

An Approach To Web Application Threat Modeling

By

Akash Shrivastava

April 2008

[Akash.InfoSec@gmail.com](mailto:akash.infosec@gmail.com)

1. Overview

In present internet computing environment one or the other form of security has become a requirement for all web applications. Importance of Confidentiality, Integrity and Privacy is increasing day by day and security has become vital in internet technology. To design a secure web application, it is very important to analyze and model the potential threats.

Threat modeling is a procedure for optimizing Network/ Application/ Internet Security by identifying objectives and vulnerabilities, and then defining countermeasures to prevent, or mitigate the effects of, threats to the system. [5]

A threat is a potential or actual undesirable event that may be malicious (such as DoS attack) or incidental (Information Disclosure). Threat modeling is a planned activity for identifying and assessing application threats and vulnerabilities.

Threat Modeling is an ongoing process so a framework should be developed and implemented by the companies for threats mitigation.

The aim of this paper is to identify relevant threats and vulnerabilities in the Web Application and build a Security Framework to help in designing a secure Web Application.

2. Practical Utilities of Threat Modeling

There are various vulnerabilities present in the Web Applications. Organizations should invest in the vulnerabilities according to their impact on the organization. A vulnerability that can be exploited is a threat to organization's functions and assets.

Threat Modeling can be used to:

- Identify potential threats that can be exploited to launch a successful attack against application and organization's assets.
- Design the application to meet the Security objectives.
- Help making key engineering decisions while prioritizing potential threats.
- Identify the vulnerabilities those are actually critical in the unique environment such as company network.
- Prioritize and Reduce risk of security issues arising during development and operations. [8]

3. Procedure of Web Application Threat Modeling

Major steps involved in the Threat Modeling of Web Application are mentioned below:

- Security Objectives Identification
- Assets Identification
- Application Walkthrough
- System Modeling
- Threats Identification
- Vulnerabilities Identification
- Threat Agent Selection
- Threat History Examination
- Prioritizing the Assets & Vulnerabilities
- Threat Impact Analysis

3.1 Security Objectives Identification:

Security objectives are goals and constraints related to the Confidentiality, Integrity, and Availability of customer's data and applications.

The Security Objectives are:

- Protect customer account details and customer credit history for example prevent attackers from obtaining sensitive customer data, including passwords, profile information, financial history, customer Credit Card Numbers, Bank details, or travel itineraries.
- Ensure the availability of the application at any time i.e. meet Service-Level Agreements (SLA) for application availability or meeting Compliance requirement or standard.
- Prevent unauthorized users from modifying information, especially financial information.
- The guarantee the company makes to their customers about service availability, confidentiality or integrity of data such as protect the company's online business credibility or what guarantee the company makes to their customers about confidentiality or integrity of the data.

3.2 Assets Identification:

An asset is a resource of value which varies by perspective. To the business, an asset might be the availability of information, or the information itself, such as customer data. It is important to identify and create a list of assets that involves considering every potential company asset and deciding whether or not it fits within the "security perimeter". Following is a list of common sensitive assets [7]:

- Computers and Laptops
- Routers and Networking equipment
- Printers & Fax Machines
- Cameras, digital or analog, with company-sensitive photographs
- Data - sales, customer information, employee information
- Company Smartphones/ PDAs
- VoIP Phones, IP PBXs (digital version of phone exchange boxes), related servers
- VoIP or regular phone call recordings and records
- Email
- Log of employees daily schedule and activities
- Web pages, especially those that ask for customer details and those that are backed by web scripts that query a database
- Web server computer
- Security cameras
- Employee access cards.
- Access points (i.e., any scanners that control room entry)

To an attacker, an asset could be the ability to misuse an application for unauthorized access to data or privileged operations.

3.3 Application Walkthrough:

In this step the web application is summarized into what it does, its communication and security mechanism etc. This step is all about acquiring maximum possible information about the target application. The objective is to identify the application's key functionality, characteristics, roles, key usage, technology and security mechanism etc. This will help to identify relevant threats during phase of *Identify Threats*.

