

Threat modelling methodology

Version: 0.1
Status: Draft
Date: Jan-2023
Contact:
E-Mail:

Copyright © Rakuten 2023

1	Introduction.....	4
2	Tools.....	4
3	Methodology for threat modelling	5
3.1	Methodology introduction.....	5
3.2	RACI table.....	6
3.3	Workflow of threat modelling report generation.....	6
3.4	Product / solution architecture	7
3.5	Communication matrix for services and data assets of product / solution	7
3.6	Prepare the data flow diagram.....	7
3.6.1	Identify the assets, interfaces in a DFD (data flow diagram).....	7
3.6.2	Input STRIDE threats for each asset, interface	10
3.6.3	Identify security controls which can be used for threat mitigation.....	11
3.6.4	Indicate mitigation and priority of each threat	11
3.6.5	STRIDE threat, mitigation mapping.....	11
3.7	Threat identification	12
3.7.1	Update the identified threats in template	12
3.8	Risk analysis and threat mitigation	12
3.8.1	Assess risk of each threat in the context of the product / solution	13
3.8.2	Map the security controls against each threat.....	13
3.8.3	Prepare a consolidate list of security controls.....	13

Document Control

Document Version History

Version	Date	Author	Description of Change
0.1	18-Jan-2023	Krishna Pramod A	Initial draft
0.2	07-Feb-2023	Kevin Feng	Updated based on internal review comments
0.3	09-Feb-2023	Krishna Pramod A	Updated various sections based on threat model lifecycle stages
0.4	22-Feb-2023	Krishna Pramod A	RACI table update

Approvals

This table shows the approvals on this document for circulation, use and withdrawal.

Version	Date	Approver	Title/Authority	Approval Remarks

Acronyms

STRIDE	Spoofing, Tampering, Repudiation, Information disclosure, Denial of Service and Elevation of Privilege
--------	--

1 Introduction

This document describes STRIDE based threat modelling methodology for Rakuten Symphony products or solutions. This methodology could be used to fill the threat model report template <https://rak.box.com/s/byi2fo1fpeq9780dm4pkxo7mncvfu0>

Threat modelling is a structured approach of identifying and prioritizing potential threats to a system and determining the value that potential countermeasures would have in reducing or neutralizing those threats.

The purpose of threat modeling is to provide defenders with a systematic analysis of what controls or defenses need to be included, given the nature of the system, the probable attacker's profile, the most likely attack vectors, and the assets most desired by an attacker. Threat modeling is a crucial part of security development lifecycle.

STRIDE is the most mature standard method to systematically identify the threats by considering different threat categories which fall under Spoofing, Tampering, Repudiation, Information disclosure, Denial of Service and Elevation of Privilege.

Once the different threats are identified, a risk analysis is done for the identified threats and counter measures are identified. The counter measures depend on a set of security controls that can be employed to mitigate the threat.

Introduction of STRIDE can be found here: <https://learn.microsoft.com/en-us/training/paths/tm-threat-modeling-fundamentals>

2 Tools

There are several threat modelling tools available, including the Microsoft Threat modelling tool, OWASP threat dragon, and others.

OWASP threat dragon is the recommended tool for threat modelling. The threat dragon is chosen because of the ease of use, cost, good user interface and flexibility in modelling the assets / threats.

OWASP threat dragon (<https://owasp.org/www-project-threat-dragon/>) is a public domain/free tool which can be used to perform STRIDE based threat modelling. The tool enables to depict different assets, its interfaces, asset/interface segregation using boundaries, associating threats with the assets, threat mitigation status (already mitigated or not).

The tool provides a graphical user interface to perform the threat modelling. The model data entered in the tool is stored as JSON files which enable easy transport of files to other users of the same tool and work collaboratively on the model. A report in PDF form can be generated to export the threat model DFD (data flow diagrams) as well.

