International Journal of Security and Its Applications
Vol.9, No.8 (2015), pp.205-210
http://dx.doi.org/10.14257/ijsia.2015.9.8.17

A Dependency analysis for Information Security and Risk Management

B. Chaitanya Krishna[1], Kodukula Subrahmanyam[1] and Tai-hoon Kim[2]

[1]*Department of Computer Science and Engineering,*
K L University, Andhra Pradesh
chaitu2502@kluniversity.in, smkodukula@gmail.com
[2]*Department of Convergence Security, Sungshin Women's University,*
249-1, Dongseon-dong 3-ga, Seoul, 136-742, Korea
taihoonn@daum.net
(Corresponding Author)

Abstract

Today major issue in IT Sector is security, now a day in every field software products are using at the same time users are struggles for their information and data security. Normally software engineers developed good software and test the all aspects and deliver to the user but they cannot bother about minuet problems because they think that those problems cannot impact the product output. But in the run time environment those problems create major problems and display the wrong outputs. Software hackers also using these minuet problems hacked the system and spoil the data. There are so many methods are available for information security and risk management but those are not universally accepted methods. In this paper I proposed a novel method for information security and risk management. Using this method to develop application very well and if any hidden mistakes are there in development stage those risks are identified in run time environment and reduce risk and provide security to the data.

Keywords: *Risk, security, information systems security, risk management, software products, hackers*

1. Introduction

Now a day's software industry facing major problem is information security and risk management, the software project quality is depends upon the risk management issues. 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. Normally the information security begins with computer security, which is to provide security physical locations, hardware and software from threats. In physical locations and hardware we provide security 98% accuracy because these are development and maintaining team take care so those are have the good security but major problem is software i.e. data or information regarding project these are various forms like raw data, system data, user data, members data, development programs etc.

The progress toward security that went beyond protecting physical locations began with a single paper, which attempted to define the multiple controls and mechanisms necessary for the protection of a multilevel computer system. Here all possibilities in the given project and is now considered to be study of computer security.

Today, the Internet uses millions of unsecured computer networks into continuous communication with each other. The security of computer's stored information is now contingent on the level of security of every other computer to which it is connected. Recent years have seen a growing awareness of the need to improve information security, as well as a

ISSN: 1738-9976 IJSIA

realization that information security is important to international level. The growing threat of cyber attacks has made governments and companies more aware of the need to defend the computer-controlled control systems of utilities and other critical infrastructure. There is also growing concern about nation-states engaging in information warfare, and the possibility that business and personal information systems could become casualties if they are undefended.

2. Risk Management

Risk management can be defined as identify, analyze, evaluation, control, and avoidance, reduce, or eliminate the unacceptable risks. 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 R_i can be defined as R_i= function (probability, impact). A common procedure to identify risk is sequential process. Each and every individual component will check and identify the risk. Using modern technology identification of risk is small issue but IT people more careful about to dependency risk that means if once we identify the risk depending upon the risk what impact is going on and if any changes are there in remaining un checking project files all are identify and reduce risks.

In real world user may not think about dependency risks. For example user is working with a product he may face an error, due to in work busy he may overlook the problem and tried for alternative paths to do the things. In this case a new error erases due to neglecting the previous error. Dependency risks are more harm full sometimes entire system works in negative directions. Robots manufacturing process dependency risks place major role. If we develop hundred percent risk free IT products automatically we provide efficient information security product.

2.1. Risk Management Process

The Software Engineering Institute (SEI) has developed a risk management paradigm, which is an elaboration of the classic plan. Here to check risks and act according to the risk, it is cyclic process and specifies a set of cyclic steps i.e., Identify, Analyze, Plan, Track, Control, minimize risks throughout an IT project. It indicates that 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

2.2. Dependency Analysis

Current risk management practices do not clearly address how dependencies between risks are managed. In this section, we review several dependency risk analysis that have been used to represent the dependency of one task event to another. All models are not suitable for all IT products and they are qualitative models. That means we cannot estimate risk exactly, in existing engineering models to estimate the risk based on the assumptions we cannot say exactly, the estimation person to person will be changed.

There are three common tree-based analysis techniques. First, fault tree is a logical graph 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.

