Proceedings of the 28th IEEE
EMBS Annual International Conference
New York City, USA, Aug 30-Sept 3, 2006

Modeling Risk in Distributed Healthcare Information Systems

Ilias Maglogiannis

IEEE Member

Elias Zafiropoulos

***Abstract*—This paper presents a modeling approach for performing a risk analysis study of networked Healthcare Information Systems. The proposed method is based on CRAMM for studying the assets, threats and vulnerabilities of the distributed information system, and models their interrelationships using Bayesian Networks. The most critical events are identified and prioritized, based on "what – if" studies of system operation. The proposed risk analysis framework has been applied to a healthcare information network operating in the North Aegean Region in Greece.**

***Index Terms*— Distributed Healthcare Information Systems, Telemedicine, Risk analysis, Bayesian networks, CRAMM.**

I. Introduction

Nowadays, computer and network based systems are expanding in order to support more healthcare activities, especially in isolated regions (i.e. isolated areas in Greece, in Scandinavian Countries and in Germany), where there is often no availability of central general hospitals [1] [2]. Networked healthcare information system can fill this gap, connecting local healthcare service providers with central regional and/or peripheral hospitals and thus making possible tele-consultation, tele-diagnosis and exchange of views between remote located doctors in certain patient treatment cases [3], [4]. Similar concerns are also encountered in healthcare networks of medical organizations and hospitals, where a large number of employees and staff access the network and data resources.

Furthermore, medical data maintained in health information systems is directly related to the patients' health and safety. According to the Recommendation No. R (97) 5 on the Protection of Medical Data issued by the Council of Europe, appropriate technical and organizational measures must be taken to protect personal data against any accidental or illegal destruction, accidental loss, as well as against unauthorized access [5]. These possible threats can damage severely health information system reliability and discourage professionals of future use. Therefore, the execution of a risk analysis is a necessity in order to assure a health information system's safety and Quality of Service (QoS).

This paper proposes a risk analysis method for distributed healthcare information systems. The UK Central Computer and Telecommunications Agency (CCTA) Risk Analysis and Management Methodology (CRAMM) has been applied for identifying the information system's asset values, threats, vulnerabilities and the corresponding risks [6]. Initially, the user services, offered by the healthcare information system and identified by the CRAMM methodology, are modelled as a Fault Tree representing the logical interrelationships of failure events that may lead to a hazardous condition [7], [8].. Finally, these relationships are represented using an advanced Bayesian Network model that provides greater flexibility in modeling failure event scenarios and highlighting system critical areas [9], [10], [11]. The proposed method has been applied to a networked healthcare information system operating in the North Aegean Region in Greece, providing the basic services of teleconference, medical reporting, medical records retrieval and analysis and patient telemonitoring.

I. Maglogiannis and E. Zafiropoulos are with the University of the Aegean, Dept. of Information and Communication Systems Engineering, 83200 Karlovasi, Samos, Greece. e-mails: imaglo@aegean.gr, eliaszafir@aegean.gr).

II. General aspects Of The Risk Analysis Model

Risk analysis involves the identification and assessment of the levels of risks calculated from the known values of assets and the levels of threats to, and vulnerabilities of, those assets [8]. In the proposed risk analysis method, the main steps of the CRAMM methodology have been adopted. CRAMM is owned, administered and maintained by the Security Service on behalf of the UK Government. Specifically, the CRAMM methodology is organized in three main stages. Firstly, system assets are identified and categorized as data, application software and physical assets (equipment, buildings, staff). Data assets are valued in terms of their impacts on breaches of confidentiality, integrity, availability and non-repudiation, which are the widely accepted principles of information security. Application and physical assets are valued in terms of their unavailability, replacement or reconstruction cost. The likely threats and known vulnerabilities are quantified against selected asset groups, while their likelihood of occurrence is estimated using predefined levels of threat and vulnerability (e.g. "Very Low", "Low", "Medium", "High", "Very High"). Finally in order to manage the identified risks, a set of countermeasures applicable to the information system is produced.

Fault Trees are very popular in dependability modeling, system reliability analysis, evaluation of large safety-critical systems and graphical representation of cause-effect

relationships in risk analysis [6], [8]. However, current studies showed that mapping Fault Trees into Bayesian Networks provide greater flexibility for studying local conditional dependencies into the system model, modeling events with more than two possible states, common cause failures, sequentially dependent failures and therefore contribute significantly risk prioritization [9], [10], [11].

