OWASP Risk Rating Methodology

DISCLAIMER

Over the years there has be lots of debate about the OWASP Risk Rating Methodology and the weighting of Threat Actor Skill levels. There are other more mature, popular, or well established Risk Rating Methodologies that can be followed:

- NIST 800-30 - Guide for Conducting Risk Assessments
- Government of Canada - Harmonized TRA Methodology
- Mozilla resources:
  - Risk Assessment Summary
  - Rapid Risk Assessment (RRA)

Alternatively you may with the review information about Threat Modeling, as that may be a better fit for your app or organization:

- https://owasp.org/www-community/Threat_Modeling
- https://owasp.org/www-community/Application_Threat_Modeling
- OWASP Threat Dragon

Lastly you might want to refer to the references below.

Note: Edits/Pull Requests to the content below that deal with changes to Threat Actor Skill will not be accepted.

Author: Jeff Williams

Introduction

Discovering vulnerabilities is important, but being able to estimate the associated risk to the business is just as important. Early in the life cycle, one may identify security concerns in the architecture or design by using threat modeling. Later, one may find security issues using code review or penetration testing. Or problems may not be discovered until the application is in production and is actually compromised.

By following the approach here, it is possible to estimate the severity of all of these risks to the business and make an informed decision about what to do about those risks. Having a system in place for rating risks will save time and eliminate arguing about priorities. This system will help to ensure that the business doesn't get distracted by minor risks while ignoring more serious risks that are less well understood.

Ideally, there would be a universal risk rating system that would accurately estimate all risks for all organizations. But a vulnerability that is critical to one organization may not be very important to another. So a basic framework is presented here that should be ‘‘customized’’ for the particular organization.

The authors have tried hard to make this model simple to use, while keeping enough detail for accurate risk estimates to be made. Please reference the section below on customization for more information about tailoring the model for use in a specific organization.

Approach

There are many different approaches to risk analysis. See the reference section below for some of the most common ones. The OWASP approach presented here is based on these standard methodologies and is customized for application security.

Let's start with the standard risk model:

- **Risk = Likelihood * Impact**

In the sections below, the factors that make up “likelihood” and “impact” for application security are broken down. The tester is shown how to combine them to determine the overall severity for the risk.

```
Step 1: Identifying a Risk
Step 2: Factors for Estimating Likelihood
Step 3: Factors for Estimating Impact
Step 4: Determining Severity of the Risk
Step 5: Deciding What to Fix
Step 6: Customizing Your Risk Rating Model
```

Step 1: Identifying a Risk

The first step is to identify a security risk that needs to be rated. The tester needs to gather information about the threat agent involved, the attack that will be used, the

vulnerability involved, and the impact of a successful exploit on the business. There may be multiple possible groups of attackers, or even multiple possible business impacts. In general, it's best to err on the side of caution by using the worst-case option, as that will result in the highest overall risk.

Step 2: Factors for Estimating Likelihood

Once the tester has identified a potential risk and wants to figure out how serious it is, the first step is to estimate the "likelihood". At the highest level, this is a rough measure of how likely this particular vulnerability is to be uncovered and exploited by an attacker. It is not necessary to be over-precise in this estimate. Generally, identifying whether the likelihood is low, medium, or high is sufficient.

There are a number of factors that can help determine the likelihood. The first set of factors are related to the threat agent involved. The goal is to estimate the likelihood of a successful attack from a group of possible attackers. Note that there may be multiple threat agents that can exploit a particular vulnerability, so it's usually best to use the worst-case scenario. For example, an insider may be a much more likely attacker than an anonymous outsider, but it depends on a number of factors.

Note that each factor has a set of options, and each option has a likelihood rating from 0 to 9 associated with it. These numbers will be used later to estimate the overall likelihood.

Threat Agent Factors

The first set of factors are related to the threat agent involved. The goal here is to estimate the likelihood of a successful attack by this group of threat agents. Use the worst-case threat agent.

- **Skill Level** - How technically skilled is this group of threat agents? No technical skills (1), some technical skills (3), advanced computer user (5), network and programming skills (6), security penetration skills (9)
- **Motive** - How motivated is this group of threat agents to find and exploit this vulnerability? Low or no reward (1), possible reward (4), high reward (9)
- **Opportunity** - What resources and opportunities are required for this group of threat agents to find and exploit this vulnerability? Full access or expensive resources required (0), special access or resources required (4), some access or resources required (7), no access or resources required (9)
- **Size** - How large is this group of threat agents? Developers (2), system