



Threat Modeling 101

From your friendly neighborhood
Nylas Security Team



Hi!



The basics

Key concepts to know
before building a
threat model



But first...

Imagine a house...

◆ Done? That's your house now.



Here's the
architecture
diagram of the
house



Threat, vulnerability, and attack

Imagine a window like this in your house....

01

What factors can cause the wall / window to break?

02

What is the weakness?

03

What if... someone trying to break into the house...



To summarize

01

Crack on the window / wall

This is the weakness AKA **vulnerability**

02

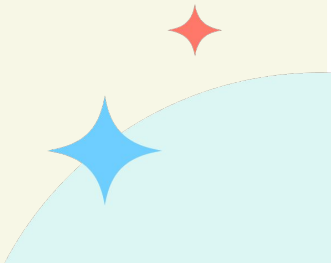
Stone, baseball bat, earthquakes etc.

These are **threats** that can exploit the weakness

03

Throwing stones

Active exploitation of the weakness that can lead to successful break in AKA **attack**



Basics done. Yay!



Ok great.. but



**Why do we need to
protect the house?**

**Because we need to stop all Kens before
they take over Barbie Land**



Let's go back to the house

Facts about this house:

- It is Barbie's dream house
- Huge closets full of expensive clothes and jewellery
- Dream car – 1962 Corvette
- Confidential documents about Barbie Land and all the Kens

So, what am I protecting here?



The answer is... Assets

What are assets?

Asset(s) are useful / valuable things.
Assets are why I am protecting the house.

Assets could be data, components, credentials, or anything else in your application/product / system

It is important to have an inventory and identify the most critical asset

- **Closets full of expensive clothes and jewellery**
- **Cash**
- **Confidential Documents about all the Kens**
- **Furniture**
- **Cars**
- **Gadgets**
- **Laptops**
- **Food and items in the pantry**
- **???**

Let's go back to the architecture...

Notice we have walls and doors?



Definition: Trust boundary

- Trust boundaries are where your trust levels change, whenever data crosses from one system to another.
- In simple terms, if you have to validate inbound data that a system is receiving, that's where a trust boundary exists.
- Trust boundaries help identify areas of focus / security concerns.

E.g., Web server & DB server

Examples of trust boundaries in a house:

- Lawn to main entrance door
- Lobby to living room
- Living room to Barbie's room
- Lawn to garage

**Threat modeling -
4 questions you
should ask**

What?

Why?

When?

How?

What is a threat model?

Any guesses?

Not just identifying.. but also

Determining and prioritizing existing, as well as, potential ways to mitigate identified threats

Definition

It is a **proactive** approach for identifying **potential threats** to your application / product / system.

But...

Threat modeling is a structured process with these objectives: identify security requirements, pinpoint security threats and potential vulnerabilities, quantify threat and vulnerability criticality, and prioritize remediation methods.

When should we do threat models?

Any guesses?

According to best practices..

It is recommended that threat modeling occurs early in the SDLC process. Threats can be identified and acted upon with ease.

How early?

Ideally, during architecture design phase.
Supports Security by Design.

But...

Remember, it is never too late to do a threat model. It is valuable even at a later stage.
(Eg., for a legacy application)

When?

Product Idea

Initial idea of the product / application

Design

Architecture of the product/app is being made and relevant components are being identified



Threat Model

Ready for threat model!

Development

Rest of the Development process continues

Why do we need threat models?

01

Reduce attack surface

Making a threat model helps us identify and reduce known attack surfaces

02

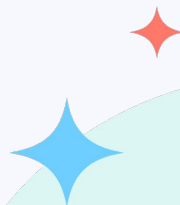
Eliminates single points of failure

Identifying all components involved in an entire system helps us identify SPoFs easily.

03

Risk reduction

Since we are identifying threats and vulnerabilities in advance, it helps us in proactive risk identification and reduction.



Why do we need threat models?



04

Security by Design

Adding security controls on top of an insecure system creates too much dependency on other tools and increases maintenance efforts.

05

Reduce occurrence of (avoidable) incidents

Same as proactive risk reduction.

06

What do you think?

We need threat models because.....

How do we make a threat model?

There are many methodologies available for threat modeling.
The commonly known ones are:

- ✓ **STRIDE**
- ✓ DREAD
- ✓ **PASTA**
- ✓ VAST
- ✓ TRIKE and so on....



There is no one-size fits all. We have the flexibility to choose one or a combination of methods that work for us.

PASTA

P

A

S

T

A

PROCESS

ATTACK

**SIMULATION
AND**

THREAT

ANALYSIS

PASTA – Explained



Our business does not want to get fined, non-resilient apps, expose sensitive data

Stage I – Define objectives

Define the purpose of the application.

Is it intended to make money to our company?

What are the security governance and compliance requirements?

Stage III – Application decomposition

How does everything we identified in Stage II communicate and interact with each other?

What diagrams do we need for that?



Data flow diagrams and trust boundaries!



Evidence based threats

Stage II – Define technical scope

AKA Know what you are protecting

What are we running?

What dependencies do we have? How many are third party?

Stage IV – Threat analysis

Involves determining what threats will arise based on the info you have from Stage II and III

What threats are pervasive for the technologies and data identified?

PASTA – Explained

Stage V – Vulnerability and weakness analysis

What are the weaknesses? What is the impact?

How are we identifying weaknesses?

- Attack scenarios from threat intel, Code Scans, CVEs, etc.

