# Threat Modelling Fundamentals

### Why do we Threat model ?

Threat modelling encompasses of a methodology which is utilized to anticipate problems when its inexpensive to deal with them. Ideally this is before any code has been written or any chips have been produced or any concrete has been poured. In essence this is the initial step, which can be customized depending on the product.

### 4 Questions to get started ? / The foundational 4 step approach to threat modelling

1. What are we building
2. What can go wrong
3. What are we going to do about it
4. Did we do a good job

1. What are we building ?

### Designing a Threat model

1. Design the network infrastructure, and make appropriate connections, making use of unidirectional data flows is essential to identify what goes in and what comes out

A screen shot of a computer

Description automatically generated

1. Configure which assets are received and sent, we can also annotate the data flow with tags

A screenshot of a computer

Description automatically generated

1. Complete the questionnaire on web applicationA screenshot of a computer

   Description automatically generated

For example if credit card data is chosen, the tool provides you functionality to further specify details regarding the cards

A screenshot of a computer

Description automatically generated

1. A close up of a sign

   Description automatically generatedWe can now update the threat model, the IriusRisk deploys a rules engine to analyze the diagram along with it configurations and update appropriately

### Templates

Templates provide a pre defined threat modelling scenario which we can update to our own liking. These can be imported to our personal projects as well.

A screenshot of a computer

Description automatically generated

A screenshot of a computer

Description automatically generated

We also have the accessibility to embed projects into other projects combining the functionality of both into one whole system, this capacity can be obtained by the IriusRisk threat modelling platform

* Current working project

A screenshot of a computer

Description automatically generated

* Copying from “my payroll application”

A screenshot of a computer

Description automatically generated

* Additional functionality is updated to the current project

A screenshot of a computer

Description automatically generated

A screenshot of a cellphone

Description automatically generated A screenshot of a website

Description automatically generated

2. What can go wrong ?

in this platform we can assign threat levels we can configure how to set up a threat indicator. Analyze what kind of threat have been detected and ensure effective counter measures are taken

A screenshot of a computer

Description automatically generatedA screenshot of a computer

Description automatically generatedA screenshot of a computer

Description automatically generatedA screenshot of a computer

Description automatically generated

**Risk**

Risk is a function of threat impact multiplied against the likelihood of realization

**Risk Pattern**

Inside of IriusRisk, we use risk patterns to group sets of threats together for application to a threat model. MOST of the time when a component is added to a project, it will bring an entire risk pattern into IriusRisk. Risk patterns are composed of Use Cases which are composed of Threats

**Use Case**

Method for organizing and grouping sets of threats. Types of use cases might include - Authentication, Authorization, Logging and Monitoring, etc.

**Threat**

Threats are ultimately the bad things that will happen if a weakness is realized. Threats are the events which ultimately lead to the loss of confidentiality, integrity, and availability for assets assigned to components.

**Threat Impact**

These three impacts demonstrate the impact that this threat will have on those three functional areas of an asset (Confidentiality, Integrity, and Availability) if realized. Not all threats will impact data in the same fashion.

**Ease of Exploitation**

This value for a threat represents the relative ease to realize this threat. Low Ease of Exploitation would represent that something is more difficult vs a high ease of exploitation would represent a threat that requires less skill and is easier to carry out.

**Standard**

In IriusRisk, standards effectively move a countermeasure from a recommended to required status. Functionally, they are attached to standards and include a reference number which might correspond to external industry or internal documentation (AC - 1.1).

**Not-Applicable**

Once a threat has been moved into an Not-Applicable status, its risk is no longer impacting the overall risk of the threat model. Those threats will also be excluded from the Risk Summary Report. By default, N/A threats are hidden from view in the threats interface. They can be added back into the view by unselecting the “Hide NA Threats” under the view icon.

**Risk Acceptance**

Defines whether or not an organization has formally accepted a risk. Generally, this is defined for only a set period of time where this risk is “accepted”

**Risk Exposure**

A risk is considered exposed when it is applicable and actionable to an organization or a threat model. Generally speaking, inside of IriusRisk, risk exposure is the opposite of risk acceptance.

**Inherent Risk**

Inherent risk is the risk innate in a project or threat model because of a configuration or the existence of components, assets, and the threats which would seek to expose or exploit those assets

**Current Risk**

The current risk is equivalent to the inherent risk minus any implemented countermeasures or mitigations.

**Projected Risk**

The projected risk is the equivalent of inherent risk minus any implemented and planned countermeasures or mitigations.

**Weakness**

Represents an event which might potentially permit a given threat to be exploited

**Countermeasure**

Countermeasures or controls are the planned mitigation or risk reducing items which are leveraged to reduce the inherent risk of a project or threat model. They can be in multiple states: recommended, required, implemented.

**Risk Response**

Risk response is a visual indicator of the threat modeler’s progress on reducing the risk on a specific threat.

**Count. Progress**

Abbreviated from Countermeasure progress, is a visual indicator of the completion status of any required countermeasures. Recommended countermeasures are not included in the visual indicator.

**Owner**

The owner of a threat is the user or group of users who are responsible for mitigating, updating, or removing this threat

1. **Inherent Risk**: The baseline risk without any mitigating controls.
2. **Current Risk**: The actual risk with existing security measures in place.
3. **Projected Risk**: Forecasted future risks based on anticipated changes.

Each type of risk informs different aspects of threat modeling, helping prioritize security efforts and mitigate potential threats effectively.

1. What are we going to do about it ?

Making use of threat details and their mitigations to ensure appropriate countermeasures have been taken place, we can align each model with various software’s and baselines to compare and contrast how different threats act in different environments

1. A screenshot of a computer

   Description automatically generatedA screenshot of a computer

   Description automatically generatedDid we do a good job

A diagram of a diagram

Description automatically generated with medium confidence