Table 1. Various Dependency Analysis Models Summary

Models/Techniques	Characteristics	Applications
Fault Tree	Tree Structure (acyclic)	Used to analyze possible causes of undesired events
Event Tree Analysis	Tree Structure	Used to analyze dependencies between different knowledge components
Cause-Consequence Analysis	undesired event and develops backward to identify its causes (presented by a fault tree) and forward to identify its consequences	Used to manage uncertainty by explicitly presenting the conditional dependencies.
Markov Analysis	Directed graph structure, A mathematical method	Used to analyze the reliability and availability of a system
Bayesian Network	Directed acyclic graph structure	Used to manage uncertainty by explicitly presenting the conditional dependencies between different knowledge components

Second, Event Tree Analysis (ETA), in this method it 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.

Third, 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.

Fourth, 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.

Last, 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.

3. Proposed Method

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

1. In this model first read the entire product individually
2. Identify Each individual component risk and risk factor using mathematical approach
3. Depending upon the risk identify the any dependency risk and estimate the exact risk factor.
4. Depending upon the individual component risk factor identify the dependency risks in existing project.
5. According to the risk factor, to display possibilities to minimize the risks of the project or automation or application.
6. After minimized risks once again to check the risk factor of product it is below 10%, calculate RL function otherwise repeat step 3 and 4.
7. Find out RL function value if it is below 8% the proposed method says it efficient software.

4. Results and Comparison

Based on the Novel Approach of the sample system, here I considered sample system is Health automation. Why I considered Health automation, if health automation developed risk free product then only is use and considered their results otherwise the impact is one human life so I applied Novel approach model to health automation. Here given result according to the proposed method.

Table 2. Risk Assessment Results based on Novel Approach Model

S. No	Module Name	Risk value	Risk Effect (%)	Dependency Effect (%)	Remedies
1	Login	30	80	25	Checking
2	Patient previous data	20	50	35	Patient money waste and Understand patient problem
3	Patient live Records upload	20	70	40	Confirmation
4	Doctors module give proscription	10	75	80	Good Interaction and Interface
5	Doctors update patient data	5	75	75	Understand problem
6	Receptionist enter patient records	5	80	80	Checking and confirmation
7	Network failure	5	80	75	Checking and understand
8	Power failure	5	60	60	According to situation react
9	Data entry module	5	80	80	Checking and confirmation
10	Guest user	7	10	10	Understand

5. Conclusion

Risk identification and security management in IT sector is continuous process to manage risks in this paper proposed method is quantitative analysis. A quantitative analysis will determine the probability of each risk event occurring. For example, Risk#1 has an 80% chance of occurring; Risk#2 has a 27% chance of occurring, and so on. Using this model identify the risks in existing products and make the product efficient and convert more reliable software.

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] A. Appari and M. E. Johnson, "Information security and privacy in healthcare: current state of research", International journal of Internet and enterprise management, vol. 6, no. 4, **(2010)**, pp. 279-314.
[3] S. Tyali and D. Pottas, "Information Security Management Systems in the Healthcare Context", proceedings of the South African Information Security Multi-Conference: Port Elizabeth, South Africa, 17-18 May 2010, pp. 177.
[4] Economic Commission for Africa (1999), "Information and communication technology for health sector", pp.8. http://www.uneca.org/aisi/docs/pfshealth.pdf, (Accessed 15 June 2008).

[5] ISO/IEC 27001: Information Technology, "Security Techniques – Information Security Management Systems – Requirements", 1st edition, Switzerland, International Organization for Standardization.
[6] ISO/IEC 27799: Health informatics, "Information security management in health using ISO/IEC 27002", 1st edition, Switzerland: International Organization for Standardization, (**2008**).
[7] International Electrotechnical Commission, "Analysis Techniques for System Reliability: Procedure for Failure Mode and Effects Analysis (FMEA)", International Electrotechnical Commission, (**2006**).
[8] K. B. Chaitanya, K. Subrahmanyam, Y. Sai Ramya, G. K. Swamy, M. Rajesh and M. Siddardha, "A Novel Approach For Information Security and Risk Management In Distributed Health Care Systems", International Journal of Applied Engineering Research, vol. 10, no. 4, (**2015)**, pp. 645-650.
[9] N. Srinivasu, K. V. D. Kiran, V. Phani Krishna, and L. S. S. Reddy, "Risk Assessment in Distributed Banking System", International Journal of Applied Engineering Research, vol. 9, no. 19, (**2014**), pp. 6087-6100.
[10] K. V. D. Kiran, LSS Reddy and N. Lakshmi Haritha, "A Comparative Analysis on Risk Assessment Information Security Models", International Journal of Computer Applications, vol. 82, (**2013**), pp. 41-46.