In the context of the present risk analysis method, the use of Bayesian Networks provide a concise graphical representation of the cause-effect interrelationships among threats, vulnerabilities and assets in the risk analysis of information systems, while the conditional dependencies among the events and the probabilistic inference of the Bayesian Network aim significantly in a more realistic risk prioritization of the undesirable events for system safety. Furthermore, the importance measures of the Fault Tree method are calculated arbitrarily of the existence or not of the top event or any other possible evidence for the tree events. However, the conditional probabilities given the existence or not of certain events incorporate this evidence in their calculation and result in a more realistic ranking of primary events [10], [11].

III. Implementation Of The Risk Analysis Method

The risk analysis of the Healthcare Information System (HIS) has been performed by experienced CRAMM-certified risk analysts, in accordance to the guidelines of the CRAMM methodology. However, several key persons of the service provider have actively participated in the study by providing, through interviews or questionnaires, the information required by the analysts. It should be stressed at this point, that the risk analysts have presented the results of each stage to the management of the HIS, in order to get their agreement and also obtain their permission to proceed with the analysis. The networked HIS under study is depicted in Figure 1.

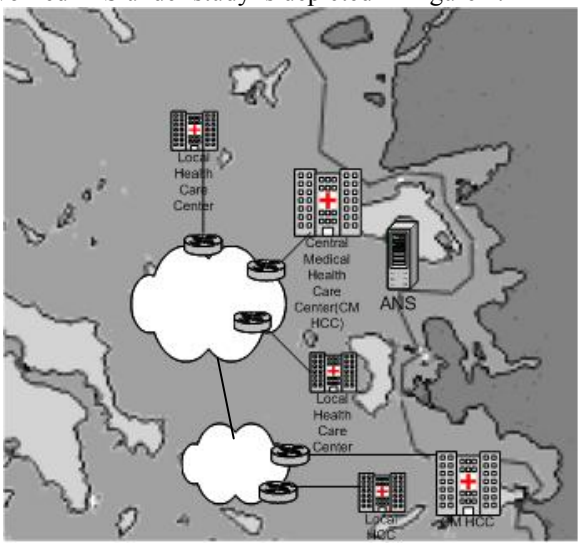

Fig. 1 The Healthcare Information Network in the North Aegean Region under study

The first stage of the risk analysis comprises of the identification and the valuation of the information system's assets. Valuation concerns the data and critical information managed by the system, as well as the hardware and software applications used for the provision of medical service. The risk analyst decides the level of granularity for the identification of the information system's assets, in accordance to the CRAMM guidelines. However, the main approach is to identify, as distinct assets, all data categories that may disrupt the user service if their availability, confidentiality or integrity is compromised. The hardware and software assets are those associated with the aforementioned data categories and thus with the offered user service. The valuation was performed on the basis of the possible impacts that a threat may cause to the requirements of medical services provision by the HIS.

A. Data and Hardware Assets

It should be noted that since the networked HIS deals with medical data (confidential information) security, trust and reliability are system's key 'services'. Therefore, a security incident is not just an internal problem (replacement cost) but has an immediate effect on the trust of patients to the system and thus to the system's capability to offer reliable Healthcare Services. Therefore, the data valuation was done by estimating the impact that could be caused by the loss of data availability and/or data confidentiality and/or data integrity, always considering the worst case scenario. The identified data assets were categorized into the following classes: *Patient Medical Records, Encoded Medical Data, Reporting Data, Voice-Log Data*.

B. Hardware and Software Assets

The hardware assets required for the successful operation of the HIS are:

1. Application Network Server (ANS). This is the main network host station that stores the patient medical records and facilitates their decoding and monitoring through specialized monitoring software. In addition, it supports logging of all communications among the doctors, hospitals, or patients.
2. Printers. These are color inkjet printers for printing graphs and laser printers for printing reports and letters.
3. Backup Media. These are magnetic tapes for back-up of the data stored on the ANS.
4. Internet Line. This is the line used for the applications traffic and the IP telephony.
5. Communication Protocol. This will be the TCP/IP protocol that will be used for any type of communication.

The software assets required for the provision of the Healthcare Information System are the following:

1 Medical Record Software. It is utilized for maintaining and processing the electronic medical records of the patients.

2 Patient Telemonitoring Support Software. It constitutes an application that both collects biosignals from patients under constant surveillance and sends them to other locations where medical personnel exists and receives the corresponding information from peer workstations.

3 Logging Support Software. It facilitates the maintenance of a log file of most communication through the network. It

also supports recording of voice communication and filing of electronic documents and emails that may be exchanged.

4 Teleconference Support Software. It supports the teleconference application and it can be modeled as a VBR (Variable Bit Rate) traffic profile.

