An Evaluation Scenario 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

***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.**

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. 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 by Abie and Balasingham [1]. 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 available: 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 [2] 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 [3], [4]. This work focuses on the development of scenarios that support the evaluation of adaptive security techniques for the IoT in eHealth.

In this paper, we develop a framework for the assessment of adaptive security solutions. For this, we study a scenario for the home environment, where different Quality of Service (QoS) requirements, contexts and adaptive security methods and mechanisms are analysed. We first 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. Second, the scenarios that have been proposed by Leister et al. [5] are reviewed and their adequacy to the evaluation of adaptive security techniques for the IoT is analysed. Finally, we propose a storyline that can support requirements analysis, as well as adaptive security design, implementation, evaluation, and testing.

The rest of the paper is organised as follows: Section II specifies the requirements of adaptive security for the scenario. In Section III, we describe the extension of a previously developed generic system model, which is used for the structure of the scenario in Section IV. In Section V, we present a storyline for our home scenario. Finally, Section VI 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

 ISBN: 978-1-61208-321-6

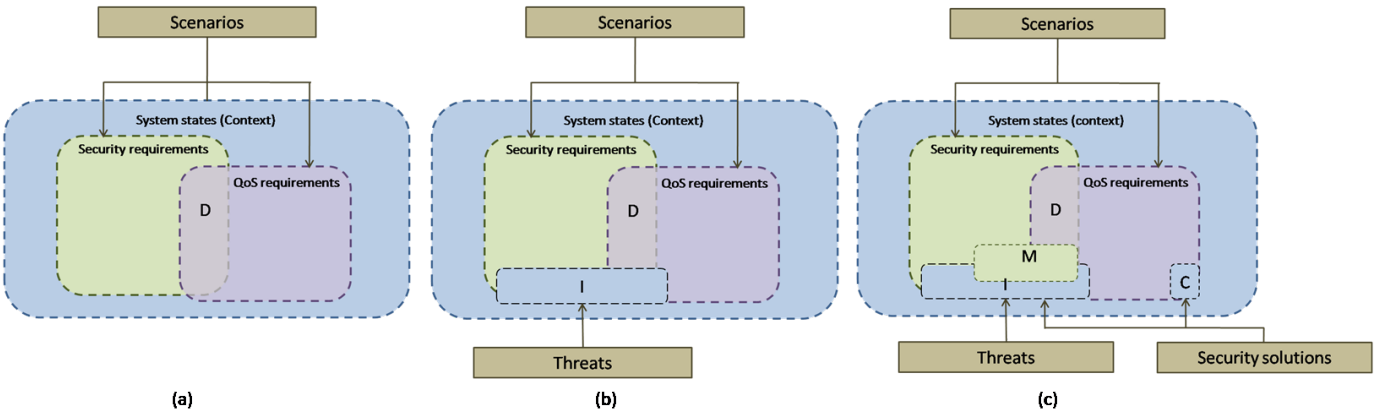

Fig. 1. The ASSET assessment framework.

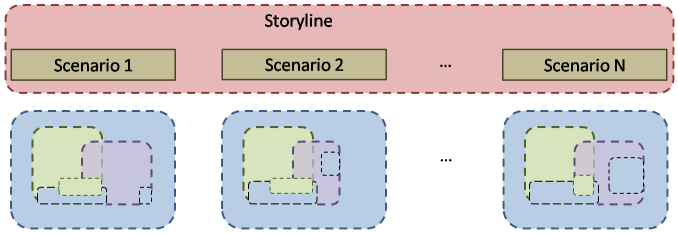

Fig. 2. Illustration of context changes during the execution of a storyline.

of threat occurrences 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 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 and illustrate the dynamic interplay between these needs and the security requirements.

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 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 and the set of states where the QoS is acceptable. The intersection of these sets is the set of desirable states, denoted in Fig. 1(a) by 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 actions that generate insecure system states while countermeasures are assumed to thwart the effects of these threats. A threat reduces the set of secure states generated by the scenario of interest and affects the QoS requirements. This is represented by the region I (Impact) in Fig. 1(b). This region represents a set of states that do not fulfil the security or QoS requirements. The countermeasures reduce the size of the set of insecure states generated by the threats. Fig. 1(c) illustrates the effect of the security solutions through the region M (Mitigate). This region extends the set of secure states. Nonetheless, the security solutions can have a negative effect on the QoS, represented by the region C (Cost), consisting of power, processing, memory, and communication overhead.