Stage VII – Risk and impact analysis

Identify risks and mitigations

Identify gaps

Tie back all information from Stages I to VI

Stage VI – Attack modeling

Map threat intel to Vulnerabilities and eventually, to assets.

Identify viable attack scenarios

Stage VIII

Pasta's done

STRIDE

S

T

R

I

D

E

SPOOFING

TAMPERING

REPUDIATION

**INFORMATION
DISCLOSURE**

**DENIAL OF
SERVICE**

**ELEVATION OF
PRIVILEGE**

STRIDE

Involves illegally accessing and using someone's authentication information

1. Pretending to be **someone** and sending emails on their behalf
2. Using stolen **API keys** to make API calls

Spooing

Denial of performing a particular action, with nothing to prove otherwise

1. Buying items from garage sale and not getting a **receipt** of purchase
2. Robbing a **bank** with no CCTV

Repudiation

Malicious modification of actual data

1. Changing grades on answer sheets
2. Changing email addresses in DB

Tampering

Exposure of data to users / individuals who do not have the authorization to view that data

1. Disclosure of passwords, API keys when screen sharing
2. Secret note to friend read by middle man

Information disclosure

STRIDE

Act of denying service of the system / application to the user

1. Sending high number of requests to a server making it unresponsive
2. You want boba tea, but the tea shop is closed

Denial of Service

A user with insufficient privileges finds a way to get sufficient access to compromise or destroy something

1. Exploiting access vulnerabilities to perform unauthorized actions
2. Steal IT admin's password and make yourself an admin

Elevation of privilege

Consider our home.. say you left the key inside and locked yourself out.

What type of threat is this?

Yes.. Denial of service

Your turn! Try to think of more examples for STRIDE..

STRIDE

S

T

R

I

D

E

AUTHENTICITY

INTEGRITY

**NON-
REPUDIATION**

CONFIDENTIALITY

AVAILABILITY

AUTHORIZATION

The background is a solid blue color with several overlapping, semi-transparent blue circles of various sizes. There are three small, four-pointed starburst icons: one red on the left, one cyan in the upper right, and one cyan in the lower center.

Note: Not all elements of STRIDE may be applicable to a component you are looking at

Guidelines for threat identification

Brainstorming

Goal / asset-oriented

- What's the most important asset at risk?
- How can someone get to the asset?

Motivation

- Which threat actor has the highest level of motivation to break into our systems?
- Eg., Ex-employee, Nation-state actors , etc.

Threat model template

Threat model template: [TM template](#)

Sections

- Description of the Product / Application
- Privacy & Security Requirements
- Business & Operational Impact Statement
- Architecture Description
- Data Flow Diagram with Trust Boundaries
- List of Assets
- List of Threats + Risk severity
- List of Compensating Controls



TM – Home Sweet Home



**Let's do a threat model for
our home sweet home!**

Procedure

After making a [copy of the template](#) and fill as much as you can

Fill the sections that you are most familiar with

Description of the Product / Application

Privacy & Security Requirements

Business & Operational Impact Statement

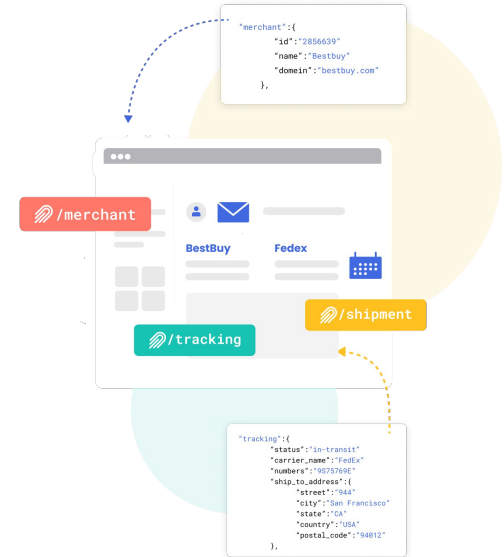
Architecture Description

Data Flow Diagram with Trust Boundaries

List of Assets

List of Threats + Risk severity

List of Compensating Controls



Sample approach

1. Define Purpose

Why are we building the product / application?

What are the privacy and compliance requirements?

2. Identify assets & decompose application

What data is in use?

What are the most critical assets?

Architecture diagram

3. Apply threat intel

What are the known threats?
(data from existing sources)

What are the possible threats?(STRIDE)

How can you identify them?

4. Identify mitigations

Can you detect the threat?

What control(s) can you implement to detect, protect and respond?

5. Assess risk

What is the impact can the vulnerability have when exploited?

Decision making

High level goals



Introducing TM to engineering

Leverage office hours/regular meeting cadences to bring more TM exposure to engineers



Architecture review process

Introducing a TM section in the Architecture Document under 'Security' Threat Model Template



Start with new products

Start with new products/app/ services and expand to all products in a slowly phased manner.

PLAN

1. Training

Leverage CSAM and Engineering Salons to train Engineers by hosting interactive sessions.

Collaboration is key

2. TM for a new product

Pick an upcoming product / app or get a team to volunteer to trial threat modeling

3. Collab via Slack channel

Slack channel similar to #architecture-reviews where everyone can come up with threats to add to the threat model!

Put on your hacker caps!!

4. Get feedback and improve process

Share feedback and help us improve the process



Thank You!

[Nylas.com](https://nylas.com)

[Github.com/Nylas](https://github.com/Nylas)

[@Nylas](https://twitter.com/Nylas)