3 Methodology for threat modelling

3.1 Methodology introduction

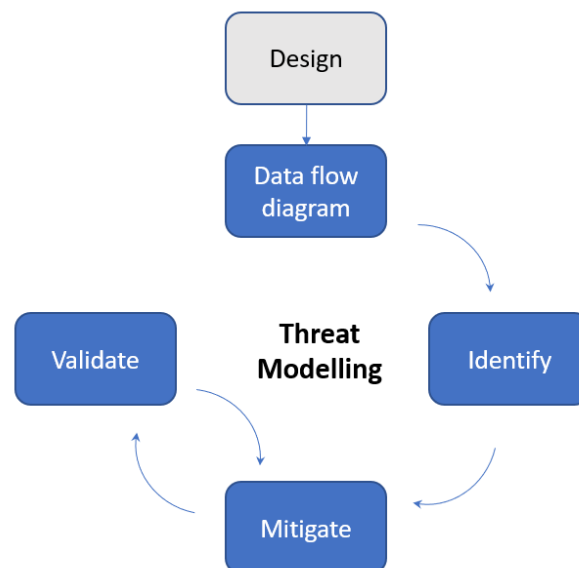
Threat modelling involves the following steps.

Firstly, create a DFD (data flow diagram) to represent the system based on the available architecture of the product/solution. With the DFD, you will get a list of elements to be analyzed, which includes assets, interfaces. A DFD needs to be updated if there are any design changes in the product / solution.

Secondly, apply a threat-modeling framework to the DFD and find potential security issues / threats.

Thirdly, identify security controls which can be used for threat mitigation, and indicate mitigation and priority of each threat.

Lastly, re-assess the residual threats to check if they can be accepted after the proposed mitigations implemented. If not, back to step 3.



The output of threat modelling is a threat modelling report.

The following links for OWASP threat dragon could be used as a quick start guide.

https://cheatsheetseries.owasp.org/cheatsheets/Threat_Modeling_Cheat_Sheet.html

<https://mike-goodwin.github.io/owasp-threat-dragon/#getting-started>

3.2 RACI table

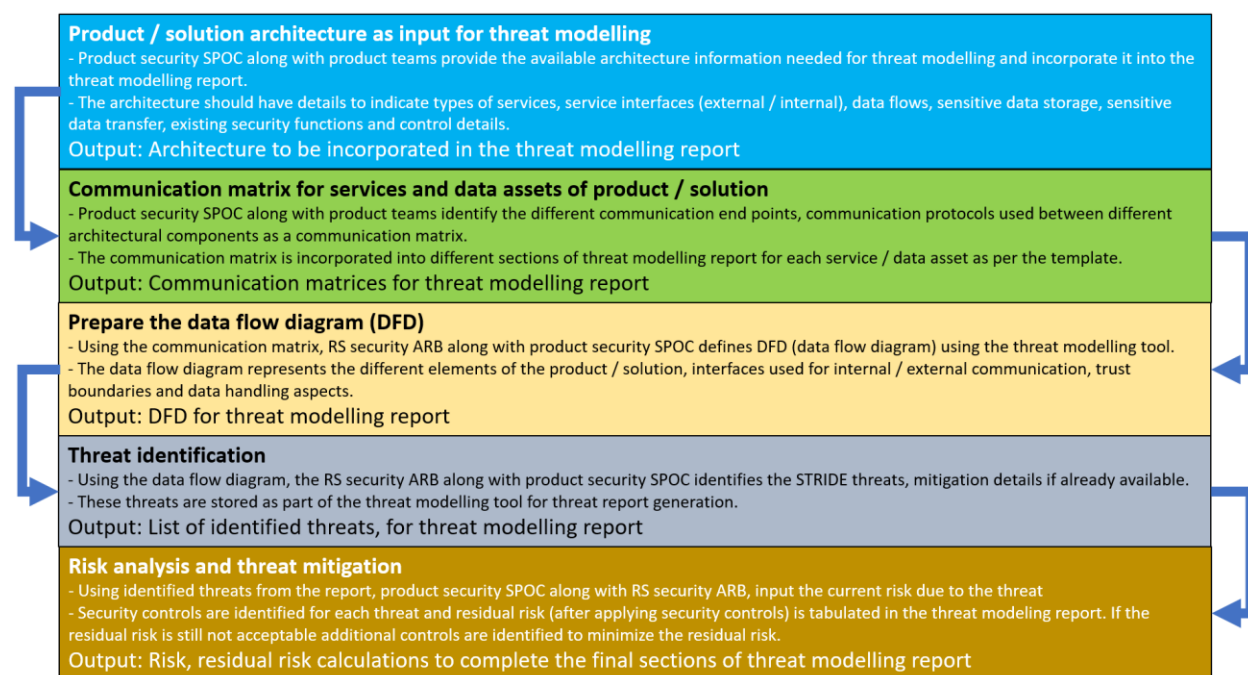
Following are the RACI (Responsible, Accountable, Consulted, Informed) roles for activities that need to be performed.

