Assignment 2 - Threat Modelling

SENG406 - Software Security

Fabian Gilson

22nd July 2025

Preamble

In this assignment, students will apply their newly acquired knowledge in threat modelling, *i.e.*

- they will identify the actors, trust levels, assets, entry/exit points and dependencies of a small-scale software system;
- they will derive one or more data flow diagrams from the requirements of a small-scale software system;
- they will conduct a threat analysis for all elements in the data flow diagrams following the STRIDE framework;
- for each threat, they will propose counter-measures, when applicable;
- they will compile their findings in a technical report.

1 System under study: ShareNote

The system under study is a web-based collaborative note-taking app, called *ShareNote*. The app allows users to create notes, and share them so others can either read or edit notes, depending on permissions set by the creator of the note. Users can also comment on notes. Figure 1 depicts a simplified domain model of this application.

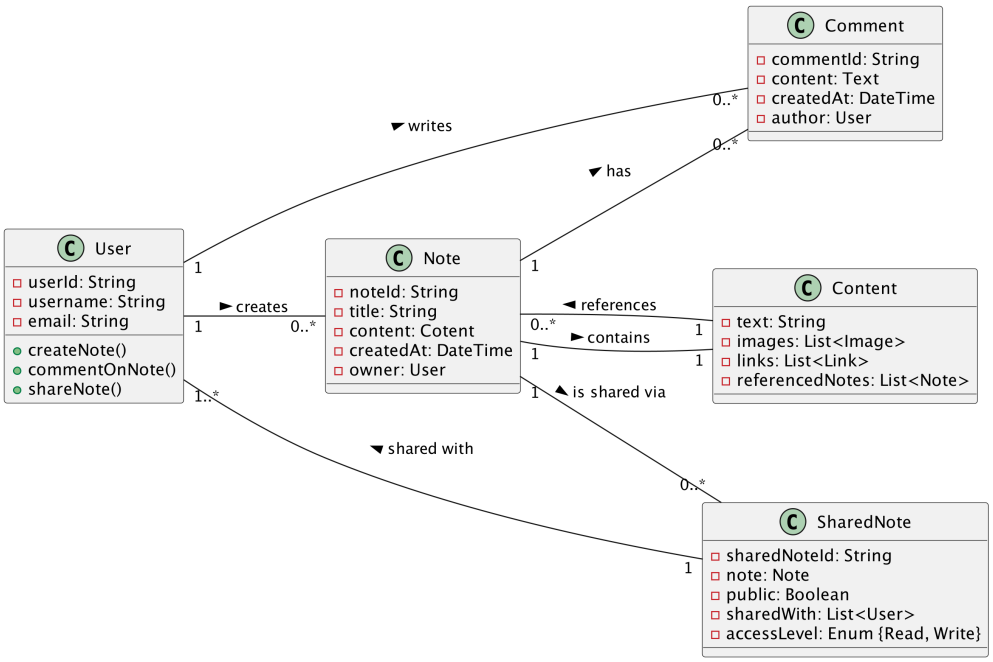

Figure 1: Domain model of the ShareNote application.

In the following, we list the features and constraints of this system.

1.1 Functional features

1.1.1 Create a note

A user can create a note that can be shared with other users. The note can contain text, images, hyperlinks to other webpages, and links to other notes.

1.1.2 Share a note

In order to share a note, the creator of the note can either share it with specific users or make it public. To make a note public, the creator will simply switch a "toggle" and the note will be accessible from the main page of the web application in a read-only mode.

To share a note with specific users, the creator can generate a shared secret link, indicating if the link can be used to read or edit the shared note. They can then share the link with other users either by email or any other way outside the scope of the web application.

1.1.3 Comment on a note

When a note is either public or shared with other users, users having access to the note can comment on the note. Comments are text only.

The creator of the note can delete comments, but other users cannot. Comments are visible to all users having access to the note, and they can be used to discuss the content of the note.

1.2 Additional constraints and non-functional requirements

Here is a list of additional constraints for this system:

- The web application is available publicly on a website, accessible from both desktop and mobile devices.
- The web application is only available via HTTPS, and the data is encrypted in transit.
- The system is deployed on premises, and the data is stored in a database on premises too.
- The web application is deployed on a server protected by a firewall, and a reverse proxy is used to handle requests.
- The database is not directly accessible from the internet, and only the web application can access it.

Important note: The features of the web application are described in a simplified way, and you are expected to make some assumptions about the system, if needed. If you make additional assumptions, you must clearly state them in your report, next to the list of dependencies (see section2.1). **Do not add assumptions that contradict the existing features or constraints of the system.**

2 Submission requirements

You are expected to submit your analysis of the system **as-is**. You are not expected to change the system, but rather to analyse it as it is described in this document.