The elements of this representation will be used in the scenarios during the assessment of adaptive security schemes. The scenarios allow evaluating the potential brought by the security techniques to minimise the effect of the attacks on the 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

 ISBN: 978-1-61208-321-6

from the ASSET scenarios. These can be viewed as a sequential application of the scenarios in a way that the selection of 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 to threats. 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 potential 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.

For the assessment of adaptive security protocols and algorithms we can employ multiple tools such as implementation in a lab [6], simulation, and formal reasoning [7]. Here, the scenarios 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.

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.

III. Extended Generic Model for eHealth Scenarios

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 [8] and suggested a framework for providing privacy, security, adaptation, and QoS in patient monitoring systems [9]. 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.

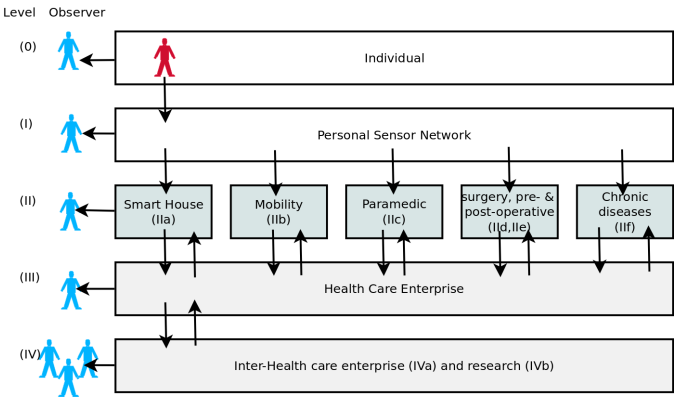

Fig. 3. Generic eHealth framework indicating the use cases in five levels (Extended from [8]).

In this work, we extend the generic model presented by Leister et al. [9] 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) 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) **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.

(IIb) **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

 ISBN: 978-1-61208-321-6

using long-distance data communication.

(IIc) **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.

(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.

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 two 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) and a hospital scenario (B).

Each of these overall scenarios contain a set of core scenarios which are denoted by the scenario identifier A or B, followed by a dash and the core scenario numbering in roman numbers. The transitions between these core scenarios model the interaction between the various components of the patient monitoring system. In this paper, we focus on the Home Scenario (A) where the patient is supposed to be monitored outside a hospital 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.

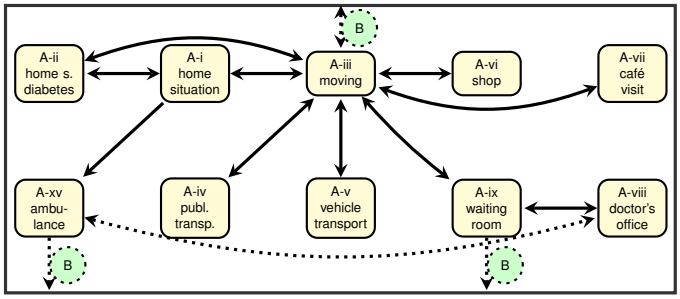

Fig. 4. The Home Scenario with the underlying core scenarios and their transitions.

IV. The Structure of the Home Scenario

Home Scenario (A) envisages that the monitored patient can be in various contexts performing normal daily actions. For example, for a patient with diabetes the following core scenarios can 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, such as the specific context information, 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 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.

 ISBN: 978-1-61208-321-6

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 the smartphone using Bluetooth. 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 an 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 ASSET other scenarios have been developed which are omitted here. Most of these are specific to the hospital scenario B. For completeness, we mention a scenario where patients are brought to a hospital in an ambulance (B-xv).

V. 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;

 ISBN: 978-1-61208-321-6

   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).
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.

To conduct an efficient threat analysis of this storyline, we apply security objectives introduced by Savola and Abie [10] and Savola et al. [11], 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.

VI. Conclusions

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 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.

VII. 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.

References

[1] 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.

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

[3] 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.

[4] 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.

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

[6] 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.

[7] 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].

[8] 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].

[9] 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.

[10] 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.

[11] 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.

 ISBN: 978-1-61208-321-6