Software Security: A Risk Taxonomy

Kavita Sahu[1]
Department of Information Technology
Babasaheb Bhimrao Ambedkar Central University
Lucknow, India
kavi9839@gmail.com

Rajshree[2]
Department of Information Technology
Babasaheb Bhimrao Ambedkar Central University
Lucknow, India
rajshree.bbau2009@gmail.com[2]

Abstract— The implementation of software has been challenging for many organizations. As given in the many reports of important failures, the implementation of packaged software and associated changes in business processes has proved not to be an easy mission. As many organizations have discovered, the implementation of software's systems can be an enormous disaster unless the process is managed cautiously. By calculating and minimizing the major business risks in the first illustration, the scene can be set for the successful performance of software's organization. Almost every software controlled system faces risk from potential adversaries. Software engineers must be cognizant of these security risk and engineer systems with probable defenses, as still delivering value to customers is priority of an organization.Software security risk management and security assessments essentials reproduces several influences. The maximum documentation arrival on security holders encloses the value to customers. In this paper there is a focus on another face of software security risk analysis which connects to arranging software in the market that assists as an intermediate between a software provider, society and its clients.

Keywords- Software Security; Security Risk; Risk factors; Risk Management; Risk Taxonomy

I. INTRODUCTION

Given the definition of risk as the possibility for an occurrence to ensue, the monitor and control of risk process involving: the estimation of risk factors which are likely to be important; and, the management of risk by estimating and prioritizing the probability of the event and its impact on the project [3].Software risk management is connected to the numerous helpful injuries that could be possible on the security of software due to some insignificant or unclear faults in software development task [15, 17]. Software developments have an amazing coincidental of dissatisfaction of that security so effective software development worth dealing with risks sufficiently. Risk management is the furthermost significant concern complexity in the software project development. This concern is usually accomplished by Software Security Management. During the software development life cycle of projects, numerous risks are connected with them. These risks in the software development is acknowledged and achieved by security risk management. Specific of the significant personality of risk management in software security are software security risk management, software security risk classification and strategies for risk management in software security [2, 5].

Software risk analysis resolutions precede testing one stage additional by classifying unidentified faintness subsequent from extraordinary harshness engineering defects in multi-tiered organizations. Software risk includes the possibility of existence for undetermined proceedings and their prospective for loss within an association. [4] Risk management has developed an essential factor of software development as organizations remain to tool extra presentations diagonally a multiple technology, multi-tiered surroundings. Analysis clarifications considered to discover these concerns before effecting deliver a chance to evaluate potential incidents and avoid difficulties before they obviously become specious. Software risk identification is domineering to commercial procedures in a difficult IT environment. Accurate analysis puts a business onward of the arc by allowing for initial documents of substructure threats and providing the data one essential to well accomplish them.[9]Recent developers and researchers need a better taxonomy which will helpful in estimating security risk earlier hence here a taxonomy is presented. In this paper, we discussed about security risk and given a new taxonomy of software security risk which is helpful in the area of software security development.

II. SOFTWARE SECURITY RISK

Software companies have much at stake in protecting their valuable intellectual belongings. Software protection techniques aim at developing procedures that defend the integrity of data and software, used on untrusted systems, from engineering and malevolent modifications. Agreeing such methods can nasty the modification between industry existence and interruption [8,15].Software security is a zone of developing significance in software engineering and security: innovative researchers have industrialized several revolutionary methods for

inhibiting or counter attack software piracy and damaging, building a dissimilar body of information covering unalike topics: disorientation, information smacking, reverse engineering, code transformation, operating systems, networking, encryption, and trusted computing. The technology and data attacks are maximizing the need of software security. The orderly development of software that considers security risks and threats clearly is increasingly predictable as critical to improving the overall software security [4]. Numerous establishments agonize from failed systems even when an enormous quantity of time and money are devoted to well-designed testing approaches. The functional methodology does classify nearly 90% of the faintness that origin system failures; conversely, it does not justification for a smaller amount specious issues skilled of disturbing reply times, organization constancy, and constituent functionality issues between use sheets. Software risk of security is two of the essential enactment disclaimers within the security management procedure conventional. The security regulation does not hypothesize precisely how a security risk analysis should be engaged.

