ISSN(Online): 2320-9801
ISSN (Print): 2320-9798

International Journal of Innovative Research in Computer and Communication Engineering

(An ISO 3297: 2007 Certified Organization)

Vol. 3, Issue 4, April 2015

A Survey on Different Software Security Attacks and Risk Analysis Based on Security Threats

D.Kavitha, S.Ravikumar

Assistant Professor, Dept. of C.S.E., Valliammai Engineering College, Anna University, Chennai, India

Assistant Professor, Department of I.T, Valliammai Engineering College, Anna University, Chennai, India

ABSTRACT: Security attacks play a major role in software. Attacks are classified in to active and passive attack some attacks are passive information are monitored whereas others are active information are altered. Attacks aims to exploit, destroy, and steal the authorized information. The main goal of software security is to protect confidentiality, maintain integrity and to ensure availability. The need of security is to identify the risk of threats and vulnerabilities in the software. The risk analysis is to identify the risk in the software the identified risks are analysed, accepted and managed. Vulnerability refers to the security flaw in the system that allows an attack to be successful. Threat includes spyware and malwares that can cause harm to the organization. The proposed work focuses on various types of security attacks are discussed in terms of information, hardware, hacker and software.

KEYWORDS: Threats, Vulnerability, confidentiality, Integrity, Availability, Security attacks.

I. INTRODUCTION

The software must be secure and it should function properly under malicious attack, so the practice of building software plays a major role and it incorporates the basic properties like confidentiality the authorized information should not be disclosed to the hackers, authentication it guarantees the information is authentic, and Integrity there should not be any modification in the original information [10]. These properties are maintained by ensuring secure channels for communication, authorization, and auditing and intrusion detection mechanism [4]. The security of the software is compromised by internal factors like inside threats whereas the authorized users can behave as an hacker, external factors include security attacks the capability of humans to maliciously break in to the system taking advantage of vulnerabilities[14]. In software security threat causes damage and it exploit vulnerability to breach system security and it might be internal or from external factors [6]. Security threats are classified in to human threats and natural disasters whereas human threat is classified in to malicious outsiders like hackers and non-malicious like insiders [15, 18]. Threats are handled by threat modelling Microsoft proposed threat classification called STRIDE whereas Spoofing of user identity, Tampering, Repudiation, Information disclosure, Elevation of privilege [9].The threat analysis process identifies the probability of occurrence risk associated with vulnerability and it provides a basis for establishing cost effective security program [7].The security risk analysis is a interrelationship between asset, threat and vulnerability. The security risk analysis is classified in to quantitative and qualitative [16]. The quantitative analysis identify asset value, determine the impact of vulnerability, estimate the likelihood of exploitation, and evaluates the cost of counter measure to control its impact whereas qualitative risk analysis generally used in information security[8]. Boehm's six phases includes risk identification, risk analysis, risk prioritization, risk management, risk resolution and risk monitoring have to be incorporated in to the software development life cycle [11].

II. RELATED WORK

Several papers have been studied in the area of software security .Ming Ni et al[1] proposes a model to improve OL-RBSA On line risk based security assessment .The proposed metrics is the severity model to capture the consequences due to equipment outage. The performance index of this paper speed analysis. The issue and challenge

ISSN(Online): 2320-9801
ISSN (Print): 2320-9798

International Journal of Innovative Research in Computer and Communication Engineering

(An ISO 3297: 2007 Certified Organization)

Vol. 3, Issue 4, April 2015

addressed in this paper is to enhance speed for online application. Spyros et al [2] proposes a model based on fuzzy set theory and fuzzy fault tree to compute security risk for attacks. The performance index of the paper is to automate the process of determining risk based on the model finally it measures the change in calculated risk. The challenges and issue addressed in this paper is the system with high risk has no security pattern. The main objective of this paper is to automatic searching of missing security pattern. Balachandra Pattanaik et al[3] proposes a model based on fault detection technique for an embedded system using rough set classifiers The issue and challenges addressed in this paper is detection of faulty components in an embedded application. The performance index of the paper is to measure the reduction of attributes and to enhance the detection capability. In this paper faults are categorized according to the functionality, behaviour and the target environment of the embedded system it can be tuned to only application specific designs not as a general framework for fault diagnosis of the system. Fadi Hajsaid et al [5] propose a model based on unified modelling language. The issue and challenge addressed in this paper is to estimate the probability and severity failure for each element and to automate the security risk assessment to access the security risk in cloud. The performance index of the paper is to calculate the risk factors. A mathematical model is proposed to estimate risk factor. The limitation of the paper is to analyse the probability and severity of security failure.

