learning algorithms employed in the evaluation loop, and *b*) to evaluate whether the behaviour of the adaptive algorithms is reasonable.

For this we follow the following recipe: We use the storylines similarly as done in Section V where we calculate the q-values for all useful cases that can appear for this storyline. Further, we use multiple tools such as implementation in a lab [21], simulation, and formal reasoning [22]. **[tbd.]** ~~Here, the scenarios and storylines can be connected to the arrangements,~~

~~which are sets of configuration settings that influences how the formal model operates. Moreover, the properties of a model checker can directly be extracted from the requirements generated from the scenarios.~~

For the purpose of learning, for all states we retrieve the measurements from the sensors, the context, the assessed q-values, transition to the next desirable state, and desirable output are used as input for the learning algorithm. Thus, the assessed data using the evaluation framework and the measured sensor data are tied together.

For the purpose of evaluating the behaviour of the network, the storylines can used as shown in Section V. After the assessment is finished, one starts with a start-state and uses either an implementation in a lab, a real implementation, or a simulation to perform rounds in the adaptation loop. The assessed values from the evaluation framework are compared with the behaviour of the adaptation algorithm and evaluated. the goal is to get a behaviour of the adaptation loop that is close to the "right" decisions deducted from the assessment. More on how such evaluations can be performed is shown in a framework presented by Leister et al. [22].

VII. Conclusions

[tbd.: update.] We highlighted the role of the scenarios in the assessment framework for IoT-based adaptive security solutions in eHealth. This is based on a generic system model, the requirements for eHealth applications, and a generic assessment framework. The Home Scenario of the ASSET project covers multiple core scenarios representing various situations. These address specific requirements related to the context, the data-communication, the devices, and the actions of the involved actors. The core scenarios are specific to the eHealth case, and make it possible to identify relevant cases that need to be evaluated, such as situations where IoT devices need to be removed or disconnected, the use of ample communication channels, or the impact of mobility.

A storyline for a home patient with chronic diseases has been described and analysed. In the future, the overall scenarios, as well as the underlying core scenarios and storylines will be used in the ASSET project to evaluate the developed algorithms within adaptive security.

VIII. Acknowledgments

The work presented here has been carried out in the project ASSET – Adaptive Security for Smart Internet of Things in eHealth (2012–2015) funded by the Research Council of Norway in the VERDIKT programme. We wish to thank our colleagues involved in this project for helpful discussions that made this study possible. Particularly, we want to thank Ragnar Hauge for discussions while developing this work.

References

[1] W. Leister, M. Hamdi, H. Abie, and S. Poslad, "An evaluation scenario for adaptive security in eHealth," in PESARO 2014 – The Fourth International Conference on Performance, Safety and Robustness in Complex Systems and Applications. IARIA, 2014, pp. 6–11.

[2] H. Abie and I. Balasingham, "Risk-based adaptive security for smart IoT in eHealth," in BODYNETS 2012 – 7th International Conference on Body Area Networks. ACM, 2012.

[3] I. F. Alexander and N. Maiden, Eds., "Scenarios, Stories, Use Cases: Through the Systems Development Life-Cycle". John Wiley & Sons, 2004.

[4] S. Faily and I. Flechais, "A meta-model for usable secure requirements engineering," in SESS – ICSE Workshop on Software Engineering for Secure Systems. Association for Computing Machinery (ACM), 2010.

[5] H. Mouratidis and P. Giorgini, "Security attack testing (SAT)–testing the security of information systems at design time," Information Systems, vol. 32, no. 1, Jan. 2007, pp. 1166–1183.

[6] W. Leister, H. Abie, and S. Poslad, "Defining the ASSET scenarios," Norsk Regnesentral, NR Note DART/17/2012, Dec. 2012.

[7] ISO, "ISO/IEC 27005:2008 Information technology – Security techniques – Information security risk management," International Organization for Standardization and International Electrotechnical Commission, standard, 2008.

[8] W. Leister, S. Boudko, and T. H. Røssvoll, "Adaptive video streaming through estimation of subjective video quality," International Journal On Advances in Systems and Measurements, vol. 4, no. 1&2, 2011, pp. 109–121. [Online]. Available: http://www.iariajournals.org/systems_and_measurements/ [Accessed: 1. Dec 2013].

[9] R. Likert, "A technique for the measurement of attitudes." Archives of Psychology, vol. 22, no. 140, 1932, pp. 1–55.

[10] A. Nevill and A. Lane, "Why self-report likert scale data should not be log-transformed," Journal of Sports Sciences, vol. 25, no. 1, 2007, pp. 1–2.

[11] J. Perl and S. Russell, "Bayesian networks," in Handbook of Brain Theory and Neural Networks, M. Arbib, Ed. Cambridge, MA: MIT Press, 2003, pp. 157–160.

[12] A.-K. Groven, K. Haaland, R. Glott, and A. Tannenberg, "Security measurements within the framework of quality assessment models for free/libre open source software," in proc. Fourth European Conference on Software Architecture: Companion Volume, ser. ECSA '10. New York, NY, USA: ACM, 2010, pp. 229–235.

[13] W. Leister, T. Fretland, and I. Balasingham, "Security and authentication architecture using MPEG-21 for wireless patient monitoring systems," International Journal on Advances in Security, vol. 2, no. 1, 2009, pp. 16–29. [Online]. Available: http://www.iariajournals.org/security/ [Accessed: 1. Dec 2013].

[14] W. Leister, T. Schulz, A. Lie, K. H. Grythe, and I. Balasingham, "Quality of service, adaptation, and security provisioning in wireless patient monitoring systems," in Biomedical Engineering Trends in electronics, communications and software. INTECH, 2011, pp. 711–736.

[15] R. Savola and H. Abie, “Metrics-driven security objective decomposition for an e-health application with adaptive security management,” in ASPI 2013 – International Workshop on Adaptive Security & Privacy management for the Internet of Things. ACM, 2013.

[16] R. Savola, H. Abie, and M. Sihvonen, “Towards metrics-driven adaptive security management in e-health IoT applications,” in BODYNETS 2012 – 7th International Conference on Body Area Networks. ACM, 2012.

[17] W. R. Ashby, “An Introduction to Cybernetics”. London: Chapman & Hall, 1957.

[18] ISO, “ISO/IEC 27001:2005 Information technology – Security techniques – Information security management systems – Requirements,” International Organization for Standardization and International Electrotechnical Commission, standard, 2005.

[19] H. Abie, “Adaptive security and trust management for autonomic message-oriented middleware,” in IEEE Symposium on Trust, Security and Privacy for Pervasive Applications (TSP 2009). Macau, China: IEEE, 2009, pp. 810–817.

[20] J. Pearl, “Probabilistic Reasoning in Intelligent Systems: Networks of Plausible Inference. Representation and Reasoning Series”. Morgan Kaufmann, 1988.

[21] Y. B. Woldegeorgis, H. Abie, and M. Hamdi, “A testbed for adaptive security for IoT in eHealth,” in ASPI 2013 – International Workshop on Adaptive Security & Privacy management for the Internet of Things. ACM, 2013.

[22] W. Leister, J. Bjørk, R. Schlatte, E. B. Johnsen, and A. Griesmayer, “Exploiting model variability in ABS to verify distributed algorithms,” International Journal On Advances in Telecommunications, vol. 5, no. 1&2, 2012, pp. 55–68. [Online]. Available: http://www.iariajournals.org/telecommunications/ [Accessed: 1. Dec 2013].