Following things need to be considered to create an application walkthrough:

- Gather details about the deployment topology, logical layers key services, Communication ports and protocols.
- Identify the application's roles like who can do what within your application, Higher-privileged groups of users, Identify internal user and Administrator, Guest user and Internet user, identify Web Service or Database roles.
- It is a very important factor to identify the key usage scenarios of your application. What are the important features of your application? What does it do? Some typical scenario will be user view and search products and add them in Shopping Cart, Registered user logs in and place an order through Shopping Cart. Identifying the functionality and usage of the application helps you to understand how the application is projected to be used and how it can be misused.
- Identify and list the Technologies and Software that the application uses. For example Operating System type, Web Server type and version, Database, Technology used i.e. .Net or C# or any other etc. This not only helps to put more focus on technology-specific threats but also helps us to determine the correct and most appropriate mitigation techniques.
- Identify which Security Mechanism is being used by the application. Various key points should be considered when identifying application security mechanisms known. For example:
 - Input and data validation
 - Authentication & Authorization Mechanism
 - Session Management
 - Cryptography Technique used
 - Auditing and logging

3.4 System Modeling:

At the start of the Threat Modeling process, the security designer needs to understand the system absolutely. With the help of the use cases and architectural model, system model for the application can be created. The more you know about the application, the easier it is to expose threats and discover vulnerabilities. This step involves breaking down the application to create a security profile.

The process of decomposition of the application involves understanding every component (Website, Web Service or Database) and its interconnections, defining usage scenarios, and identifying assumptions and dependencies (external or internal such as AD, Mail System etc).

There are different techniques that can be used to model a computing system. Following points can be considered to create a model of the application/ System:

- Identify trust boundaries of the system such as a perimeter firewall or the boundary between the Web Application and a third-party service.
- Draw the Data Flow Diagram (DFD) of the application which dissects the application into its functional components and indicates the flow of data into and out of the various parts of system components such as user login method, data flow between Web Application, Database Server and a Third Party Service or Web Service.
- Identify the entry points to the application as they also serve as entry points for attacks such as Web request through Port 80 or Port 443, Login Pages for internal and external users, admin pages etc.
- Identify exit points as they can also be used as an attack vector such as search page, which writes the client's search string and the corresponding results and index page, which displays product details.

What we need is a system model that reveals the essential characteristics of the system and helps in identifying threats which may arise due to specific application logic or technology engaged in the application. The more complete and detailed the model is, the more successful the other stages will be.

3.5 Threats Identification:

In this step, those threats are identified, which may affect the system and compromise the assets. Threat identification is the key to a secure system. Identifying threats consists of analyzing each entry/exit points, examine the application tier-by-tier, layer-by-layer and feature-by-feature.

The following threats could affect the application:

- Dictionary based Brute Force attacks.
- Network eavesdropping occurs between the browser and Web server to capture client credentials.
- An attacker may capture cookies to take-off the identity.
- SQL Injection, which enables an attacker to make use of an input validation vulnerability to execute commands in the database and thereby access and/or modify data.
- Cross-site scripting through injecting script code.
- Information leakage.
- An attacker takes control of the Web server, gain unauthorized access to the database, and run commands against the database or gain unauthorized access to Web server resources and static files.
- Discovery of encryption keys used to encrypt sensitive data (including client credit card numbers) in the database.

3.6 Vulnerabilities Identification:

To identify weaknesses related to your threats, layers of application should be reviewed. Using vulnerability categories help focusing on those areas where mistakes are most often made.

Common application vulnerabilities are:

- Authentication related vulnerability such as lack of password complexity enforcement or lacks of password retry logic
- Invalidated Data & Inputs
 - Is all input validated?
 - How is it validated?
 - Is it validated for type, length, format, and range?
 - What does good data look like?
 - Where is it validated?
- Exception handling
 - What information is needed for troubleshooting?
 - What information should be presented to the end user?
 - An attacker may gain useful exception details
 - Providing detail error message to the end-user/ client
- Weak Encryption key or encryption key is using wrong algorithm
- Revealing an administration function through the Web application
- Remote Code Execution vulnerability
- SQL Injection or Cross Site Scripting
- Username enumeration
- Parameter Tempering
- Authorization Manipulation and User Privilege Escalation
- Session & Cookie

3.7 Threat Agent Selection:

Threat agent is the person or event that has the ability to generate threats. In the above mentioned scenario following are the main threat agent/ event:

- Insiders and users
- Hackers and Crackers (Hackers/ Crackers Group)
- Worm, Trojans and Viruses
- Natural and environmental events (Floods, Fire etc)

3.8 Threat History Examination:

Now we have a compiled list of current threats. But it is always better to consider future threats, which may arise. The first step towards predicting future threats is to examine the company's records and speak with long-time employees about past security threats that the company has faced.

