Modeling Adaptive Security in IoT Driven eHealth

Waqas Aman
Norwegian Information Security Lab(NISLab)
Gjøvik University College, Norway
waqas.aman@hig.no

Abstract

The implementation of Internet of Things (IoT) in eHealth will indeed significantly enhance ubiquitous healthcare services. Existing research in these areas and corresponding systems are more focused on functional designing and developing preventive and detective security controls. However, threats faced in IoT are more complex due to the diverse nature of technologies involved and the evolving threat landscape. They have become more sophisticated and challenging for preventive and detective technologies. Hence, we need to develop adaptive security solutions for IoT-eHealth which can predict security threats and respond to them dynamically to protect personal health information. This paper presents an adaptive security model that will learn adverse influences in IoT-eHealth infrastructure, predict and estimate the risks involved in a context-aware manner and autonomously adapt security measures in order to minimize the risk faced. The model presented is a preliminary abstraction that reflects how adaptive security can be achieved in IoT-eHealth.

1 Rationale

IoT is a global network focusing on the interconnection of various technologies (things) to support services quality and their extensions [1]. IoT inherit intelligent and self-* capabilities, such as self-learning and self-adapting, which makes it favorable for dynamic environments [2]. However, due to the fact that IoT allows diverse technologies, wired and wireless, it is subjected to an array of threats as underlined by [3, 4, 5, 6]. This provides an adversary multiple means and opportunities to target personal health information that is transmitted from body sensors to remote hospital sites.

Traditional preventive and detective measures such as IDS, Access Control Lists (ACLs), firewalls, anti-viruses, etc., as stand-alone controls cannot provide the reality of an ongoing attack. They lack to add contextual information failing to distinguish a security event from a non-event thus leading to high rate of false

This paper was presented at the NISK-2013 conference.

positives [7]. Adaptive security can provide a comprehensive security solution for IoT-eHealth where diverse technologies used are threatened by an array of ever changing security and privacy risks [2, 8, 9]. This approach can be seen in various security models, such as [10, 11, 12, 13] however, they are not intended for IoT-eHealth. To elaborate the process, adaptive security systems continuously monitors user, device and network related events (as environmental influence), establishes a context among them to analyze the situation (risk) reality and devise a new security strategy (as a response to the influence) as per the risk evaluated to defend against it. This mechanism provides a *predictive security* solution where the threats are apprehended before it becomes reality [14].

To be aligned with the nature of IoT-eHealth, which is a continuous monitoring service, security risks should also be assessed and responded dynamically. In the ASSET (Adaptive Security for Smart Internet of Things in eHealth) project [15] we aim to achieve this objective by developing risk based adaptive security methods to ensure predictive and autonomous security in IoT-eHealth. This paper presents an adaptive security model for IoT-eHealth based on the requirements we analyzed in [9]. These essentials entail that: **a).** Risks need to be dynamically assessed, **b).** The solution should provide context awareness to increase security intelligence required for risk analysis and to reduce false-positives, **c).** Autonomous adaptation needs to be incorporated to evolve security settings and responding to the analyzed risks autonomously and **d).** The solution should assimilate lightweight analysis methods to reduce the computational complexity. The objective of this paper is to answer the questions: How adaptive security can be modeled in IoT-eHealth? And, what are the necessary components and actions to accommodate the mentioned requirements? The model is still in the development phase and will be explored and evaluated in the near future. However, it illustrates the ground concept that addresses the requirements we analyzed earlier and gives an abstract solution for the adaptive security process in IoT-eHealth.

The rest of the paper is organized as follow: Section 2, presents a typical IoT-eHealth infrastructure. The proposed model will be detailed in Section 3. In Section 4, an objectives-based evaluation is presented aiming to recognize how the proposed model meets the risk management requirements in IoT-eHealth. Finally, the concluding remarks and our future research endeavors regarding the proposed model will be detailed in Section 5.

2 IoT-eHealth Infrastructure

A typical IoT-eHealth infrastructure, depicted in the figure 1, includes wearable body sensors which collects various bio-signals and transmits them to a hospital site for medical investigation via intermediary nodes and communication paths. In ASSET's lab, we have used a planar architecture [16] at the edge of the Body Sensor Network (BSN) in which bio-signals are collected, interpreted and (locally) analyzed by a terminal node using single-hop communication. We have introduced the terminal node as a smart *thing*, a smartphone or a tablet, in order to utilize its features and resources to support eHealth services such as mobility, emergency calls, local analysis and reporting, patient-doctor communication and e-prescriptions etc. ZigBee and Near Field Communication (NFC) are used as channel protocols between the BSN and smartphone. The bio-signals are then sent to a remote hospital site using Internet or mobile network (3G/4G, GPRS) for further investigations.