Activity	Product team	SPOC from Product team	RS Security architecture review board
Product / solution architecture as input for threat modelling (Section 3.4)	R	A	C, I
Communication matrix for services and data assets of product / solution (Section 3.5)	R	A	C, I
Prepare the data flow diagram (Note 1) (Section 3.6)	-	R, A	R, C
Threat identification (Note 1) (Section 3.7)	I	R, A	R, C
Risk analysis and threat mitigation (Note 1) (Section 3.8)	C	R, A	R, C

Note 1: This activity is a shared responsibility of the product security SPOC and RS security architecture team, but accountability lies with Product security SPOC.

3.3 Workflow of threat modelling report generation

Threat modelling workflow below defines the different key stages of the modelling process.



Subsequent sections describe the different steps of threat model report preparation.

3.4 Product / solution architecture

Owners: Product team and Product security SPOC

In the threat model report template, the product team and product security SPOC provide the architecture of the product / solution with following details.

- Diagrams which clearly identify the hardware and software components
- All interfaces of each component
- Identity / user management of the product
- Sensitive data handling aspects in transit and at rest
- Security functions of the product
- Security controls already in place

Note that the product / solution architecture and communication matrix are pre-requisites for proceeding with the below steps.

3.5 Communication matrix for services and data assets of product / solution

Owners: Product team and Product security SPOC

Provide communication matrix details for service and data assets of product / solution. The communication matrix helps to identify the security controls needed to protect the communication link and its end points.

Following table shows the columns for service asset communication matrix.

Interface name	Interface type	protocols	Ports	Comments
----------------	----------------	-----------	-------	----------

Following table shows the columns for data asset communication matrix.

Data	Protected in transit	Protected at rest	Authorization details for data handling	Comments
------	----------------------	-------------------	---	----------

3.6 Prepare the data flow diagram


Owners: Product security SPOC and RS security ARB

The DFD preparation involves representing the different architectural components and the communication matrix information in the threat modelling tool. Once this information is input, the threat identification and inputting existing security control information will follow.

3.6.1 Identify the assets, interfaces in a DFD (data flow diagram)

The first step in threat modelling report generation is to identify the different assets and their interfaces and input them in the threat dragon tool. The assets are modules / micro services, interfaces, and sensitive data.


A new, empty threat model can be created using OWASP threat dragon or an existing threat model can be opened and updated.




Welcome to Threat Dragon

Threat Dragon is a free, open-source threat modeling tool from OWASP. You are using the standalone desktop app for Windows, Macs and Linux. It can also be used as a **web application**. The desktop app is great for local use, but if your project is in GitHub you should consider the web app for better integration with your dev workflow.


You're ready to start making your application designs more secure. Use the file menu or the buttons below to create a new threat model or open an existing one from a file.



Open an existing threat model from a file on your local file system.



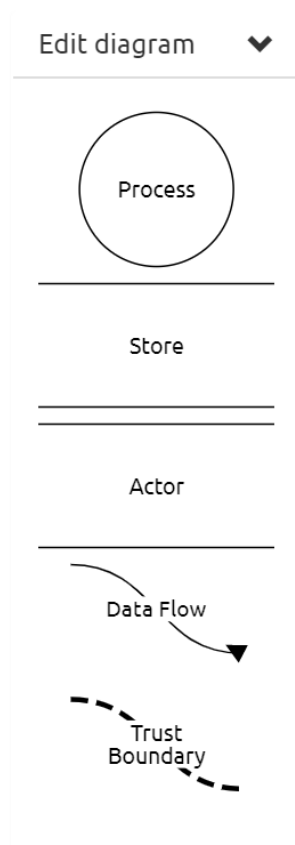
Get started by creating a completely new, empty threat model.



Explore a sample model. This is a good option if you are new to Threat Dragon.

Once the threat model is open in the tool, a new diagram can be created and edited. In the edit diagram view, graphical elements on the left side panel can be used to create the DFD.

