ISSN (Online) 2278-1021
ISSN (Print) 2319-5940

International Journal of Advanced Research in Computer and Communication Engineering
Vol. 4, Issue 4, April 2015

Mitigation of Threats using Secure SDLC

Ekta Bhardwaj[1]**, Devendra Kumar**[2]

Student, M.Tech (CS), IEC College, Greater Noida, India [1]

Professor, Computer Science, IEC College, Greater Noida, India [2]

Abstract: Security agencies still consider this threat as one of the most common software vulnerabilities. Aiming to increasing security resistance against this software threat, emphasize on software design phase is highly reasonable where cost and time required for fixing error in design level is several times lesser than coding or implementation levels. In this purpose, we use the Secure SDLC . In this paper, we describe how to apply the secure SDLC. Software design phase in such a way that additional cost and time are not required for system analyzing and defining threat scenario.

Keywords: Secure software, software design, software threats, security analysis, SDLC

I. INTRODUCTION

Now a day's organization are not just make an application and selling it to client. But organization have to forces on certain security issues. They thought about many type of complexities.

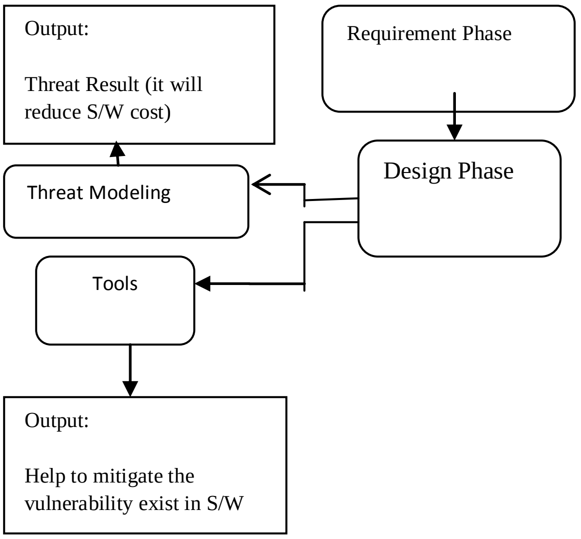
Output:
Threat Result (it will reduce S/W cost)
Requirement Phase
Threat Modeling
Design Phase
Tools
Output:
Help to mitigate the vulnerability exist in S/W

Fig 1.Overview of Design Phase of Secure Software Development Life Cycle

To make secure the whole system we have to design the secure SDLC(Software Development Life Cycle). Organization wants to implements in a cost efficient manner. We can reduce the cost of a secure system by applying earlier in software development Life cycle. Some type of people who want to break the security of system and network to damage them. It can be intentially. whether it can be for fun or for profit. It can be a group of organized criminals who work silently .They don't make noise but when their job is done. It makes a drastic loss of system.

There are following phases of SDLC:

1: Requirement: we gather the security requirement and risk assessment.

2: Design: Identify Design security requirement, Design review and Threat modeling

3: Coding: Coding Best practice and perform static analysis.

4: Testing: vulnerability assessment

5: Deployment-Server Configuration Review and Network Configuration Review

II. HOW TO MAKE A SECURE DESIGN PHASE?

a. Establish Design Requirement:

In design Phase we can consider security and Privacy concerns. This will be helpful to reduce the risk of schedule disruption and reduce a projects expense.

b. Attack Surface Analysis /Reduction:

Reducing the opportunities for attacker to exploit a potential weak spot or vulnerabilities requires thoroughly analyzing overall attack surface and includes disabling or restricting access to system services. Applying the principle of least privilege and employing layered defense wherever possible.

III. THREAT MODELING:

Threat modeling approach work on structured approach and identify security vulnerability. It determines risk from those threats and applies appropriate mitigation.Thread modeling is a core element in Software Development Life. Threat Modeling allows Software architects to identify and mitigate potential security issues.

DOI 10.17148/IJARCCE.2015.44117

It will be helpful to reduce the total cost of development.SDL threat modeling Tools enables any developer.

In this research we are considering we need to protect data. System security can break because of Malicious user may try to hack into the system and destroy it.