Most threats repeat themselves, so by cataloging the company's past experiences and including the relevant threats on your threat list you'll get a more complete picture of your company's vulnerabilities.

3.9 Prioritizing the Assets & Vulnerabilities:

We have now developed a complete list of all the assets and security threats that the company may face. It is important to consider that every asset or threat does not have the same priority level. In this step, we shall prioritize the assets and vulnerabilities in order to know the company's greatest security risks.

Following step should be taken to prioritize the Assets & Vulnerabilities:

- Developing a Risk and Probability Calculation Matrix
 - Calculate Risk.
 - Calculate Probability.
 - Calculate Impact

The implementation of the countermeasure depends on the criticality of the assets and vulnerabilities. There are various techniques available to prioritize threats and vulnerabilities. Microsoft's DREAD (Damage, Reproducibility, Exploitability, Affected Users, and Discoverability) model of prioritizing threats and vulnerabilities seems to be one of the popular methods.

3.10 Threat Impact Analysis:

The term Impact is used to indicate the result of a threat reaching an asset. Threat Impact can be categorized into following:

- Minor: minor loss of a business asset, no change in business order
- Moderate: business disruption, moderate changes in way of conducting business
- Major: out of business unless countermeasures are deployed immediately
- Catastrophic: out of business from the moment that the threat was realized

The impact of a threat may affect Market Shares, Business Capital, Users, Stakeholders & Business Partners Trust and Company reputation.

The immediate outcome of the threats reaching to an asset could be disclosure, modification, destruction, loss, interruption and unauthorized access.

4. Development of Security Threat Response Plan:

In this step a primary response plan to a particular threat based on the priority list of assets and vulnerabilities should be developed. Although these security responses are not the only appropriate ways to deal with a security threat, but they cover the vast majority of the threats the company faces.

Apart from the primary response plan to the threats, following implementation is required as security strategy:

- Implementing Network ACLs
- Implementing IDS/IPS
- Implementing IDM
- Backups
- Content & Email Filtering
- Implementing Physical Security

Conclusion:

Modeling the application is important to identify threats and vulnerabilities in the application, which may affect the company business. It provides an understanding of the company assets and risk to the application, assets and overall business.

We have discussed potential threats to the application and requirement for the threat modeling process. Threat modeling process provides a security framework to secure the web application.

Using the frame is helpful in identifying threats and vulnerabilities in the System. While creating and implementing a Frame for Web Application security, two main points are considered as critical:

1. The most common mistakes, which the developers make
2. The most proficient improvements

Based on the study, it can be concluded that modeling the application for present and future threats and vulnerabilities can provide great level of security to the company. Security policies can be a very helpful practice in protecting networks from the threats vulnerabilities and maintains Confidentiality, Integrity and Availability of the system.

Finally, being ever cautious and watchful will keep the attackers at holiday. So, it is always better to hide yourself from Hacker, Cracker and Script Kiddies to survive in the today's technological environment.

References:

1. Understanding and Developing a Threat Assessment Model, Stilianos Vidalis and Andrew Blyth, University of Glamorgan.
2. J.D.Nosworthy, A Practical Risk Analysis Approach: Managing BCM Risk. Computers & Security, 2000. Pg. 596-614
3. Analyzing Threat Agents & Their Attributes, Dr. Stilianos Vidalis, Dr. Andrew Jones, University of Glamorgan.
4. Electronic Warfare Association – Australia (URL: www.ewa-australia.com/infosec-stream2.htm)
5. http://searchsecurity.techtarget.com/sDefinition/0,290660,sid14_gci1166533,00.html
6. An Introduction to FAIR: The Factor Analysis of Information Risk (FAIR) Framework. (URL: http://fairwiki.riskmanagementinsight.com/?page_id=18)
7. <http://www.itsecurity.com/features/it-security-audit-010407/>
8. <http://msdn2.microsoft.com/en-us/library/ms978516.aspx>