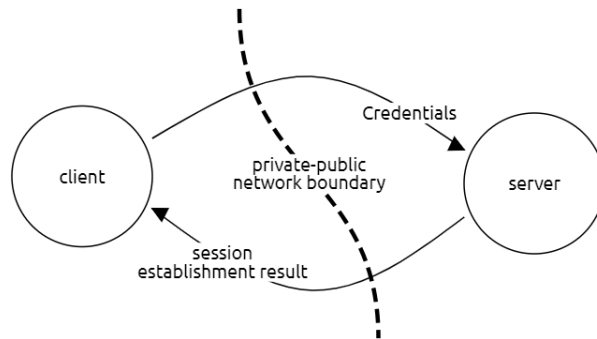
Below is a screen capture of the left side panel with graphical elements.



A mapping of the above OWASP graphical controls to DFD elements is provided below.

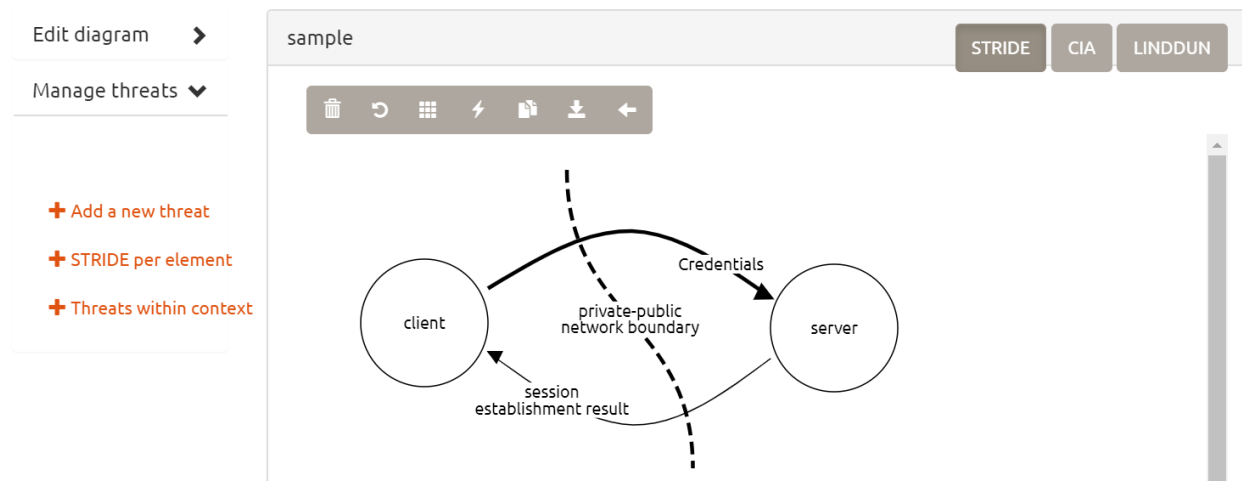
Graphical element	Mapped entity
Process	Micro-service, software process
Store	Database, datastore
Actor	Human users, Attackers
Data flow	Direction of data flow from one Process to store or another process
Trust boundary	Bifurcation of trust zones or security zones

Following diagram depicts a sample DFD involving two modules and a session establishment request response procedure. There are many modules which interact with other modules and all the modules being considered for threat model should be represented in the DFD as shown in the sample below.



3.6.2 Input STRIDE threats for each asset, interface

Once the different assets are identified and the DFD is completed for the product / solution, identify and manage different threats. This can be done by selecting an asset or an interface and then using the “Manage threats” menu as can be seen in the below figure.



When “manage threats” menu is used and STRIDE per element menu option is selected, threat for each STRIDE category can be specified and saved.

For example, the “information disclosure” category threat can be specified as shown below, for the interface between client and server when client sends its credentials for authenticating with the server.

Add this threat? (1 of 3)

Title

Potential credential disclosure

STRIDE threat type

Information disclosure

Threat status

NA Open Mitigated

Priority

High Medium Low

Description

The credentials are not secured on the interface, because a secure transport is not used for providing the credentials to the server by the client.

Mitigations

TBD

3.6.3 Identify security controls which can be used for threat mitigation

The next step after identifying all the threats is to list down the existing security controls that are used to mitigate the threat. These security controls could be the following or more.

<ul style="list-style-type: none"> • Namespace • Network policies / Firewall • Encryption at rest • Encryption in transit • Authenticated access • Authorized access 	<ul style="list-style-type: none"> • Credential rotation • High availability • Secure storage • Pruning • Quota • Input validation
--	--

3.6.4 Indicate mitigation and priority of each threat

Identify existing security controls for each identified threat and identify the priority in the tool.