5 Database Transaction Software. It supports electronic health records retrieval and security.

C. Evaluation of the threats

The next step is the evaluation of the threats that the system is facing, as well as the identification of the vulnerabilities that may allow some threats to occur. These, in turn, will provide us with the security-related needs of the users. The evaluation of threats and vulnerabilities in conjunction with the system's asset valuation are used to calculate the risk level of each system asset. A list of threats is presented in Table I and can be analyzed further down to more detailed causes.

The basic services that constitute the successful system operation are identified and their unavailability is analyzed to its causes in a top-down approach (Fault Tree model), using logical AND-OR gates to model the causality. In the present case study, the basic services are: *Teleconference, Patient Telemonitoring, Medical Records Retrieval, Reporting Service*. The specific details about each one of them have been given previously. The unavailability of any of these services will lead to the HIS failure to satisfy the specifications, which is a fact depicted by the logical-OR gate of Figure 2.

TABLE I.
HEALTHCARE INFORMATION SYSTEM THREATS

Threat	User Need
1. Masquerading	Authentication
2. Unauthorized Use of an Application	Authorization
3. Introduction of damaging or Disruptive Software	Viral Software prevention
4. Misuse of System Resources	Controlled use of resources
5. Communications Infiltration	Confidentiality
6. Theft	Staff integrity
7. Willful Damage	Staff integrity
8. Technical Failure of Network Interface	Technical support
9. Technical Failure of Network Services	Service provision
10. Power Failure	Power supply availability
11. System or Network Software Failure	System quality
12. Application Software Failure	Testing and quality
13. Operations Error	Operations control
14. Hardware/Software Maintenance Error	Technical support
15. User Error	Verification
16. Fire	Fire prevention
17. Water Damage	Flood prevention
18. Natural Disaster	"Acts of God" prevention
19. Staff Shortage	Staff availability

The four basic services can be further decomposed down to the events leading to their unavailability, using the findings of the CRAMM analysis. The events that are no further decomposed are considered far beyond the scope of the present analysis. The developed Fault Tree is mapped into a Bayesian Network, where the conditional probability tables of the child nodes are constructed based on the Boolean logic of the AND – OR gates i.e. a child node representing an AND node will be in the 'True' state if and only if all the parent nodes are in the 'True' state. The threats identified during the CRAMM risk analysis can be categorized according to their probability of occurrence in five different levels, characterized as "Very Low", "Low", "Medium", "High" and "Very High", while each of these levels can be described by three different sublevels. The engineering expertise acquired during system operation as it is expressed by the information acquired during interviews and questionnaires, and the existing specification reliability data for the hardware threats aim significantly in the estimation of their probability of occurrence. These values can be used in the Bayesian Network model of the information system in order to estimate the posterior probabilities of failure events during certain scenarios of system operation. Risk prioritization of the threats can be based on these "what-if" studies since their likelihood of occurrence is estimated given the occurrence of an undesirable event for system operation.

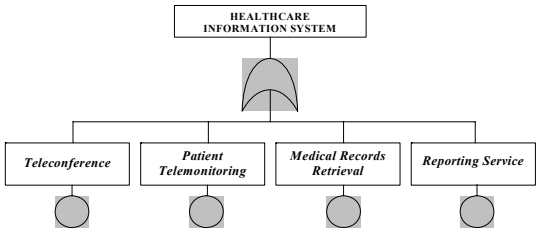

Fig. 2: A simple Fault Tree model of an OR gate for the HIS top services.

IV. RESULTS AND DISCUSSION

The Bayesian Network model has been implemented using the Bayes Net Toolbox for Matlab, available at: http://bnt.sourceforge.net/. Using the Bayesian Network semantics, the most critical threats can be identified, given the fact that the HIS has failed, by calculating the posterior probabilities of the node-states. The four basic services of the HIS can be further investigated, by assuming that each one has failed and calculating the posterior probabilities of occurrence for the threats. These "what –if" studies have been executed, the top five threats have been ranked according to their posterior probabilities of occurrence and the results are depicted in Table II.

The most critical threat for the HIS and each of the basic services is the power failure of the server, while the power failure of the Workstation is the second most critical failure for the HIS. The deficiency of power supply is mainly rooted from sudden interruptions or low power quality (high harmonics of load current, voltage sags etc), which are usual phenomena in islands or areas isolated from the main power grid. A possible countermeasure for power failures is the use of a UPS in combination with a small generating unit on the single site of the server, while the workstation power supply reliability can be improved by the use of a UPS since it is characterized by an acceptable cost.