Security attack can be classified into:

(1)Direct: Such as Outside Hacker

(2)Indirect: random attack, viruses, computer worms

IV. HOW Risk Analysis is Beneficial for secure SDLC?

Risk analysis:

Security concept are applied when security risk are identified. Security engineering is implemented at the initial stage of Software development or we can say at design phase. If security concern is identified then it will consume less time and costly to fix future security

Risk Analysis can also do at Design Phase. If we want to identify threats in our system then we can use Threat Modeling.

We need to understand those asset which are essential for organization. and details of how the project will mitigate those threats.

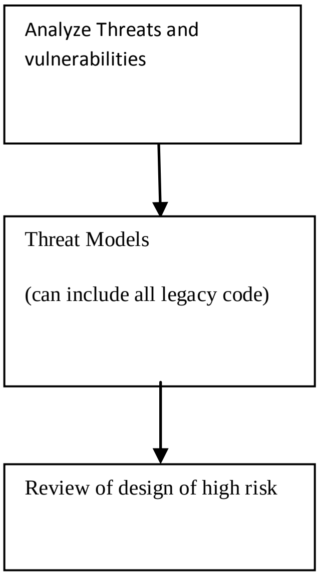
Analyze Threats and vulnerabilities
Threat Models
(can include all legacy code)
Review of design of high risk

Fig 2.Risk Analysis

V. CONCLUSION

This paper provides knowledge about Threat removal. It defines that how to implement a secure SDLC. This paper also contains details about the Threat Modeling.

By applying these concept we can improve the security level. we propose threat modeling as an essential foundation for defining security requirements of computer systems. Without identifying threats, it is impossible to provide assurance for the system and justify security

Threat modeling plays a crucial role in mitigating security threats and thereby facilitating the development of secure applications.

These secure applications can prevent the malicious activities of the cybercriminals who are taking advantage of vulnerabilities in an application.

We had a concluded that without the use of threat modeling one can not enabled the security.

REFERENCES

[1] Michael N. Johnstone, “Threat Modeling with Stride and UML” nov 2010 conference

[2] Diana M. Rojas & Ahmed M. Mahdy , ”Integrating Threat Modeling in Secure Agent- Oriented Software Development” International Journal of Software Engineering (IJSE), Volume (2): Issue (2): 2011

[3] Swapnesh Taterh, K.P Yadav, “Threat Modeling and Security Pattern used in Design Phase of Secure Software Development life Cycle” Volume 2, Issue 4, April 2012 ISSN: 2277 128X

[4]Ronald, Aaron, Dawn,” Introduction to Insider Threat Modeling, Detection, and Mitigation Track”

[5]Guifre, Elisa and Eduardo, “Automating Threat Modeling through the Software Development

[6]Muhammad Aamir and Mustafa Ali Zaidi, “DDoS Attack and Defense: Review of Some Traditional

[7] Valentin Razmov, “Denial of Service Attacks and How to Defend Against Them” May 10, 2000

[8] Sam and Yun-Tse, “Toward Software Assurance: Infusing a Threat Modling Methodology into

[9]Nawal, “Divided two-part adaptive intrusion detection system” June 2012 URL:http://www.cybersecurity.my/data/content_files/13/72.pdf

[11]Ruby B.Lee, Stephen , “Distributed Denial of Service: Taxonomies of Attacks” Tools and Counter URL:http://palms.ee.princeton.edu/PALMSopen/DDoS%20Final%20PDCS%20Paper.pdf

[12] staurt and smith, “Distributed Denial of Service Attacks”.

[13] D. Basin, M. Clavel, J. Doser and M. Egea, “Automated Analysis of Security-Design Models,” Information and Software Technology, vol. 51, no. 5, pp. 815-831, May. 2009

[14] S. Ambler. (2010, March) Introduction to Security Threat Modeling. [Online]. Available:http://www.agilemodeling.com/artifacts/securityThreatModel.htm.

[15]H. Mouratidis, P. Giorgini, and G. Manson, “Using Security Attack Scenarios to Analyze Security During Information Systems Design,” in Proc. 6th International Conference on Enterprise Information Systems, 2004, pp. 10-17.

[16] S. Burns. (2010, March) Threat Modeling: A Process to Ensure Application. [Online].Available: http://www.sans.org/reading_room/whitepapers/securecode/threat-modelingprocess-ensure-application-security_1646

DOI 10.17148/IJARCCE.2015.44117