Currently, the Internet is used as a communication model between the patient and hospital sites.

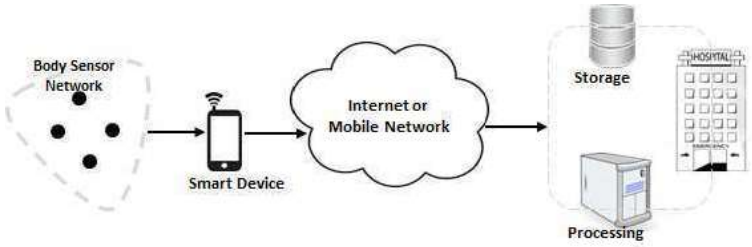

Figure 1: Typical IoT-eHealth Infrastructure

3 Proposed Model

This section elaborates our proposed risk based adaptive security model. The model is built on the concept of Security Event Management (SEM). SEM systems collects *interested* events from network devices, applications and systems and examine them to analyze the overall system security [14, 17]. They intend to provide a consolidated and centralized security management solution. The model consists of three major functional components: Monitor, Analyzer and Adapter. The entire Monitor-Analysis-Adaption process is done in a continuous real-time manner. Critical information, such as risk metrics, policies, analyzed risks, correlation rules, adaptive rules etc., are stored in the adaptive database, which are referenced and updated along the process. An abstract view of adaptive security process is depicted in figure 2 whereas, the proposed model is shown in figure 3. A description of the components and their functions is detailed in the subsequent subsections.

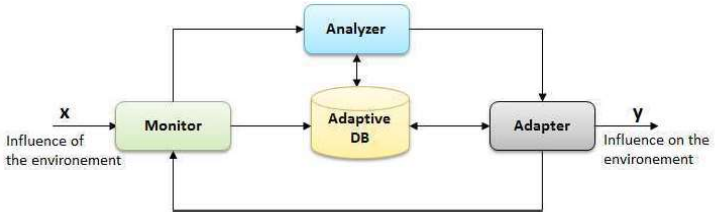

Figure 2: Continuous Adaptive Security Loop

Monitoring

The *Monitor* component is used to capture the environmental influence on the individual infrastructural elements, such as the sensors, smart device, etc., as well as the associated network behavior and statistics. Depending upon the event syntax and semantics generated by a specific source, events can be sent to monitoring (Collector) unit using different transport protocols, such as Syslog [18], which is the most common protocol used to collect events(logs) remotely. The collector component can be configured with the corresponding protocols' *sinks* in order to receive or collect the events in its integral form. To analyze events collected from different sources using different transport protocols, they must be transformed to a common format understandable by the *Analyzer* component. This transformation

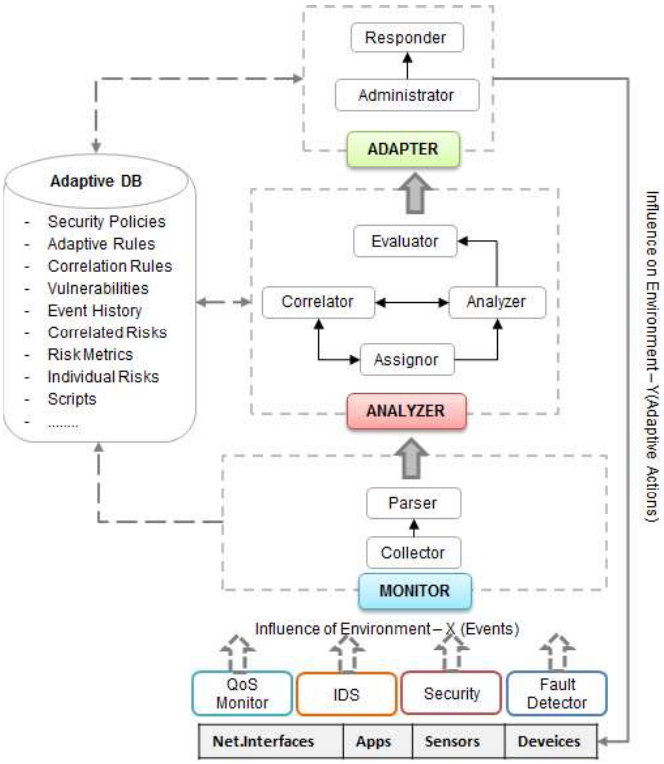

Figure 3: Proposed Adaptive Security Model

is done by the *Parser* which extracts the interested fields for analysis from the raw events and transform them to a universal format. We will be using regular expressions and XML libraries, such as [19, 20], as a standard universal techniques for events to be recognized and analyzed by the Analyzer effectively. Context of individual events are stored as XML tags which defines various attributes reflecting the situation of an event.

