International Journal of Applied Engineering Research
ISSN 0973-4562 Volume 10, Number 4 (2015) pp. 10119-10126

http://www.ripublication.com

A Novel Approach For Information Security and Risk Management In Distributed Health Care Systems

B.Chaitanya Krishna[1], Dr.Kodukula Subrahmanyam[2] , Y. Sai Ramya[3] , G.Kumar Swamy[4], M.Rajesh[5], M.Siddardha[6]
#1, 2, 3,4,5,6 Department of Computer Science and Engineering, K L University, Andhra Pradesh, India.
E-mail: chaitu2502@kluniversity.in[1], smkodulula@gmail.com[2], ramya.yamalakonda@gmail.com[3], kumarswamy245@gmail.com[4], rajesh.malempati94@gmail.com[5], siddardha.maddineni@gmail.com[6]

Abstract

As the security is most concerned aspect in each and every health care organization, the record of the patients are kept highly confidential and is therefore maintained within the organization only. Because of this, if for any reason the patient desires to get treated in the other organization, then there will be a chance for the current doctor to get scarce of the patients previous details like what is the previous treatments he undertook and what are the medicines etc. There also will be a chance for the current doctor that he cannot be able to treat hierarchical diseases by not getting access to his/her ancestors immunity. So, in this paper we are proposing some new methodologies and concepts that will most be helpful in efficiently treating the patients, studying the diseases and thereby treating them.

Index terms: Risk assessment, security, Health-care information systems security, risk management, dependencies.

Introduction

The information security and risk management are commonly associated with IT projects and both must be there in a successful project.As no IT project can ever be risk free, many methodologies have been applied to quantify the likelihood and estimate the impact of risks that a project may encounter. Risk is inherent in the delivery of healthcare. The security risks associated with healthcare systems have increased as direct (network) and indirect (media) connectivity has increased. With sophisticated equipment, there are always more risks than any organization can afford to fully eliminate. Therefore, the need arises for a systematic, documented method to assign risks so that they can be listed in priority order, mitigated accordingly, and

have residual risks documented and accepted. The process for managing healthcare systems IT security-related risks is very similar to long-standing device safety processes. The medical device industry has been engaged in safety risk analysis for over 30 years. This paper recommends that similar methods be applied to security risks to healthcare systems. These methods support a manufacturer in assisting the healthcare provider and directly support a healthcare provider in maintaining confidentiality, integrity, and availability of protected health information. The process of IT security risk management as described in this document includes

1. Listing the assets under consideration and understanding their intended use;
2. Collecting security-related requirements for the assets;
3. Elaboration of threats and applying them to systems to determine vulnerabilities including actors, threat paths, and possible outcomes;
4. Evaluating the risks;
5. Proposing and implementing mitigations for vulnerabilities appropriate to the healthcare domain;
6. Summarization of residual risks along with the system‘s role in advancing the healthcare mission, in order to obtain a ―go‖ or ―no-go‖ decision from manufacturer‘s executive management to give the authority to proceed with development of the system.

Health Care Systems Significance

Health is a state of complete physical, mental and social wellbeing, and not merely the absence of disease or sickness; it is a fundamental human right, and the attainment of the highest possible level of health is a most important worldwide social goal. Since health care systems is very sensitive and any minute fault may result in very severe consequences and it is associated with lots of money. The healthcare sector is defined as a category of supply relating to medical and healthcare goods or services which includes hospital management firms, health maintenance organizations, biotechnology and a variety of medical products. There are various types of healthcare services provided by the health sector. These include traditional health service providers such as private hospitals and day surgeries, medical practitioners and pharmacists. In recent years healthcare organizations worldwide have undergone major reorganization and adjustments to meet the demand of improved healthcare services accessibility and quality; in addition, the use of information technology to process health data continues to grow and more than ever critical information stored electronically is needed by healthcare administrators, providers and other users . Health information is essential for lanning and decision making at all levels of the healthcare spectrum. The sensitive nature of health-related information cannot be disputed. While the protection and security of personal information is important to all individuals, corporations, institutions and governments, there are special requirements in the health sector that need to be met to ensure the confidentiality, integrity, auditability and availability of personal health information . Therefore custodians of health information should ensure that proper ISM practices are followed. Through the establishment of an information security management system, an organization can ensure the selection of

adequate and proportionate security controls that protect information assets and give confidence to interested parties.

Risk Management

A risk is a potential event that will adversely affect the ability of a system to perform its mission should the risk event take place . A risk has two basic attributes, Probability P and Impact I, where Probability stands for the likelihood that an event will occur. A risk Rx can thus be defined mathematically as a function of two attributes: Rx= f(Px, Ix). A common way to compute the risk value is the linear method, which multiplies the values of Probability and Impact: Rx = Px, Ix, where Px has a value between 0 and 1. There are three situations where events are not regarded as risk : 1) The event will never happen (Px = 0;Rx = 0), 2) the event will certainly happen (Px = 1; Rx = Ix), and 3) the event will not have any impact even if it does happen (Ix = 0;Rx = 0). A more precise computation of risk under the linear method is Rx = PxIx, 0 < Px < 1, and Ix!= 0.