The publication suggestions an inclusive methodology to include risk management into the software or project development life cycle [12,13]. Threats in the atmosphere are recognized, and then security vulnerabilities in software are evaluated. Intimidations are then matched to susceptibilities to designate security risk. The document encloses a description of the types of several societies in security risk analysis and management. It highlights the significant character senior management productions in appreciative security risk, creating way, and providing properties. Organizations necessitate conveying accountability to the security authorized for the improvement and execution of security strategies and techniques.[11,14] This discrete may lead the side that essentially accomplishes the risk analysis, do considerably of the procedure and technique inscription, and commend or even select numerous of the controls and monitors. The circumstance that classifies the foremost information officer, software and owners, business and functional superiors, information technology security analysts recognizes the significance of a team that encompasses beyond information technology and includes customers [16, 18]. In a scientific situation, customers of systems not only can contribute in providing software and data criticality information, but necessitates also elaborating in influential which mitigation approaches will work.

III. COMMON RISK FACTORS

After evaluating the answers gathered from our analysis program and applying them to our three areas of threat profile, hazard occurrence, investigation and general risk factors, they are allocated to the asset or the components of the asset. When all available data about each identified risk has been collected, each risk will be rated without consideration to any countermeasures. This produces a list of risks. A separate list will be produced taking in account current. [5, 19]This will help show how current countermeasures are impacting the asset by reducing the risks. General risk factors that might be used in the initial approach could be:

A. Confident

The event will happen. There are no used passwords on an unattended software design in an open zone will at some time permit an unauthorized consumer access.

B. Extraordinary

The potential for the event occurring is much countless than that the potential for the event not happening. For a sample, recognized and described bugs in the software or system where accessible covers have not been fixed; the software certainly exists to an enormous number of consumers.

C. Sensible

The event is more likely to succeed than not to occur. For a sample, unauthorized access to a system or software on a complex even with the procedure of a password may existent a worry.

D. Partial

The event is less probable to happen than not to succeed. For a sample, unauthorized access to a system or software on a complex protected by passwords.

E. Unidentified

Not sufficient information of data is available to estimate. For a sample, complexity with a new type operating system or system software that has not been completely confirmed.

IV. SOFTWARE SECURITY RISK MANAGEMENT

Meanwhile there could be numerous risks interrelated with the security of software development projects, the key to classify and accomplish individual's risks is to distinguish about the theories of security risk management [21, 17]. Numerous conceptions about security risk management could be renowned but the maximum noteworthy are security risk analysis, security risk index and security risk assessment.

Figure: Risk Management of Software Security in Development Process

A. Security Risk Index

Mostly risks are characterized into two issues namely influence of security risk procedures and possibility of incidence. Security risk index is the development of influence and possibility of incidence. Security risk index can be described as high, medium, or low dependent upon the creation of back-up and occurrence. Security risk index is significant and essential for prioritizing of security risk.[6]

B. Security Risk Analysis

There are quite miscellaneous categories of risk analysis that can be used. Essentially, risk analysis is used to classify the extraordinary risk fundamentals of a development project in software engineering. Equally, it suggests methods of identifying the impact of risk mitigation and modification methodologies. Security risk analysis has also been fixed to be dangerous noteworthy in the software security design to assess criticality of the system, where security risks are examined and vital security procedures are improved. The main determination of risk analysis is to recognize risks in better ways and to authenticate and correct security attributes. An effective risk analysis contains significant fundamentals related difficult explanation, challenging formulation, data collection.[6]

C. Security Risk Assessment

Risk assessment is substitute significant case that assimilates risk management and risk investigation of software security. There are numerous risk assessment methods that inspiration on various types of risks. Risk assessment needs truthful clarifications of the separate software and all security constructions. It is momentous that risk significant elevations similar to presentation, cost, nourishment and schedule necessary be perfect appropriately for risk assessment to be commercial.[6]

V. RISK TAXONOMY IN SOFTWARE SECURITY

The noteworthy determination of classifying risk is to improve a combined perception on assembly of security factors. These are the classifications of security factors which will provision software improvement project administrators to categorize the bunch that countersigns the tough risk. A top and furthermost systematic technique of prospective risks is to classify them based on risk individualities. Risk taxonomy is reflected as well-organized technique of studying risks and their foundations by arrangement of analogous risks together into modules. Software risks could be confidential as internal or external security complexity. Those security risks that consequent from features of security risk within the suggestion are called interior risks although the exterior risks plagiaristic from available of the relationship and are problematic to controller.[14,11] Interior risks are developing plan, product, process risks. Exterior risks are frequently industry with the commercial, technical risks, consumer's satisfaction, and rigid immovability. There are numerous security risks in the software engineering which is actual challenging or difficult to identify all of them [19, 21]. Some of greatest significant security risks in software engineering project are classified as software security requirement risks, software security cost risks, software security scheduling risk, software security improving quality risks, and software security business risks. These risks are described with their features below.