III. TYPES OF SECURITY ATTACK

The security attack includes passive monitoring of network, active attack, close in attack, insider exploitation, service provider attack [17]. Passive attack monitors the system and network it does not affect the system and it capture the credential information about the authorized user. An active attack monitors the system and it attempts to modify the information of the system [12].

a. *Spoofing Attack:*

Spoofing attack sends message to the user from a bogus e-mail address or faking the e-mail address of another user, it provides wrong information to the user. The spoofing attack exploits the vulnerability and modifies the source address of the packet and it modify the network protocols by causing damage to the network by modifying the source address of the packet.

b. *Non Reputation Attack:*

Non Reputation attack refuses to provide acknowledgement to the user this attack changes the authorized information. The attack can be detected by Checking and maintaining the authorized user time stamp this attack can be counter measured by Providing Digital signature. The user verifies the authorized information by verifying the digital signature and this signature provides authentication and integrity of the information. This attack Causes Company loses customer and revenue

c. *Tampering-Data integrity Attack:*

Tampering data integrity attack attempts to modify the data of Authorized parties and it causes data Loss. This Attack outputs the loss of integrity of information. The rights and privileges of authorized users can be modified and it also makes the device failure. Authorized information may be disclosed and it reduces the loss of trust among the users.

d. *Denial of service Attack*:

This attack causes the network resource unavailable to its intended user due to the unavailability of resource the response of the network is slow and it degrades the performance of the network. This attack delays the availability of websites to the authorized user and it also causes the device Disruption in web service.

e. *Eaves dropping Attack*:

Eaves dropping attack secretly listens the private conversation of others to perform loss of confidentiality of the information and it also causes the network path failure. This can be encountered by checking identity of the user by fixing the time stamp to the data. Attacker's gains access to the data path it can be checked and monitored by maintaining session login and logout time.

ISSN(Online): 2320-9801
ISSN (Print): 2320-9798

International Journal of Innovative Research in Computer and Communication Engineering

(An ISO 3297: 2007 Certified Organization)

Vol. 3, Issue 4, April 2015

f. *Malware Attack*:

Malware attack gathers sensitive information and credential of the authorized user, or it gains the access to private computer systems of the user and it enables the disclosure of sensitive information. Firewalls safeguard the attack against malware the updating of antivirus prevents the software and hardware failure.

g. *Phishing Attack*:

Phishing attack attempts to acquire information such as username, password, and credit card details of the intended user. The attacker creates fake website to hack user name and password attack and the security of the system and network is lost.

h. *Malware Attack*:

Malware attack disrupts computer operation, gathers sensitive information, or it gains access to the private information of the computer systems. Malware is a term used to represent various intrusion software includes viruses, Trojan horse, spyware, adware and malicious programs it exploits the security defects of the system.

i. *Buffer Overflow Attack*:

This attack overruns the buffer's boundary and it occurs while copying the data from one buffer to the destination buffer without checking the size of the buffer. It gains the administrator access and it causes security breach on data integrity. The attacker sends the oversized packets without checking the buffer boundary and it causes the system failure.

j. *Hijacking Attack*:

The attacker gains unauthorized access to information or loss in services in a computer system .Attacker takes control over communication it exploits the computer session. The session is hijacked by sending the email to the user with a link containing the session id.

k. *Password attack*:

Password attack cracks the password stored in the computer system the purpose of this attack is to gain access the privilege of the user .the most common method of password cracking such as dictionary attack, pattern checking, word list checking. The best method of preventing from this attack is by hashed password.

l. *Information disclosure Attack*:

Information disclosure attack enables an attacker to gain valuable information of the system and it enables the loss of trust and loss of data integrity. The information is protected from this attack by frequently changing the password and analyzing the traffic of the network.

m. *Exploit attack*:

An exploit is a piece of software or a sequence of commands and it takes the advantage of vulnerability. Exploits are of many types the most common is by exploiting the security of the system network, it exploits the system resource, and it exploits the credential of the user.

n. *Man in the middle attack*:

This attacker secretly listens to the private conversation of two parties and making them to believe that they are talking directly to each other over a private connection. It can be prevented by maintaining timestamp and by incorporating crypto techniques.

o. *Sniffer attack*:

In this attack, attacker captures network traffic and captures sensitive information. Sniffer attack is also known as network protocol analyzer. If the network packets are not encrypted the data within the packets are read by this sniffer attack.

ISSN(Online): 2320-9801
ISSN (Print): 2320-9798

International Journal of Innovative Research in Computer and Communication Engineering

(An ISO 3297: 2007 Certified Organization)

Vol. 3, Issue 4, April 2015

p. *Hacker attack*:
This attack exploits weakness in the computer system and reveals administrator credentials it manipulates the behavior of network connections. It attacks the network to fail.

q. *DNS server spoofing Attack*:
DNS returns incorrect IP address the malicious party modifies DNS server and it reroutes specific domain name application routed to different IP address causes system failure it spreads worms and viruses.

r. *ARP Positioning Attack*:
The attacker sends fake message on to local area network and by replying with wrong MAC addresses and it causes wrong mapping in ARP table and it also makes service delay with an forged MAC address.

s. *Ping of death Attack*:
This attack sends malicious ping to the computer and the malicious ping to the host machine causes buffer overflow, denial of service and it often causes system crash.

t. *Session hijacking Attack*:
This attack exploits the valid computer session to gain unauthorized access to information. Hijacking includes cookie hijacking, session hijacking. It makes information disclosure and delay in connection.

u. *Smurf Attack*:
In this attack system is flooded with spoofed ping packets delay information, high network traffic, delay in service and it attacks the network.

IV. RISK IDENTIFICATION

Risk is defined as potential loss of the event or uncertainty of occurrence of the event. Risk is a function of triggering or exploiting particular vulnerability which results in impact to the organization. Risk is not a single factor it is a collection of threat and vulnerability [13].

The risk analysis steps include:
1. Identify Hazard
2. Assess the risk
3. Select control measures
4. Implement control measure
5. Monitor and review control measure.

Step 1: Identify hazards
The hazard has to be identified and the hazard is different from risk whereas hazard is a potential to cause harm. Risk is the possibility of occurrence or likelihood of occurrence of the event or loss of protection. Hazards can be identified by using a number of different techniques such as walking round the workplace, or making discussion among employees.

Step 2: Assess the Risk
After the identification of hazard you need to understand how much it is harm who might be harmed. Risk can be measured by high likelihood ie. A high probability of threat exists and it triggers to exploit more vulnerabilities. Medium likelihood a medium probability of threat exists and it triggers to exploit some vulnerabilities. Low likelihood probability of threat exists and it triggers to exploit to a single vulnerability. The levels of risk is analysed by means of Risk matrix. The risk matrix contains the high, medium and low levels of risk.

Step 3: Select control measures
After identifying the hazards and the levels of impact the risk measures is selected some risk can be acceptable and managed some or not acceptable and it can be determined based on the levels of risk. The risk evaluation plan and measures have been developed to prioritize, mitigate and to manage the risk.

ISSN(Online): 2320-9801
ISSN (Print): 2320-9798

International Journal of Innovative Research in Computer and Communication Engineering

(An ISO 3297: 2007 Certified Organization)

Vol. 3, Issue 4, April 2015

Step 4: Implement Counter measure

The control measures and standards are documented with their essential requirements. The risk management plan is developed to meet the requirements. The risk has been managed based on the severity levels of risk. Prioritize the risk and establish a suitable countermeasure to evaluate the risk.