Analysis

The *Analyzer* establishes a context among related events and analyzes the impact and risk associated with them. It (*Assignor*) assigns risk metrics to the transformed events received from the monitor thus, adds more to the context of an event. Risk metrics can be pre-determined or dynamic values, for instance impact, likelihood, reliability or probability, which can be assigned to the event based on its sensitivity and the asset generating it. The *Correlator* relates different events (contexts) coming from different sources and provides an advance context that provision a true picture of the faced threat. This reduces the false-positives and increase security intelligence for the risk analysis and optimized adaptation [21]. Correlation can be achieved using pre-defined rules or using formal modeling techniques such as Bayesian network modeling or Machine Learning techniques.

Adaptation

Risks beyond acceptance are notified to the *Adapter* where a decision to circumvent the anticipated risk and a mitigation action is taken. Events from external security and performance tools, such as QoS monitors, Fault detectors, IDS and vulnerability management, can also be used to enrich the intelligence of security analysis process.

The main objective of this function (*Administrator*) is to administer the decision of an optimal security response that reduces the analyzed risk to an acceptable level. It may consult stored adaptation rules or may use established approaches, such as Decision theories. Machine learning techniques can be used to complement the enrichment of existing adaptive and correlation knowledge. The adapter also directs the necessary steps to be taken to mitigate the faced risk. These directions are provided to the *Responder* which formulate them and consult the stored scripts to execute the security adaptation.

4 Objectives-Based Evaluation

In our previous study [9] we analyzed various requirements for dynamic risk management, which were formulated based on the nature and needs of IoT-eHealth. To revise, we identified IoT-eHealth as a continuous monitoring service where patient health information is transmitted, analyzed and responded to in a continuous manner. The main data producers in the infrastructure are the body sensors. Another critical resource is the smart device which is the first point of contact data collection, interpretation and (local) analysis for the sensor's data. These two resources are considered to be low-end devices.

Basing these facts, we conclude that IoT-eHealth needs an InfoSec risk management solution which should: assess the risks faced in a *dynamic* and *contextual* manner; its analysis needs to be *lightweight* to accommodate the computational constrains and to ensure immediate analysis and decisions; and that it should provide *autonomous adaptation* to mitigate the risk. In the subsequent sections, the proposed model is evaluated to ensure how it meets these requirements.

Dynamic Assessment

The model is designed as continuous-feedback loop which provides a dynamic and continuous mechanism for monitoring, analyzing and managing system and network behavior [22]. This property is a vital design consideration in self-* systems [23]. In the proposed model, events are collected, filtered, translated, analyzed, stored continuously and decisions on the analyzed events are performed dynamically. The environmental influences on the system are monitored and analyzed continuously and in realtime whereas, system influence (security adaptation) on the environment to mitigate an analyzed risk though, performed in realtime but is done when necessary.

Context Awareness

Context is the information required to characterize the situation of an entity [24]. In IoT-eHealth, an entity could be any of the infrastructural object as well as the users (patients, doctors or healthcare stakeholder in general). In the proposed model, we intend to achieve context awareness by modeling the information collected in Extensible Markup Language (XML). Events collected will be tagged with attributes that will define their situation and impact. When events are generated, there are certain attributes that are logged by the source. These attributes detail questions like who, where, when and what, which characterize the situation of an event. Context will be represented and stored in XML which will be analyzed by the Analyzer during risk analysis.

Furthermore, a threat faced is an organized collaboration of different events and exploits which are experienced and logged by different sources as it progresses to the actual target(s). Thus, analyzing a risk based on a single event does not reveal the actual risk confronted and may results in false-positive redundancy [21]. It is therefore, necessary to relate events from different sources to provide holistic and contextual information for the risk analysis and to predict or detect the anticipated risks accurately. The correlation engine in the proposed model will correlate events from different sources with different context thus, providing new, advance and more refine context(s) based on reasoning (for instance, stored correlation knowledge) to make the risk analysis process more accurate.

