Threat Modeling Training (Le Wagon) Playbook

Objectives

- Develop skills to identify critical trust boundaries.
- Simulate STRIDE risk analysis using a threat modeling methodology (RTMP).
- Learn how to use RTMP to speed up the threat modeling process.

Case Study: New Gamification Platform

Context

Company X is planning to design and develop a new gamification platform, hereinafter referred to as *Game Point*.

The concept is simple- the more games users play, the more points they can redeem. For the first phase, the new system will have the following functionality:

- Provide game content for users
- Display the user's point available for redemption.

Main user story

For this project, *Game Point* will integrate with multiple game content providers (3rd party vendors). End users will be redirected to each game vendor's server that hosted the game content and afterwards, each game points earned by the end-user for each game (provided by game vendors) will be exchanged for points.

Game Point consists of multiple components as described below:

1. Web Application (*gamepoint.co.jp*)
2. API endpoint (*api.gamepoint.co.jp*) which the vendor will consume to send game point information back to our system.
3. MySQL server - main database to store all application data and secrets.

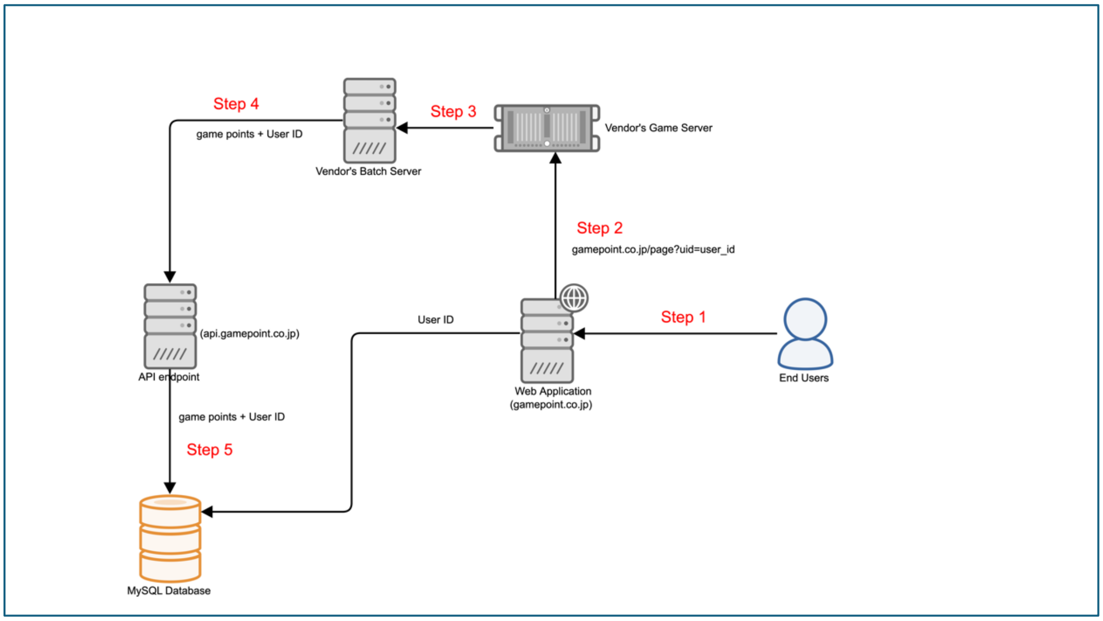


Figure 1: High-Level Architecture for Game Point System

The simplified Data Flow is explained before (refer to each Step# label on the Figure 1 diagram above):