TABLE II.
THE HIGH RISK THREATS FOR THE HEALTHCARE INFORMATION SYSTEM AND ITS BASIC SERVICES IDENTIFIED USING THE BAYESIAN NETWORK MODELING AND THE FINDINGS OF THE CRAMM ANALYSIS

HEALTHCARE INFORMATION SYSTEM SERVICES				
Teleconference	**Patient Telemonitoring**	**Medical records retrieval**	**Reporting service**	**HEALTHCARE INFORMATION SYSTEM**
− Power Failure of ANS	− Power Failure of ANS	− Power Failure of ANS	− Power Failure of ANS	− Power Failure of ANS
− Power Failure of Workstation	− Power Failure of Workstation	− Power Failure of Workstation	− Power Failure of Workstation	− Power Failure of Workstation
− System and Network Software Failure of ANS	− System and Network Software Failure of ANS	− Air-condition failure of ANS	− Air-condition failure of ANS	− System and Network Software Failure of ANS
− Air-condition failure of ANS	-Telemonitoring application software failure	− -Masquerading user identity	− User error in log support software	− Air-condition failure of ANS
− Communication Infiltration	-User error in telemonitoring application	− System and Network Software Failure of ANS	− System and Network Software Failure of ANS	− User error in log support software

The implementation of these countermeasures will significantly limit the vulnerability of the system by the air-conditioning failure, as well. Furthermore, high-risk threats for the HIS are "system and network software failure of ANS", "User error in log support software", "Telemonitoring software failure" and "masquerading user identity".

A possible countermeasure to combat the security related threats is the extensive implementation of verification and validation procedures during the development and maintenance of these software units, which should be also applied periodically during the field operation of the HIS, in order to detect any deviations timely and calibrate the system accordingly. Moreover, another possible countermeasure is the periodic backup of the medical data and patients' records managed by the server for a quick and reliable restoration in case of a possible software failure and loss of data.

In Table II, there are a number of high-risk threats related to the human factor, such as user errors in using the software assets of the HIS and "Masquerading the User Identity" during system operation. These threats may result in erratic input to the system and deterioration of system confidentiality, which may discourage physicians and patients of further use. There are a number of possible countermeasures to limit the vulnerability of the HIS to these threats, such as proper training of the users and enhanced security options for network operation.

V. CONCLUSIONS

An improved risk analysis method has been presented that combines basic features of the CRAMM risk analysis framework with the Bayesian Network modeling technique in order to identify assets, threats and vulnerabilities of Healthcare Information Systems (HIS) and present these interrelationships in a concise and flexible model. A case was presented and the HIS assets, threats and vulnerabilities have been thoroughly analyzed using the basic features of CRAMM. The findings of the analysis have been used to develop a Bayesian Network model to rank the threats with the highest risk, based on their posterior probability of occurrence in the case of the basic services and system failure. The highest risk threats were identified and several countermeasures were suggested in order to limit the vulnerability of the healthcare network operation to these threats.

VI. REFERENCES

[1] Park S. et al. Real-time monitoring of patient on remote sites. Proc. 20th Annual Int. Conf. IEEE EMBS, vol.20, no.3, pp. 1321-1325, 1998.

[2] Reponen J, Marttila E, Paajanen H, Turula A., Extending a multimedia medical record to a regional service with electronic referral and discharge letters, J Telemed Telecare. 2004;10 Suppl 1:81-3.

[3] Yang B., Rhee S., and Asada H. H. A twenty-four hour tele-nursing system using a ring sensor. Proc. 1998 IEEE Int. Conf. Robotics Automation; 1998, pp. 387-392.

[4] Andreasson J et al.. Remote system for patient monitoring using Bluetooth/spl trade. Sensors, 2002. Proceedings of IEEE, pp. 304 -307 vol.1 June 2002

[5] Council of Europe, Recommendation No. R (97) 5 of the Committee of Ministers to Member States on the Protection of Medical Data (1997). Available at http://www.cm.coe.int/ta/rec/1997/word/97r5.doc.

[6] UK Security Service. CRAMM: the UK Government's Risk Analysis and Management Method.

[7] Shooman M.L. Reliability of Computer Systems and Networks. John Wiley & Sons, Inc., 2002.

[8] Modarres M., Kaminskiy M., Krivtsov V. Reliability Engineering and Risk Analysis. Marcel and Dekker Inc, New York, 1999.

[9] Jensen V. Finn. Bayesian Networks and Decision Graphs. Springer-Verlag, New York, 2001.

[10] A. Bobbio et al., Improving the analysis of dependable systems by mapping fault trees into Bayesian networks, Reliability Engineering and System Safety 71 (2001) 249-260.

[11] Ha J. S., Seong P. H.. "A method for risk-informed safety significance categorization using the analytic hierarchy process and Bayesian belief networks". Reliability Engineering and System Safety 83 (2004) 1–15.