New Thingy Homework

# Choose an existing web application for conducting threat modelling: Airbnb, Uber, Netflix, YouTube, Amazon

Ebay

# Create a use case diagram of your system (What are we building?)

The users will be able to

Create Accounts

Login into Accounts

Sell items

Buy items

Buy Items without signing up

Place bids

Hold bids

Put items on sale

Take items off sale without a purchase

# Create 2 abuse cases and 2 misuse cases for your system (What could go wrong?)

Abuse cases

1. Fake listing
2. Account takeover

Misuse cases

1. The user accidentally takes a listing down thinking it was sold but the auction did not finish.

Use creates product listing with incorrect or incomplete information

1. Buyer mistakenly enters wrong payment details

# Do threat modelling using STRIDE methodology (What could go wrong? And What we will do about it) and create a DFD of the system or 1 flow

Spoofing Identify: Hackers could gain access to a user's details and pretend to be them. To prevent this, we must implement a two-step verification whether that is a use of security key, message to mobile or security question

Tampering: The price of an item with a buy now option may be artificially deflated, then when user presses buy now, they send more money than they thought they would pay. Store the pricing information in different relational database tables.

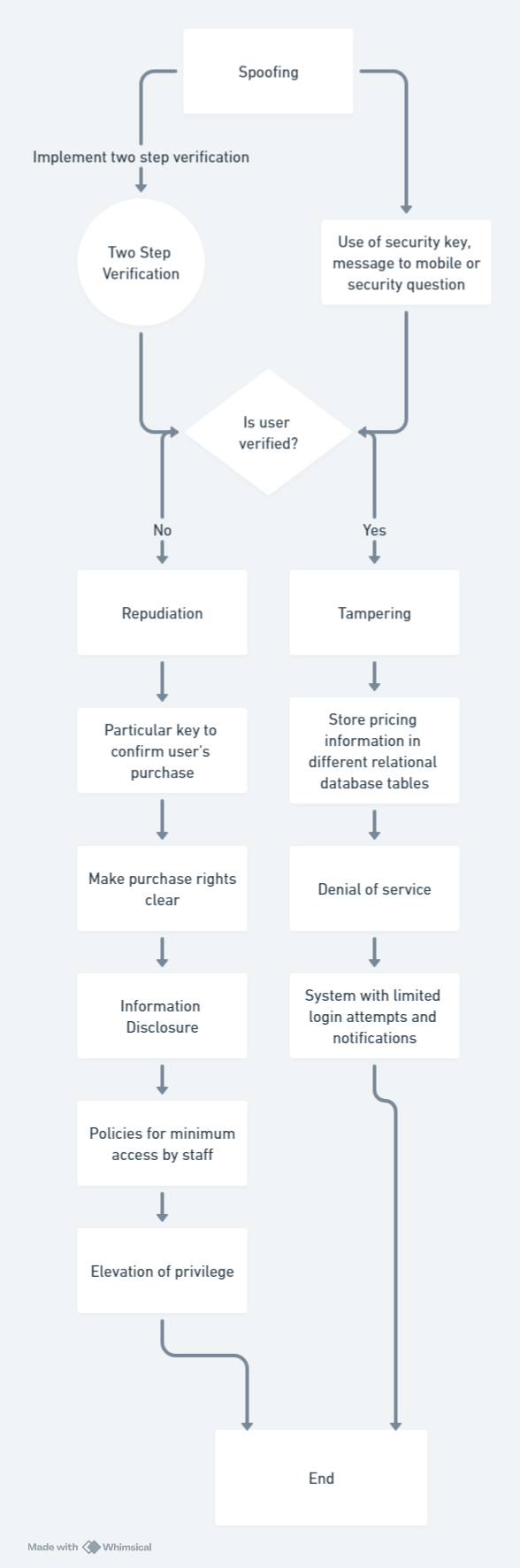
Repudiation: A user made a valid purchase, they realised they could not afford it and tried to claim they did not make the purchase and deserve a refund. To prevent this, we need a particular key to be set up to confirm that the user accepts a purchase. Within this message, we need to make it clear what their purchase rights ar.

Information Disclosure: Someone’s purchase history could be leaked without their consent. We need to employ a policy of minimum access so staff cannot see this unless necessary.

Denial of service: An attacker uses a botnet to flood eBay's servers with excessive HTTP requests, such as constantly searching for items or refreshing product pages. This overwhelms the servers, causing slowdowns or making the site unavailable to legitimate users.To prevent this . **CAPTCHA for Bots**:

Use CAPTCHAs to verify that requests are coming from real users, especially during login or critical transactions.

Elevation of privilege: A user may be able to grant themselves admin permissions and mess with normal accounts, forcefully closing them or altering item prices. To combat this, we follow minimum access policy and admin accounts are secured even safer.



# Define 2 security requirements derived from your analysis of threat modelling

* Implementing MFA for all users: this will add a security layer to all user
* Enforcing data encryption for sensitive information: such as SSL/TSL when communication between client and server

# Show the analysis view in MS Tool, mitigate 5 identified threats, and generate the threat modelling report

Creating system diagram   
Identify threats   
Analyse threats   
Mitigate

# Threat modelling Tools

# Microsoft Thread Modelling ([https://learn.microsoft.com/en-us/azure/security/develop/hreatmodeling-tool](https://learn.microsoft.com/en-us/azure/security/develop/threatmodeling-tool)) – Automated (Download this one, and on the website, go to the “Getting Started” menu to follow the tutorial)

x

# OWASP Threat Dragon (<https://owasp.org/www-project-threat-dragon/>) – Manual

x