THREAT MODELING LAB

1. PREPARATION

TOOLS

1. Each trainee should install and examine one of the following (or both :D):
    a. Microsoft Threat Modeling tool (https://docs.microsoft.com/en-us/azure/security/azure-security-threat-modeling-tool)
    b. OWASP Threat Dragon (https://owasp.org/www-project-threat-dragon/)

and create a basic threat model of a prior project.

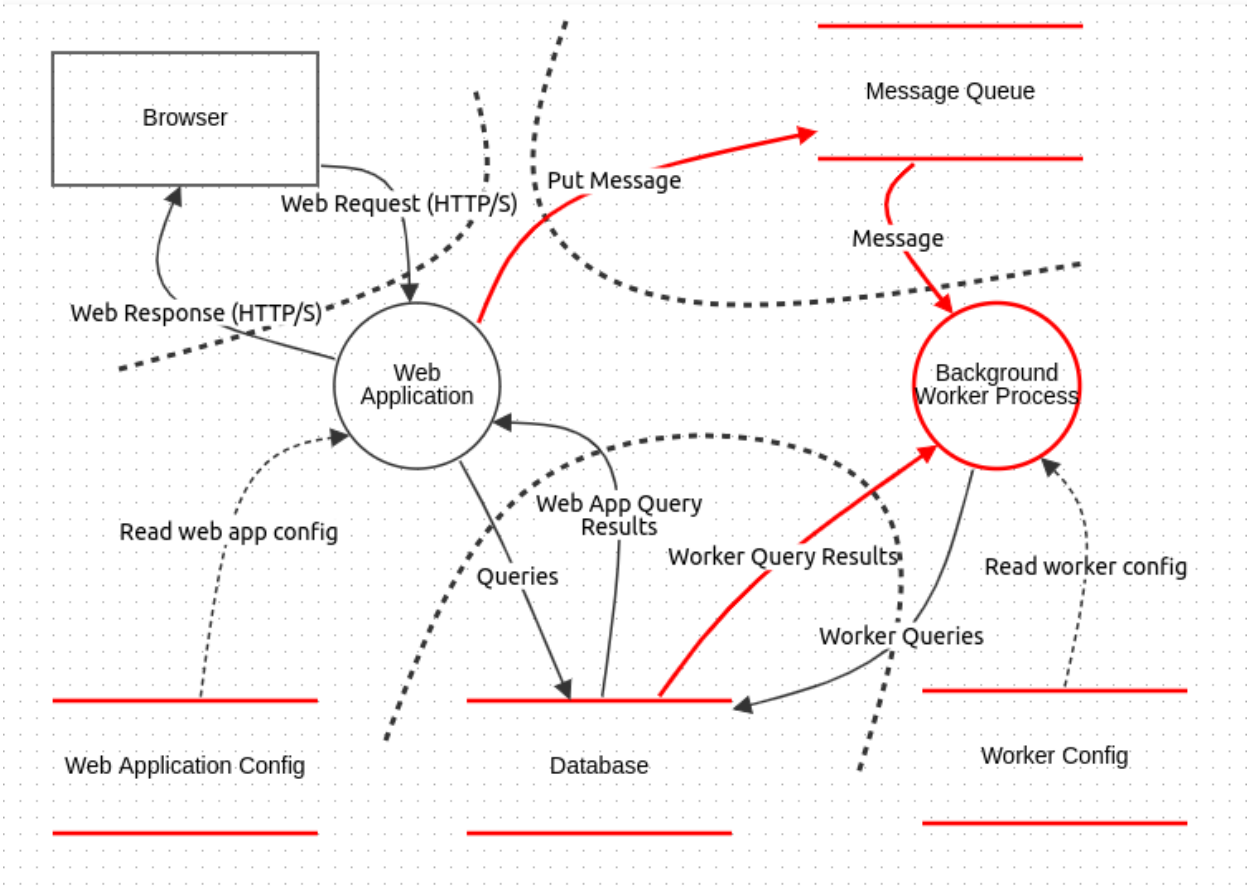
2. INTRODUCTION

Threat modeling spans both risk assessment (in which case we are talking about requirements-level threat modeling) and security design analysis (also known as design-level threat modeling). It entails the application of the security mindset to a system, where the potential attackers and their goals are identified, and the attack surface is mapped.