Step 5: Monitor and Review Counter measure

Monitoring and reviewing are the most important part in risk management the results should be monitored, reviewed and documented. The ultimate aim of this step is to reduce the effect of risk

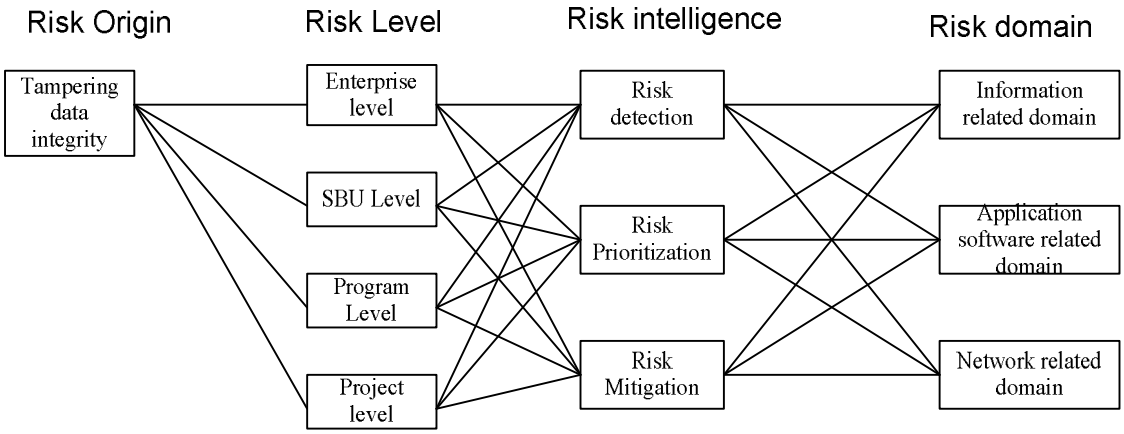

Fig1: Risk origin and levels in different domains

Fig 1 represents the Tampering of data integrity as the risk origin whereas the risk level is described in enterprise level, strategic business unit, program level and in project level. The risk intelligence describes the risk detection strategies, risk prioritization techniques and risk mitigation plan in different risk domains.

V. RISK MANAGEMENT

The risk management should be done throughout the software life cycle which involves risk identification, analysis, prioritization, planning, mitigation, monitoring and communication. The risk management cycle includes the following steps

1. Risk identification
2. Risk analysis
3. Risk prioritization
4. Risk plan
5. Risk mitigation
6. Risk Monitoring

Step 1: Risk identification

In risk identification the type of risk is identified whereas product risks, process risk, business risk, people risk or an organizational risk.

Step 2: Risk analysis

After risk identification the next step is risk analysis whereas the probability of occurrence of the event and the likelihood of the event is determined based on the impact and severity levels of risk. The risk levels in the risk matrix table include low, medium, high and catastrophic.

ISSN(Online): 2320-9801
ISSN (Print): 2320-9798

International Journal of Innovative Research in Computer and Communication Engineering

(An ISO 3297: 2007 Certified Organization)

Vol. 3, Issue 4, April 2015

Step 3: Risk Prioritization

After risk analysis risk has to be prioritizing based on the severity level the high priority risk is to be managed first.Risk is a combination of an abnormal event or failure and the consequences of that event lead to failure, to a system operators, users, or environment.

R= L .E. C

L - Likelihood of occurrence of a risky event.

E - Exposure of the system to the event.

C - Consequence of the event.

R - Computed risk

Step 4: Risk Plan

The risk management plan has to be developed for the prioritized risk the risk plan includes risk reduction and risk acceptance. Fig 2. Describes the risk assessment document

Title of the project : Development team ID : Risk Assessment team : Network connection protocol :	
Risk Name : Priority of Risk : Assets : Vulnerability attack types : Vulnerability existing : Vulnerability exploited :	
Risk Acceptance	Risk Assessment

Fig 2: Risk assessment document

Step 5: Risk Mitigation

The identified and prioritized risk is mitigated with respect to the different levels of risk and the new risk are identified**.** The risk mitigation strategies include accept, avoid, control, transfer and monitor the risk.

Step 6: Risk Monitoring

This step monitors the identified risk and it evaluates the risk reduction technique the risk response is monitored and reported periodically to the risk team leader and to the project manager.

