Information systems security
Risk assessment: Threat modelling

STRIDE is a model for identifying computer security threats, and Praerit Garg and Loren Kohnfelder at Microsoft developed it. When we think about threats, we ask ourselves questions like:

1. How can an attacker change the data?
2. What is the impact if an attacker can read the data?
3. What happens if a legitimate user can't log into the system?

We can group threats into categories to help analyze such issues. STRIDE is one of the models that can be used for this purpose. It is derived from the acronyms for the following six threat categories:

1. **S**poofing - An example of identity spoofing is accessing and using data to authenticate as another user.
2. **T**ampering - Data modification involves malicious modification of data. Examples include unauthorized changes made to data.
3. **R**epudiation - Threats are associated with users who deny what they have done without the system owner can prove otherwise. Nonrepudiation refers to the ability of a system to prove who made these changes.
4. **I**nformation disclosure – Gaining access to the data one should not have access to.
5. **D**enial of Service (DoS) attacks deny service to legitimate users.
6. **E**levation of privilege - In this type of threat, an unprivileged user gains privileged access and thereby has access to compromise the system.

The simplest way to apply the STRIDE model to an application or system is to consider how each of the model's threats affects the service's components. Essentially, one looks at the components of the service and determines the existence of threats (STRIDE) to that component or process. Most components will have numerous threats. So, one must list them all.

Example of website threats (shortlist):

1. Threat: A malicious user views or changes data in transit from the web server to the client or from the client to the web server. (Information disclosure)
2. Threat: A malicious user views or changes data in transit from the web server to the database. (Information disclosure)
3. Threat: A malicious user browses authentication directories (LDAP) and tries to find a way to present themselves as legitimate user. (Spoofing identity / Information disclosure / Elevation of privilege)
4. Threat: A malicious user changes one or more websites. (Tampering with the data)
5. Threat: An attacker disables access to the database by sending a large amount of TCP/IP packets. (Denial of service)
6. Threat: The attacker deletes or changes logs. (Tampering with dana / Repudiation)

Process: Internet banking (e-banking)

E-banking is the process that allows bank customers to conduct money transactions, apply for a loan, and use other services that the bank offers.
In addition to the functionality the e-banking service provides today, security is among the most critical components.
The e-banking process under consideration in the framework of this exercise includes the activities of the uses of e-banking. The process starts with logging users into the e-banking system and conducting various activities on the e-banking system until the user is logged off.
The process diagram is shown in Figure 1: e-banking process diagram.

E-banking process diagram:

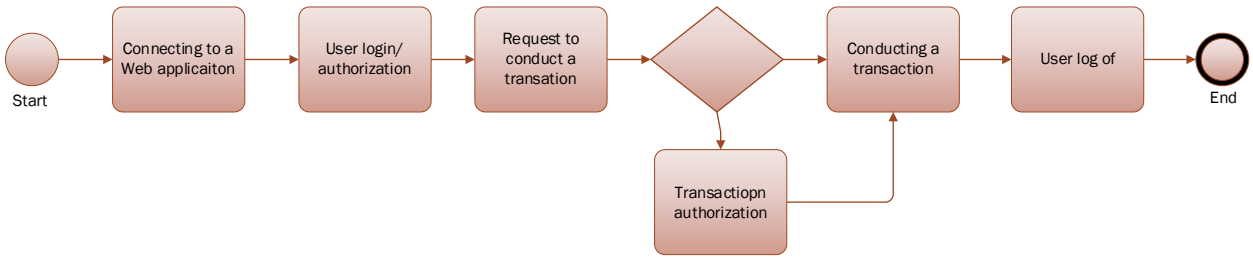

Figure 1: e-banking process diagram

Network schematics with application list:

Figure 2: e-banking network schematics with the application list shows how applications are distributed across servers, i.e., on which physical servers individual applications are installed.

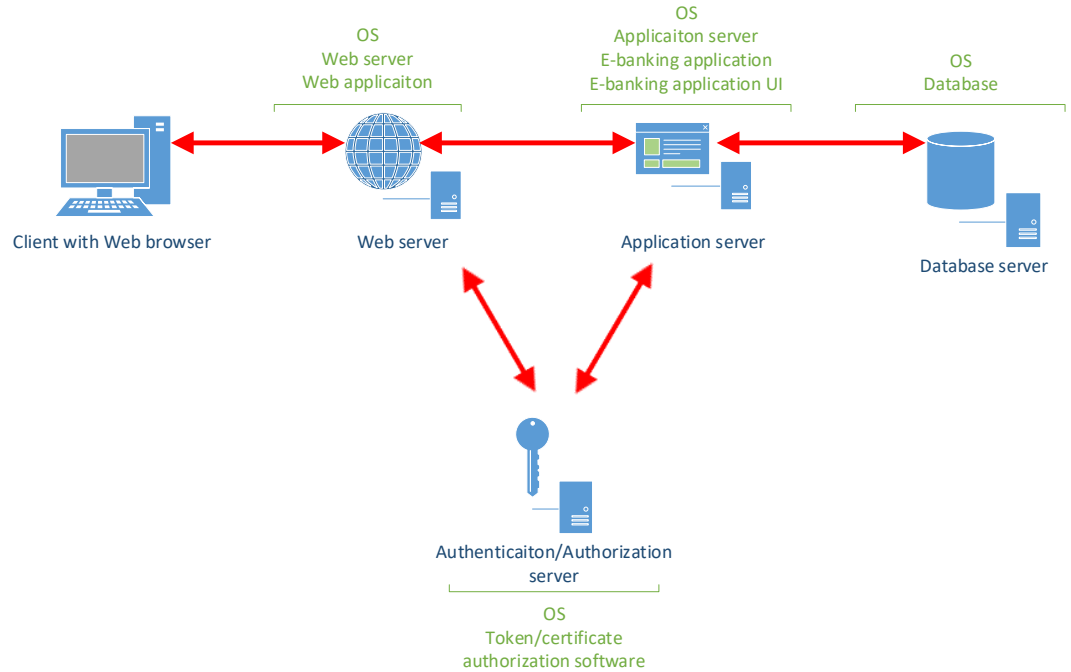

Figure 2: e-banking network schematics with the application list

We will use the EoP game to analyze the threat landscape of the abovementioned application.

More information about the game can be found at https://www.microsoft.com/en-us/download/details.aspx?id=20303&msockid=0cd1b45d1f366ddc0bc8a1c71e776c42. The game exists as the physical cards, but we will use the pdf version. From the above link download `EoP_Card Game Images.pdf` file.

From the card deck, choose 2 cards from each of the STRIDE categories (no A's, please) that could be used to define the vulnerability in e-banking system. Choose one of these and explain the vulnerability and potential fix to the classroom.