Example

We are developing an innovative e-commerce platform called "ElectroShop". ElectroShop is an online platform that enables users around the world to quickly and securely purchase electronic devices and accessories. Our system consists of a web server that receives HTTPS requests from customers and a PostgreSQL database to store product and customer information. ElectroShop faces a large number of orders, and in order to ensure fast and efficient processing of these tasks, a background worker process named "ElectroProcessor" is introduced. ElectroProcessor is a separate workflow that efficiently processes orders and handles payments.

In order to adapt to the dynamic needs of the system, both the web server and the background worker process have a separate config store.



EShop context threat model (OWASP TD Default Example)

3. ASSIGNMENTS

The goal of the following assignments is to perform threat modeling on an imaginary software system run by an international corporation specialized in providing travel services (akin to Expedia: https://www.expedia.com). What follows is an advert briefly describing the imaginary corporation:

MegaTravel is a multinational travel technology company. Our mission is to help you plan and experience the ultimate vacation. We cover a wide range of services, including:

- *Accommodation booking, where we select the most suitable headquarters for your trip.*
- *Transportation, where we find the best deals to get you to your dream destination.*
- *Vacation planning, where we schedule excursions, rent vehicles, prepare parties and perform a variety of services to truly bring you the best experience possible.*

Our corporation spans the globe, with three major divisions in London, Boston, and Hong Kong, and dozens of branch offices in most metropolises. Our ten thousand employees, supported by the latest and greatest technological advances, work tirelessly to research and plan your experiences, so you don't have to.

With over a hundred million returning customers, we have had the opportunity and time to perfect our craft and to produce the world's number 1 leading service for travel.

A. ATTACKER MOTIVATION

Not all information systems are the targets of sophisticated nation state attackers. Consequently, a website for a dentist's office does not require the same amount of security as a nuclear reactor.

ASSIGNMENT

Examine who would want to attack MegaTravel and why. Determine which classes of attackers would harm the system. Furthermore, for each class of attackers, determine their general skill level, their inherent access to the system, and their ultimate goals.

B. ASSETS

While security can be discussed and planned in a vacuum, often it requires financial investment to integrate into a system. This requires prioritization through risk assessment, which is accomplished by examining the affected assets.

ASSIGNMENT

Guided by the attacker motivation, the business requirements of MegaTravel and any laws and regulations that might affect this corporation, determine a list of sensitive assets. For each asset, examine:

- What its inherent exposure is – who has access to the asset;
- What the security goals of the asset are (i.e., confidentiality, integrity, availability);
- What impact would harming those security goals have on the corporation.

C. ATTACK SURFACE

By examining which users interact with the system, it is possible to identify the entry points to the system and from there the attack surface.

ASSIGNMENT

Examine which users (human, external systems) interact with the MegaTravel system and from there map the attack surface as a set of entry points from which attackers can deploy their attacks.

D. DATA FLOW DIAGRAMS

With a good idea of the attack surface and the assets, it is possible to develop data flow diagrams that illustrate both the attack surface and the different layers of trust that exist within a system. While a system might be exposed to the Internet, that does not mean that the core functionality is directly accessible. Instead, a demilitarized zone (DMZ) acts as a landing pad for all requests, validating them before sending them to a more critical zone.

ASSIGNMENT

Using all the gathered information, draw a data flow diagram of the MegaTravel system, including the attack surface, the external entities and sensitive assets. Note the trust boundaries that exist within a system. Start with a context diagram and from there decompose all complex processes until there are no significant trust boundaries left.

E. THREAT AND MITIGATION ANALYSIS

A data flow diagram is a convenient abstraction to reason around threats. Through threat identification we examine which events we want to avoid – most often the harming of a security objective of an asset. Once threats are identified, we decompose them to examine attacks which can realize the threats, vulnerabilities in the system which enable these attacks, and security controls or countermeasures that resolve these vulnerabilities.

ASSIGNMENT

Using the drawn data flow diagrams and the STRIDE threat identification methodology, identify and decompose threats. For each threat, define mitigations that prevent the threat from occurring.

4. ADDITIONAL READ – WILL BE PROVIDED TO YOU

1. Security Development Lifecycle (Michael Howard, Steve Lipner)
2. Online Banking Security Analysis based on STRIDE Threat Model (Tong Xin, Ban Xiaofang)