Risk Management Practices: The Software Engineering Institute (SEI) has developed a risk management paradigm , which is an elaboration of the classic ―plan-do-check-act" cycle and specifies a set of cyclic steps (i.e., Identify, Analyze, Plan, Track, and Control) throughout an IT project . It emphasizes the risk management as a continuous process in which each risk goes through these steps sequentially and independently.

The common risk management processes and management practices are :

1) Identify Project Risk
2) Evaluate and Prioritize Risk
3) Develop Risk Response Plans
4) Monitor Status of Risk and Associated Risk
5) Response Actions.
6) Control Risk Response Actions

Dependency Analysis Models

Current project management practices do not clearly address how dependencies between risks are managed. In this section, we review several dependency analysis models that have been used to represent the dependency of one event on another .

There are three common tree-based analysis techniques. First, fault tree is a logical diagram used in the Fault Tree Analysis (FTA) to represent the possible causes of an undesired event. The root of the tree represents the undesired event, and the other events that lead to the root are modeled by independent leaf nodes with a series of logical expressions.

Summary of Various Dependency Analysis Models

Models/Techniques	Characteristics	Applications
Tree-based Analysis	-Tree Structure (acyclic) -Qualitative or quantitative analysis	Used to analyze possible causes of undesired events
Markov Analysis	-Directed graph structure -A mathematical method	Used to analyze the reliability and availability of a system
Bayesian Network	-Directed acyclic graph structure -Qualitative or quantitative analysis	Used to manage uncertainty by explicitly presenting the conditional dependencies between different knowledge components
Goal-Risk Model	-Directed graph structure -Qualitative analysis	Used to model the risks with the relations between stakeholders _goals

Second, Event Tree Analysis (ETA) is a method to illustrate the sequence of possible outcomes after the occurrence of an undesired event. similarly to a fault tree, an event tree starts from an undesired event, and the event is linked to its outcomes Toward the final consequences with a probability of occurrence assigned to each tree branch.

Last, cause-consequence analysis (CCA) combines the FTA and ETA and is performed with a cause consequence diagram which starts from an undesired event and develops backward to identify its causes (presented by a fault tree) and forward to identify its consequences

Markov analysis provides a mathematical method to analyze the reliability and availability of systems which are well specified and have strong component dependencies. In this analysis, a system is modeled as a number of discrete states with possible transitions among the states. The states are graphically presented as nodes in a directed graph.

In a Bayesian network , each node represents a variable and each arc represents causal or probabilistic influential relationships between variables. A link between two variables represents a probabilistic dependency between them.

A goal model, represented as a directed graph, is used to refine the goals of a target system by decomposition into measurable sub goals.

Healthcare Security Risk Management Process

The process for managing healthcare system IT security-related risks is very similar to long-standing device safety processes. For example, tools such as Failure Mode and Effect Analysis (FMEA) as applied to safety considerations can be used for security investigations as well. We will not detail safety risk assessment other than to note the

relationship where security must be subordinate to patient and operator safety. To avoid conflict and confusion, we recommend that the security risk assessment process be performed separately from the safety risk assessment, because overall, they have different requirements and involve fundamentally different assets. Whenever a security risk has a credible safety risk, even after proposed mitigation, the safety risk assessment process takes precedence. In general, this means moving the primary discussion of the risk to the safety team accompanied by a knowledgeable, security team member. In this manner, the two processes generally proceed in parallel throughout the product creation process. The skills of the risk management team members require specific elaboration. People with general IT knowledge as a background often are not aware of the healthcare-specific issues that may lead to impractical measures at the end.

This paper proposes a new methodology for providing security to the information and globalization of patient records in the following way:

1. Assigning an unique token to patient which is used as reference for the patient‘s records.
    a) A unique token id is identified through biometrics like thumb prints, retina scans etc.,
    b) Whenever the patient went to hospital his previous medical records are retrieved by using the token number so that the doctor easily knows the patients health condition , blood group , and about the diseases he/she has like blood pressure , diabetes etc.,
    c) The information associated with the token number about the patient helps the doctors to know easily about patient and what type of medicine is suitable for him.
    d) When a patient enters into hospital a token is assigned to him for the first time and after every time token assigned is used.
    e) These token numbers are maintained globally so that all the hospitals will have that data.
2. The data is maintained in one domain and the trusted doctors can access the patient information through some login credentials.
3. The data is continuously monitored and updated in the server which gives many advantages.
4. A list contains the hospitals data is maintained which contains the hospitals name , address and for which treatment they are serving better etc.,
5. This data helps the patients, easy to approach a better hospital quickly.
6. A server is maintained globally by having a proper network connection which must be available 24*7.
7. This data can be accessed by every doctor who has been recognized from a standard institution , so that there is no chance of misleading the patient through charging extra money for unnecessary tests, scanning, etc.,.
8. By maintaining patient records globally every doctor can view the patient‘s condition, so that he can suggest the better treatment for that patient through emails , messages , phone calls to respective hospitals.