VI. CONCLUSION AND FUTURE WORK

In this paper briefly describes about the various types of software security attacks and elaborates in detail about the causes, effects, vulnerability and threats of security attacks. It reviews in brief about the survey of various papers in software security attacks and it compares with the earlier models like STRIDE and OCTAVE. The causes of the security attacks in various domains like application, network and information related are analysed. The risk caused due to the vulnerability has been identified and elaborated in various steps. Risk hazards are been identified, accessed, counter measures are selected, implemented and reviewed. The identified risk through various steps of risk analysis is managed, maintained and documented in risk assessment document.

REFERENCES

1 Ming Ni,JamesD.McCalley “Online Risk-Based Security Assessment” IEEE TRANSACTIONS ON POWER SYSTEMS, VOL. 18, NO. 1, FEBRUARY 2003

2. Spyros T.Halkidis,NikolaosTsantalius “Architectural Risk Analysis of Software Systems Based on Security Patterns”IEEE Transactions on Dependable and Secure Computing archive Volume 5 Issue 3, July 2008

ISSN(Online): 2320-9801
ISSN (Print): 2320-9798

International Journal of Innovative Research in Computer and Communication Engineering

(An ISO 3297: 2007 Certified Organization)

Vol. 3, Issue 4, April 2015

3 ChandrasekaranSubramaniam,Balachandrapattanaik" Fault Detection in Embedded System using Rough and Fuzzy Rough Sets" Recent Researches in Computer Science ,ISBN: 978-1-61804-019-0.

4 Sodiya A.S,Longe H.O.D, Fasan O.M "Software Security Risk Analysis Using Fuzzy Expert System" Received January 18, 2008 / Accepted July 16, 2008

5. Fadi HajSaid1, Yousef Hassouneh2, Hany Ammar1, "Security Risk Assessment of Software Architecture" ICCTA 2011, 15-17 October 2011.

6. B. D. Jenkins "Security Risk Analysis And Management "Copyright © 1998, Countermeasures, Inc.

7 Ming-Chang Lee "Information Security Risk Analysis Methods and Research Trends: AHP and Fuzzy Comprehensive Method" International Journal of Computer Science & Information Technology (IJCSIT) Vol 6, No1, February 2014.

8 Catriona Norris "Project Risk Analysis and Management" The Association for Project Management March 1992 ,rebublished jan 2002.

9 Tony Van Gestel, Bart Baesens" Credit Risk Management Basic Concepts: Financial Risk Components, Rating Analysis, Models, Economic And Regulatory Capital" Oxford University Press, Isbn 978–0–19–954511–7.

10 Zhao D, Liu J, Zhang Z. (2009), "Method of risk evaluation of information security based on neural network". IEEE international Conference on Machine Learning and Cybernetics, Vol. 1, No. 6,pp.1127-1132.

11 Vorster A, Labuschagne, L. (2005), "A framework for comparing different information security risk analysis methodologies". University of ohannesburg. 2005.

12 Liu Y, Lin Q, Meng K.(2010), "Research on quantitative security risk assessment method of an enterprise information system based on information entropy", Computer Science, Vol. 37, No. 5, pp.45-48.

13 Yazar Z. A (2011), Qualitative risk analysis and management tool – CRAMM, SANS Institute InfoSec Reading Room. 2011.

14 Rot A. (2008), "IT risks assessment: quantitative and qualitative approach". WCECS, 2008, October 22-24, San Francisco, USA.

15 Feng N, Li M. (2011), "An information systems security risk assessment model under uncertain environment". Applied Soft Computer, Vol. 11, No.7, pp. 4332-4340.

16 Tamjidyamcholo A, AI-Dabbagh R. D (2012), « Genetic algorithm approach for risk reduction on information security". International Journal of Cyber-Security and Digital Forensics, Vol. 1, No. 1 pp. 59-66.

17 Hoglund, G. and McGraw, G. Exploiting software, how to break the code. *Addison-Wesley publisher)*,2004.

18 Smith, E. and Eloff, J. Cognitive fuzzy modeling for enhanced risk assessment in a health care institution. *IEEE Intelligent systems & their applications*,15(2), 2000.