3.6.5 STRIDE threat, mitigation mapping

Following are the STRIDE threats and the generic mitigations that could be applied as a counter measure for the threat.

STRIDE threat	Mitigation
<u>S</u>poofing	Authentication (using credentials, certificates, and SSH)
<u>T</u>ampering	Integrity checking (Hashing, digital signature)
<u>R</u>epudiation	Authentication, logging
<u>I</u>nformation Disclosure	Confidentiality protection (encryption, ACL, RBAC, local policies)
<u>D</u>enial of Service	Highly available systems (redundancy, load balance, resource quotas, monitoring, observability, alerting, event analysis)

Elevation of Privileges

Authentication, static code analysis, vulnerability patching, audit and remove unnecessary capabilities / privileges, isolation

Once the security controls are identified, update the previously identified threats with the security control and mitigation information. If the threat is already mitigated, the tool allows to mention the same.

The screenshot shows a web-based form for entering threat information. It includes fields for 'Title' (containing 'Potential credential disclosure'), 'STRIDE threat type' (a dropdown menu set to 'Information disclosure'), 'Threat status' (radio buttons for 'NA', 'Open', and 'Mitigated', with 'Open' selected), and 'Priority' (radio buttons for 'High', 'Medium', and 'Low', with 'High' selected). Below these are two text areas: 'Description' (containing text about unsecured credentials) and 'Mitigations' (containing text about implementing encryption in transit).

Title

Potential credential disclosure

STRIDE threat type

Information disclosure

Threat status

Priority

NA Open Mitigated

High Medium Low

Description

The credentials are not secured on the interface, because a secure transport is not used for providing the credentials to the server by the client.

Mitigations

Perform "Encryption in transit" by implementing a certificate based secure transport.

3.7 Threat identification

Owners: Product security SPOC and RS security ARB

Generate a report from the threat modeling tool and populate threat information in the threat modeling report.

3.7.1 Update the identified threats in template

Once all the security controls are mentioned in the threat model, a report can be generated using the threat dragon tool.

Note the generated report will be in PDF format and the authors of the threat model report should extract the relevant threats and update the template.

3.8 Risk analysis and threat mitigation

Owners: Product security SPOC and RS security ARB

Identify the risk of each threat by taking existing security controls into consideration. If the risk is high or medium, propose new security controls to bring the residual risk to low. The security

controls and risk information is noted against each threat and updated in the threat model report.

3.8.1 Assess risk of each threat in the context of the product / solution

Based on the report, the risk for each threat can be assessed. Following table can help to determine the risk, given the likelihood and impact values.

Impact	3-High	3-Medium	6-High	9-High
	2-Medium	2-Low	4-Medium	6-High
	1-Low	1-Low	2-Low	3-Medium
		1-Low	2-Medium	3-High
		Likelihood		

3.8.2 Map the security controls against each threat

After the risk assessment, the final step is to map the previously identified security controls to different threats that are not yet mitigated. For each un-mitigated threat, an entry can be made in a table with the following columns.

#	Asset/Function	Threat Category	Threat Description	Mitigations	Existing Security Controls	Proposed Security Controls	Risk	Residual Risk	Comments
---	----------------	-----------------	--------------------	-------------	----------------------------	----------------------------	------	---------------	----------

Description of the columns in the table above are as following.

Asset/Function: The service or data asset of the production / solution which is considered as part of threat model

Threat category: One of the STRIDE categories (namely Spoofing, Tampering, Repudiation, Information disclosure, Denial of Service and Elevation of Privilege)

Mitigations: Description of the counter measure needed to mitigate the risk from the threat

Existing Security controls: Countermeasures that are already in-place for each threat. This could be "None" if there are no existing countermeasures.

Proposed Security controls: Countermeasures that are newly proposed to reduce the risk and reach a low residual risk level for each threat

Risk: The perceived risk before the proposed security controls are applied (This is the current risk that is perceived with the existing security controls)

Residual risk: The perceived risk after the proposed security controls are applied

Comments: <self explanatory>

3.8.3 Prepare a consolidate list of security controls

At the end of the report, fill the section which consolidates all the identified security controls. Mention the security control and its description only once for each unique security control,

even if the security control is used to mitigate multiple threats. Mention all existing, planned/future security controls in this table.