Lightweight Analysis

To achieve fast response in the entire adaptive security process and to accommodate the computational resources of the low-end devices in the infrastructure, we are aiming to introduce lightweight mechanisms into the proposed model. The model is currently in the development phase where we haven't selected any specific methods. However, we intend to use simple tools and techniques, for instance, [25, 19, 20] for common jobs, such as event filtration, parsing, representation and their storage, to give enough time for the actual risk analysis and adaptation. Currently, we are exploring traditional risk metrics formulation as well as lightweight formal approaches to Game, Decision, Utility theories based approaches, such as [26, 27], as they tend to model the dynamic behavior of entities in a conflicting situation.

Autonomous Adaptation

The Adapter component in the proposed model will fulfill two objectives in the context of security adaptation:

1. Enhancing the stored correlation and adaptive knowledge by learning new trends and patterns from risk analysis and mitigation decision (performed by the *administrator*) processes. This will assist in accurate threat prediction, precise risk analysis and optimized mitigation strategies in future adversarial confrontations.

2. Adapting an optimized mitigation response to reduce the negative impact of a currently faced risk. Decision instructions (provided by the *Administrator* to the *Responder*) will be formulated which will trigger the stored scripts to execute the adaptive response. The response formulated can either be a security action for instance, blocking an unsecured port or employing a more secure protocol for future communications.

From design perspective we will be using Machine Learning techniques and Decision theories to meet this objective.

5 Conclusion & Future Work

IoT enabled eHealth will significantly enhance remote and mobile health monitoring. However, the introduction of IoT will increase the security risk as diverse technologies will be incorporated which can furnish multiple paths of attacks for the adversary. Furthermore, threat sophistication has also increased. Thus, traditional

preventive and detective technologies seem to be ineffective to apprehend the risks faced. To overcome this problem, a risk-based adaptive security model is proposed in this paper that provides a continuous, realtime, context-aware assessment and an autonomous and optimized mitigation response to reduce an anticipated risk in IoT-eHealth. Its continuous and context-aware event correlation ensures to capture the threat before they become realistic. Thus, provides a predictive security solution to analyze the unknown threats.

In future, we intend to refine the proposed model which includes, identifying, detecting and categorizing security events in IoT, devising methods for correlating dependent events as well as risk analysis and identifying security metrics upon which the system will adapt. Beside formal methods, such as Game theory, Bayesian modeling and Utility theory, which are the primary design focus, we intend to achieve these objectives using lightweight approaches. Security metrics necessary for adaptation will be explored. An attack-defense case study will be formulated to validate the proposed model and a prototype will be developed on which formal tests and experimentation will be performed.

Acknowledgments

The work presented in this article is a part of the ASSET (Adaptive Security in Smart IoT in eHealth) project. ASSET (2012-2015) is sponsored by the Research Council of Norway under the grant agreement no: 213131/O70. Wishing thanks to the project colleagues and partners for their valuable suggestions and comments.

References

[1] Rolf H. Weber. Internet of things: New security and privacy challenges. *Computer Law & Security Review*, 26(1):23 – 30, 2010.

[2] Habtamu Abie and Ilangko Balasingham. Risk-based adaptive security for smart iot in ehealth. In *Proceedings of the 7th International Conference on Body Area Networks*, BodyNets '12, pages 269–275, ICST, Brussels, Belgium, 2012.

[3] M. Meingast, T. Roosta, and S. Sastry. Security and privacy issues with health care information technology. In *Engineering in Medicine and Biology Society, 2006. EMBS '06. 28th Annual International Conference of the IEEE*, pages 5453–5458, 2006.

[4] Hemanta Kumar Kalita and Avijit Kar. Wireless sensor network security analysis. *International Journal of Next-Generation Networks (IJNGN),*, 1:1–10, December 2009.

[5] Luigi Atzori, Antonio Iera, and Giacomo Morabito. The internet of things: A survey. *Computer Networks*, 54(15):2787 – 2805, 2010.

[6] Sumari Putra Ramli Rusyaizila, Zakaria Nasriah. Privacy issues in pervasive healthcare monitoring system: A review. *World Academy of Science, Engineering & Technology*, 72:741, 2011.