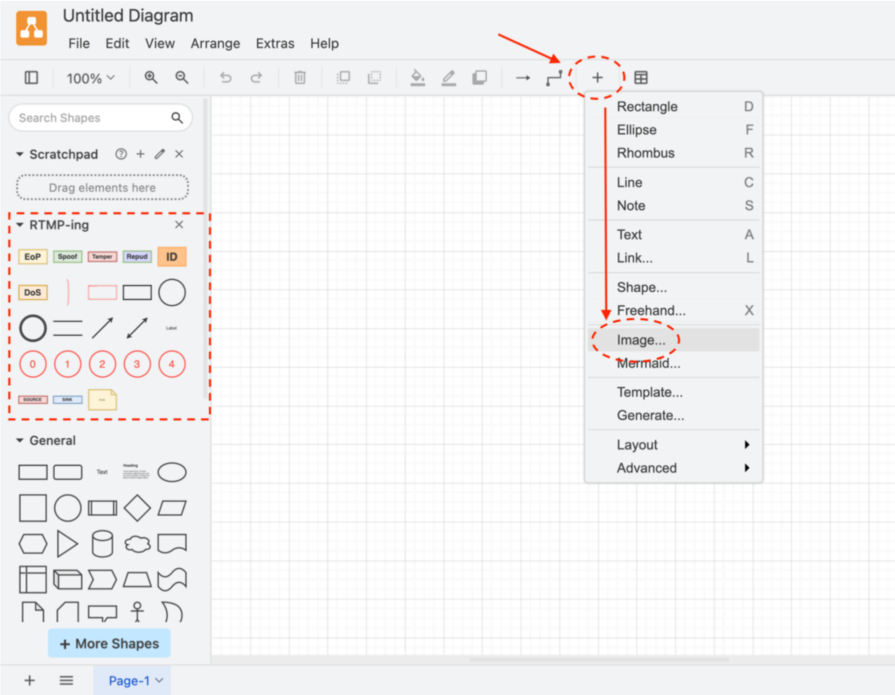
1. End users access the web application and choose to play any games. Their User ID will be stored in the MySQL database server for mapping with the game point later.
2. Once decided, clicking the chosen game will redirect the user to one of the vendor's game servers. The User ID will be passed to the vendor using the HTTP GET method.
3. Once the user has finished playing the games, their game points will be accumulated in the vendor's batch server.
4. Periodically, the vendor's batch server consumes the *Game Point* API endpoint and sends the game point along with each corresponding user ID.
5. All the game points and user ID information sent by the vendor will be stored in the MySQL database server.

Hands On - Rapid Threat Modeling Prototyping

Pre-requisite: A step-by-step instruction

Before jumping into the actual tasks, please follow the instructions below to get started:

1. Read the Case Study section above carefully.
2. Navigate to the training repository URL and download the architecture diagram located inside the repository. We will import the diagram into the diagramming tool later (details in Step 4)
    - URL: https://github.com/kur05uke/tmt_lw
    - Diagram filename: GamePoint_architecture_diagram.png
3. Navigate to the draw.io (URL: http://bit.ly/2TWFSCc) to start the STRIDE analysis using RTMP methodology. (Make sure you can see the RTMP-ing XML library on the left side panel of the draw.io tool interface)



4. (Refer to image above) Import the downloaded architecture diagram (in Step 2) into the *draw.io* tool as shown.
    - Click on the " *+*" symbol on the upper tab panel
    - Choose "*Image..*" from the drop-down list.
    - Choose to import the diagram you downloaded from Step 2.
6. From this point onwards, please refer to the slide deck located in the same training repository to complete the task described in the section below. Please use the provided RTMP XML library (highlighted in Step 3) to label the STRIDE threat accordingly using the specified RTMP rules.

Notes:

- *If the RMTP XML library is not loading on the draw.io:*
  - *Navigate to "draw.io XML" folder*
  - *Import RTMP XML library file (filename: RTMP-ing.xml) into the draw.io.*

Tasks

Review the system diagram above and try to complete these tasks:

1. Try to identify all important trust boundaries. (Tips: Pay attention to all processes talking over a network. This will help you to focus and identify critical components of the architecture).

2. Perform a STRIDE analysis using RTMP methodology to label all potential weaknesses with this design on all the components. (As some critical information is not provided, you may come up with your assumption to complete this task).

Tip: Instead of analyzing the whole diagram, try focusing on only one specific trust boundary at a time. After you finish with one, move to the next trust boundaries until you cover all the components in the diagram. Narrowing down the scope like this helps when threat modeling a complex diagram.

Summary

From the results of this exercise, we just learned how to utilise RTMP to speed up the whole process of threat modeling. This, however, will not provide a complete, in-depth threat model output. RTMP is only a supplementary tool that helps to kickstart Threat Modeling or to start the conversation in the effort to secure your design.

For full threat modeling, your next action is to identify the relevant risk that each STRIDE label signifies. RTMP helps you identify where each STRIDE threat can potentially exist, but it cannot tell you the details of the nature/scenario of risk or threat that can happen.

Threat Modeling requires us to understand all the potential risks (not just labelling the risk) because each risk will require different mitigation techniques and each of the risks can have different priority levels depending on its impact and likelihood. In this training, unfortunately, we will not have time to go through the details of threat modeling as well as each threat and its mitigation, but hopefully, from now on, you have learnt that there’s a simpler approach to threat model :)