9. The patient‘s health records are continuously monitored and that data is updated time to time.
10. The advantage by doing this is, all the doctors available are given information about the condition of patient so that immediate treatment should be made possible.
11. The patient can get the medicines for some mild illness by not going to hospital through some emails or messages.
12. The security to the data can be maintained by keeping all the data in the encrypted form and the doctors are given the key to decrypt so that only certified doctors can access data.
13. The continuous data connection is maintained through wifi and if any data connection is lost a local server is maintained to serve at those times.

Existing System

There are so many systems prevailing which provide security to electronic health records, but so many of them are lagging significant features as following:

- No generalization of the patient info i,e the data is maintained within the organization only.
- with the present one doctors cannot know how the patient responded for the previous treatment or medicines.
- if any new diseases occur and if the doctor is unable to identify the disease, it is not possible to study his/her ancestors immunity right at the moment when the doctor needs.
- No unique token numbers are provided for the patients in order to easily maintain the information like medicines, blood group...etc
- Private hospitals data are not disclosed to the government and is kept confidential, and because of this govt is facing a lot of difficulty in conducting a research of frequently occurring diseases that are prevailed among a particular community or group in order to provide proper vaccination.

Proposed System

By overcoming the limitations of the existing systems we are proposing a new system with the following features:

- We globalize the patients records such that the information is disclosed to all the doctors within the circle based on the trust policy.
- By this method current doctor can understand totally about the patient i,e he can have an idea about how the patient responded to the previous treatment, medicines etc.
- The disclosure is done entirely based on trust and an authentication mechanism is proposed in order to keep the info safe. Encryption is performed with in the circles in order to keep the VIP records safe.

- Unique token numbers is assigned to the patients and they can use this number any where they would like to take treatment.
- Due to the globalization of info government can easily track and conduct a research on the prevalent diseases and they can take measures accordingly.
- Hierarchical diseases can be treated easily by getting access to their ancestors info that is how they responded and what are symptoms they suffered with.

Conclusion

As Risks are inevitable in any IT project and Information security is an ongoing process to manage risks. One could say that risk management is essentially a decision making process. The risk assessment stage is the collection of information that is input into the decision. The risk mitigation stage is the actual decision making and implementation of the resulting strategy. The effectiveness evaluation is the continual feedback into the decision making. This approach can be further extended to eliminate corruption for various government schemes in health sector. The fully automated and wifi connected system can be implemented as real time project which will be very useful. The advantage of using these fuzzy cognitive approach and risk evaluation techniques together is that it takes into account intuitive human observation, which forms the basis of any risk assessment, and also accounts for the vagueness regarding patient information and risks when calculating a phase‘s risk level in a typical patient route. By identifying a phase‘s IT risk value, this approach helps health care staff manage risks by facilitating the decision-making process. Since the information should be accessible for the clients throughout the day and the records are disclosed to the required one‘s wherever needed, requires the server to stay active 24*7. Also multiple number of clients will be connected to a single server at a time, this can be a little bit bottle neck. Hierarchical diseases can be efficiently treated by studying his/her ancestors record. If managed in an efficient way, this system will have a great scope in the future.

References

[1] Cookbook for the Security Section of IHE Profiles, Aug 20, 2006, http://www.ihe.net/Technical_Framework/upload/IHE_ITI_TF_White_Paper_Security_Cookbook_PC_2006_08_30.pdf

[2] Ajit Appari, M. Eric Johnson Information Science and security for privacy in healthcarehttps: //inderscience.metapress.com/content/dp52k03546006x0r/resource-secured/?target=fulltext.pdf

[3] S. Tyali and D. Pottas Information Security Management Systems in the Healthcare Context. www.cscan.org/openaccess/?paperid=195

[4] Economic Commission for Africa (1999), –Information and communication technology for health sector”, http://www.uneca.org/aisi/docs/pfshealth.pdf, (Accessed 15 June 2008)..

[5] ISO 27001. (2005). ISO/IEC 27001: Information Technology – Security Techniques – Information Security Management Systems - Requirements (1st ed.). Switzerland: International Organization for Standardization.

[6] ISO 27799. (2008). ISO/IEC 27799: Health informatics — Information security management in health using ISO/IEC 27002 (1st ed.). Switzerland: International Organization for Standardization.

[7] IEC 60812 Ed. 1.0: Analysis Techniques for System Reliability - Procedure for Failure Mode and Effects Analysis (FMEA).

[8] International Journal of Applied Environmental Sciences ―Information Security and Risk Management for Health Care System" ISSN 0973-6077 Volume 9, Number 3 (2014), pp. 645-650, http://www.ripublication.com.

[9] International Journal of Applied Engineering Research ―Risk Assessment in Distributed Banking System" ISSN 0973-4567 VOLUME 19 (2014), pp. 6087-6100, http://www.ripublication.com.

[10] International Journal of Computer Applications ―A comparative analysis on Risk Assessment information security models", Volume NO.82 Number 9 (2013).