A. Software Security Requirements Risks

The objective of improvement is to distribute software which happens the security necessities of the software or system consumers. Software security improvements are regularly non-failure. Because the erroneous mechanism is constructed and prerequisites to be improved. No one knows the full security requirements at the start of project. Developer can truly know the requirements when it has completed the project. Hence it becomes the rise of software security requirements risks which are listed below:

- Deficiency of analysis for change of security requirements.

- Change postponement of security requirements
- Deficiency of report for security requirements
- Poor definition of security requirements
- Ambiguity of security requirements
- Change of security requirements
- Inadequate of requirements
- Impossible security requirements
- Invalid security requirements

B. Software Security Cost Risks

Software security cost risks are the risks that the project security costs extra than considered. It can principal to performance risk if cost attacks major to decreases in possibility or worth. Some major security related cost risks are listed below:

- Deficiency of good estimation in development projects
- Doubtful schedule of security
- The hardware does not work well
- Social errors
- Deficiency of security testing
- Deficiency of monitoring of software security
- Security complexity of architecture
- Large size of software architecture
- Additional requirements change in security
- The implements does not effort glowing
- Personnel, management and environment modifications.
- Deficiency of reassessment of management cycle

C. Software Security Scheduling Risks

Software security scheduling risks are a risk which takes the project time longer than scheduled. It can too primary to cost risks, as extended projects continuously cost added than predictable. Software security scheduling risks are programmed below to understand their nature:

- Insufficient software security budget
- Change of security requirements and extension of security requirements
- Social errors
- Insufficient knowledge about tools and techniques of software security
- Long-term training of security for personnel
- Deficiency of employment of manager experience in security
- Deficiency of enough ability of security
- Deficiency of good estimation in development projects

D. Software Security Improving Quality Risks

Software quality is very important in today's competitive world. It is a critical control on software projects. Quality is directly dependent on software processes hence managing quality risk is an important challenge when designing security. When designing security some quality risks which should be considered as critical are listed as:

- Inadequate software security documentation
- Deficiency of development standard
- Deficiency of design or OO design documentation
- Inadequate budget of security
- Social errors
- Improbable schedule of security
- Extension of requirements change in software security

- Neglected definition of security requirements
- Deficiency of enough ability of security
- Deficiency of security testing and worthy estimate in development projects
- Inadequate understanding about methods of security, programming language, implements, tools and so on.

E. Software Security Business Risks

To be effective, several test risk dimension has to deliberate on the native specific issues related to the commercial. Throughout the test risk dimension process, security risks to industry tasks will be recognized and estimated. Security business risk are associated with the risks which concentrates on the following factors:

- The products that no one want them
- The products that are not suitable with total strategy
- The products that sellers do not know how to advertise them
- Breakdown in total financial plan
- Breakdown in assurance
- Breakdown in management because of change in different group of people

VI. STRATEGIES FOR RISK MANAGEMENT IN SOFTWARE SECURITY

During the software improvement practice several strategies for risk management of security could be recognized and defined permitting to the amount of risk encouragement. Founded upon the quantity of risk encouragement in software increase scheme, risk strategies could be distributed into three classes namely cautious, flexible, and classic. Usually, suspicious risk management approach is projected for new and inexpert establishments whose development projects are related with new and unconfirmed technology;[7,5]characteristic risk management strategy is definite as a maintenance for established organizations with understanding in software development projects and used equipment, but whose software projects carry apparel number of risks;[18] and flexible risk management approach is involved in proficient software security development establishments whose development projects are formally defined and based on established equipment. All development projects have some stages of security risk associated with them. Even if the software under enhancement is basically another version of an existing software or product, security risks may appear in parts such as:

• Changes in software or product development trainees (and consequential knowledge stages with the software or product)

• Changing market circumstances and customer prospects

• Changing business circumstances for the development society

The more one understand the risks, the better equipped he is to manage them. Risk and opportunity go hand in hand. Success cannot be achieved without some degree of security risk. Security risk is essential to progress, and interruption is often a key part of knowledge. But we must learn to balance the possible negative penalty of risk against the potential profits of its related unplanned failures. Risk is the probability of damage of software or security. It is a purpose of mutually the likelihood of a confrontational event happening and its impact. The impact discloses itself in a combination of monetary loss, time delay, and damage of performance. A risk is the originator to a problematic situation for some quantified dissimilarity in the software development life cycle; the projected aspirations cannot be accomplished within available properties. Risk cannot be excluded from a software development project. Risk management is dangerous to the victory of several software energy and is a planned characteristic of all software development projects.