1. a PDF report presenting your threat modelling and analysis of the system. Use Threat Dragon to guide your reflection. However, the generated report from that tool may not contain all information that we expect (e.g., actors, trust levels) so you will have to append the content of the generated report into a complete PDF report, or to structure your report similarly to the example used in lab 1.
2. the **JSON** model exported from *Threat Dragon*.

2.1 Expected content of report

Your report must explicitly refer to the authors' names, have a descriptive title, and display the date when the report was due (not finalised, without considering the grace period). All sections must be clearly **numbered and**

identified with a descriptive title. At the end of the report, each student must disclose their contribution to the assignment depicting:

- what sections of the report they worked on; and
- the overall percentage contributed to the report.

Additionally, you must include a declaration of usage of Generative AI models where you state whether or not you used Generative AI models to edit any part of the report. The declaration must be included at the end of the report. Per this course's policy, the usage of Generative AI models is restricted to editing and formatting the report, but not for the content of the report. **You must not use Generative AI models to write any part of the report, nor to generate any data flow diagrams or threat analysis.**

We expect your report to contain the following sections. The marking schedule is given between *[brackets]*, for a total of **100 marks**, weighting 20% of the course total grade. A good reference to guide your process is available on the OWASP website[1] and the simplifed example used in lab 1:

1. an exhaustive list of **actors** of the system *[2.5 marks]*;
2. an updated list of the **dependencies** of the application that you have identified (see section 1.2), as well as any additional assumptions you made *[2.5 marks]*;
3. an exhaustive list of **trust levels** (also called "privilege" level in *OWASP Threat Dragon*) *[5 marks]*;
4. an exhaustive list of the foreseen **entry/exit points** of the system *[10 marks]*;
5. an exhaustive list of **assets** *[10 marks]*;
6. from the *Threat Dragon* report (you can append the report generated by Threat Dragon to your report):
   (a) one or more data **flow diagrams** depicting the system *[20 marks]*;
   (b) for all relevant diagram elements (i.e. actors, processes, data-flow, stores), a list of STRIDE **threats** and their **countermeasures** *[30 marks]*;
7. a critical discussion of potential improvements to the system's functioning if you believe some **functional aspects** of the system are insecure; for each proposed change, a threat analysis must be conducted *[20 marks]*

2.2 Practical details of submission

You must submit both a PDF and the JSON *Threat Dragon* model named `seng406_asg2_groupX` where "X" is your group number on Learn. You need to submit before **Friday 8 August 2024 at 8PM** with a 5-day grace period, meaning that you can submit up to Wednesday 13 August 8PM with no penalty. No other extension will be granted unless approved by the course supervisor **prior the due date**, *i.e.* no exceptional extensions will be granted past the due date.

You have to register yourself in a group before **Friday 1 August 2024 at 8PM**. After that date, you will not be authorised to submit an assignment and will be awarded 0 marks for this assignment.

2.3 Academic integrity

Academic integrity is a principle at the University of Canterbury whereby both staff and students agree to act honestly, fairly, ethically and with respect for each other in teaching and learning. For some students, there may be increased temptation to cheat and engage in dishonest academic practices such as:

Plagiarism using someone's ideas and information without acknowledging them as the source, this includes the undisclosed usage of Generative AI models such as ChatGPT, or Claude;

Self-plagiarism where someone attempts to submit their own writing to two different assessments to gain credit twice;

Collusion copying the work of someone else or allowing someone else to copy your work without disclosing this with the intent to deceive;

Impersonating/Ghost writing having another person, commercial organisation, or Generative AI tool (e.g., ChatGPT, Claude) impersonate you and complete an assessment item on your behalf;

Fabrication "inventing", data for example in a lab report or from a publication.

[1] See `https://owasp.org/www-community/Threat_Modeling_Process`.

Declaration:

By **taking part to** and **completing** this assignment,

1. I confirm that I have **read and understood the expectations** of the assignment and the **Academic integrity** principle.
2. I understand that the **assignment is considered confidential (within a group)** and I should not share detailed information with others (outside my group).
3. I understand that **the usage of Generative AI models** is restricted for this assignment to editing and formatting the report, but not for the content of the report. I will not use Generative AI models to write any part of the report, nor to generate any data flow diagrams or threat analysis. I will indicate in the report if I used Generative AI models to edit any part of the report.
4. I understand that **failure to comply** with these requirements may mean that **the matter will be referred to** the Head of Department, Dean or **Proctor** as appropriate for disciplinary action.