[7] Dave Shackleford. Real-time adaptive security. Technical report, SANS, December 2008. http://www.sans.org/reading_room/analysts_program/adaptiveSec_Dec08.pdf [Online Accessed on 16 Jul 2013].

[8] Reijo M. Savola and Habtamu Abie. Metrics-driven security objective decomposition for an e-health application with adaptive security management. In *Proceedings of the International Workshop on Adaptive Security*, ASPI '13, pages 6:1–6:8, New York, NY, USA, 2013.

[9] Waqas Aman and Einar Snekkenes. An empirical research on infosec risk management in iot based ehealth. Accepted in: The Third International Conference on Mobile Services, Resources, and Users. MOBILITY 2013, Portugal, August 2013.

[10] Robert W. McGraw. Risk adaptable access control, 2009. http://csrc.nist.gov/news_events/privilege-management-workshop/radac-Paper0001.pdf. Online Accessed on 6 Sept 2013.

[11] RSA. Rsa adaptive authentication. a comprehensive authentication and risk management platform, 2013. http://www.rsa.com/products/consumer/datasheets/6559_AA_DS_0511.pdf. Online accessed on: 19 July 2013.

[12] Habtamu Abie. Adaptive security and trust management for autonomic message-oriented middleware. In *Mobile Adhoc and Sensor Systems, 2009. MASS'09. IEEE 6th International Conference on*, pages 810–817. IEEE, 2009.

[13] Sathishkumar Alampalayam and Anup Kumar. An adaptive and predictive security model for mobile ad hoc networks. *Wireless Personal Communications*, 29(3-4):263–281, 2004.

[14] Roland Rieke and Zaharina Stoynova. Predictive security analysis for event-driven processes. In *Computer Network Security*, pages 321–328. Springer, 2010.

[15] Asset - adaptive security for smart internet of things in ehealth. Approve by Research Council of Norway under the grant agreement no: 213131/O70 (2012-2015).

[16] S Munir, Xie Dongliang, Chen Canfeng, and J Ma. Mobile wireless sensor networks: Architects for pervasive computing, 2011.

[17] Mark Nicolett and Kelly M Kavanagh. Magic quadrant for security information and event management. *Gartner RAS Core Reasearch Note (May 2009)*, 2011.

[18] The bsd syslog protocol. RFC 3164: http://www.ietf.org/rfc/rfc3164.txt. Last Accessed on 1 Sept 2013.

[19] Python - fast xml parsing using expat. http://docs.python.org/2/library/pyexpat.html.Last Accessed on 1 Sept 2013.

[20] Python regular expressions library. http://docs.python.org/2/library/re.html. Last Accessed on 1 Sept 2013.

[21] He Wei. A correlation analysis method for network security events. In Wenjiang Du, editor, *Informatics and Management Science III*, volume 206 of *Lecture Notes in Electrical Engineering*, pages 269–277. Springer London, 2013.

[22] Yuriy Brun, Giovanna Di Marzo Serugendo, Cristina Gacek, Holger Giese, Holger Kienle, Marin Litoiu, Hausi Müller, Mauro Pezzè, and Mary Shaw. Engineering self-adaptive systems through feedback loops. In *Software Engineering for Self-Adaptive Systems*, pages 48–70. Springer, 2009.

[23] Jeffrey O. Kephart and David M. Chess. The vision of autonomic computing. *Computer*, 36(1):41–50, January 2003.

[24] Gregory D Abowd, Anind K Dey, Peter J Brown, Nigel Davies, Mark Smith, and Pete Steggles. Towards a better understanding of context and context-awareness. In *Handheld and ubiquitous computing*, pages 304–307. Springer, 1999.

[25] Xml::parser - a perl module for parsing xml documents, 2011. `http://search.cpan.org/~toddr/XML-Parser-2.41/Parser.pm` Last Accessed on 20 July 2013.

[26] Lisa Rajbhandari and Einar Arthur Snekkenes. Mapping between classical risk management and game theoretical approaches. In *Communications and Multimedia Security*, pages 147–154. Springer, 2011.

[27] Lisa Rajbhandari and Einar Arthur Snekkenes. Using game theory to analyze risk to privacy: An initial insight. In *Privacy and Identity Management for Life*, pages 41–51. Springer, 2011.

NISK 2013 Norwegian Information Security Conference / Norsk informasjonssikkerhetskonferanse

ISSN 1893-6563
ISBN 978-82-321-0366-9