Threat Modelling

An introduction

Threat modelling works to identify, communicate, and understand threats and mitigations within the context of protecting something of value.

A threat model is a structured representation of all the information that affects the security of an application. In essence, it is a view of the application and its environment through the lens of security.

A threat model typically includes:

- Description of the subject to be modelled
- Assumptions that can be checked or challenged in the future as the threat landscape changes
- Potential threats to the system
- Actions that can be taken to mitigate each threat
- A way of validating the model and threats, and verification of success of actions taken

Threat modelling is best applied **continuously** throughout a software development project!

Updating threat models is advisable after events such as:

- A new feature is released
- Security incident occurs
- Architectural or infrastructure changes