VII. FUTURE WORK

Using a structured Taxonomy to help identify risk increases the likelihood of delivering usable systems or capabilities into secure use. Taxonomy based identification of risks may help developers to mitigate security risks at the early age of development. Future work in the field of this research will be to define each and every risk deeply so the developers and researchers may get help to develop new risk mitigation schemes and methodologies. In their current form, these databases over tantalizing yet ultimately inadequate information for the purposes of vulnerability discovery modeling. This work has sketched a design for a next generation of public vulnerability databases: the fleshing out and implementation of that design remain for future work. [4, 11] This assignment is perhaps the single peak significant one for accomplishing high quality, worthwhile estimates on susceptibility finding. Further work on economic approaches includes formally modeling the bug auction. The bug auction would be modeled as a sequential open first-price ascending auction with an unknown number of asymmetric independent private-value bidders, high entry costs, variable demand, and minimal bid

costs. A recognized prototypical could also be discovered to mitigate the risks using security attributes as it will be a cost effective method in developing a fully secure software.

VIII. CONCLUSION

Risk management of software security, risks taxonomy, and strategies for risk management are obviously designated in this paper. If risk management process of security is in domicile for each and every software improvement process then future difficulties could be minimized or completely eliminated. Hence, sympathetic numerous influences under security risk management process and directing on security risk management approaches clarified above could support in structure risk free software security in future. This analysis and assessment makes possible to estimate the risk of breakdown of software projects qualitatively and measurably. The process of risk analysis is constant and applies to many changed stages, at once classifying software design vulnerabilities, assigning prospects and impact, and determining reasonable improvement strategies. By considering the ensuing hierarchical risks, industry financiers can regulate how to manage particular security risks and what the furthermost cost-effective controls might be.

REFERENCES

[1] H. Hoodat, H.Rashidi, "Classification and Analysis of Risks in Software Engineering". World Academy of Science, Engineering & Technology, 56446-452. Retrieved from EBSCOhost, 2009.
[2] M. Boban, Z. Pozgaj, H. Sertic, "Strategies for Successful Software Development Risk Management", Management, Vol. 8, Issue 2, 2003.
[3] K. Sahu, R. Shree, "Risk Management Perspective in SDLC", International Journal of Advanced Research in Computer Science and Software Engineering, pp. 1247-1251 Vol. 4(3), 2014.
[4] Khan S. A., Khan R. A., "Securing Object Oriented Design: A Complexity Perspective", International Journal of Computer Applications, Vol. 8- no.13, October 2010.
[5] P. Zubcsek, I. Chowdhury, Z. Katona, "Information communities: The network structure of communication", Social Networks 38, P.P. 50–62, ©Elsevier B.V., 2014.
[6] S. Chandra and R. A. Khan, "Object Oriented Software Security Estimation Life Cycle: Design Phase Perspective", Journal of Software Engineering, USA, pp. 39-46, 2009.
[7] S. Sapkota, "Risk Management in Software Engineering", Advanced Software Engineering, Oct 20, 2011.
[8] R. Kumar, S. A. Khan, R. A. Khan, "Software Security Durability", International Journal of Computer Science and Technology, Vol. 5, Issue 2, pp. 23-26, 2014.
[9] Available at: http://www.castsoftware.com/research-labs/software-risk.
[10] Available at: http://nehanarang786.blogspot.in.
[11] Available at http://www.nap.edu/openbook.
[12] Available at http://www.byte-vision.com/MitigatingRiskWithAgile.
[13] Available at http://www2.latech.edu.
[14] Available at http://www.ieee-security.org/Cipher/PastIssues.
[15] Available at http://pdfcast.org/pdf/spm-2nd-assignment.
[16] Available at http://www.sqa.org.uk/e-learning/ProjMan01CD.
[17] Available at http://www.computer.org/portal/web/computingnow/swcfp2.
[18] T. T. Moores, R. E. M. Champion, "A Methodology for Measuring the Risk Associated with A Software Requirement Specification", AJIS, Vol. 4, Issues 1, pp. 55-63.
[19] S. V. Grabski, S. A. Leech, B. Lu, "Risks and Controls in the Implementation of ERP Systems", The International Journal of Digital Accounting Research Vol. 1, No. 1, pp. 47-68.
[20] SANS Institute InfoSec Reading Room, "A Perspective on Threats in the Risk Analysis Process", 2002.
[21] J. Venkatesh, C. Aarthy, "Threats in Implementation of ERP Applications", International Journal of Marketing, Financial Services & Management Research, Vol.1 Issue 7, 2012.