Analysis Class Diagram over Problem Domain

Author: Victoria, Luca

Responsible: Victoria

Description: <https://learnit.itu.dk/mod/page/view.php?id=186437>

|  |  |  |  |
| --- | --- | --- | --- |
| Version | Change | Author | Date |
| 0 | Added ChangeLog (change me) | Peter | 22/09 |
| 1 | Added class event table, class diagram and descriptions of these | Victoria | 08/11 |
| 2 | Added more detailed description of the process and relations in the class diagram | Luca | 09/11 |
| 3 | Reviewed | Cecilie | 09/11 |
|  |  |  |  |
|  |  |  |  |
|  |  |  |  |

Problem domain analysis

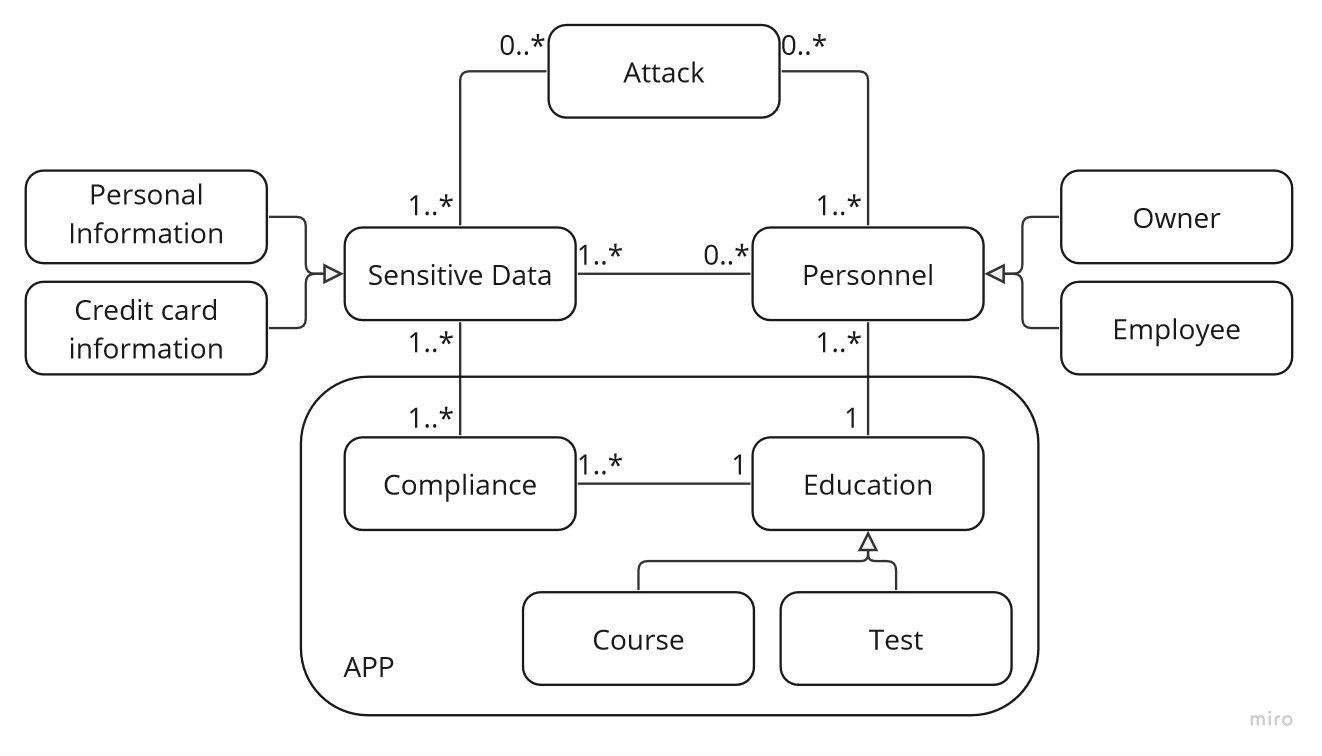
Class event table

After iterating on the class event table many times, we simplified which classes should be incorporated. Previous versions might have included classes such as ‘PC’ or ‘Regulator’, which might not have a direct implication for our Problem domain.

As our Problem-domain is ‘only’ about securing, educating and awareness we simplified which classes needed securing or education. In this case ‘Sensitive-Data’ and the ‘Owner’ and ‘Employee’ are specific targets for our Problem-domain.

|  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- |
| Events | Owner | Employee | Courses | Tests | Comp-liance | Sensitive  data | Attack |
| Employee accessed data |  | x |  |  |  | x |  |
| Starts course | x | x | x |  |  |  |  |
| Owner starts a course on data security | x |  | x |  |  | x |  |
| Owner starts a course on compliance | x |  | x |  | x |  |  |
| Owner starts a course on awareness of attacks | x |  | x |  | x |  | x |
| Employee got fished from a malicious email |  | x |  |  |  | x | x |
| Owner chooses what courses employees should start | x |  | x |  |  |  |  |
| Change system to adhere to new regulation | x | x |  |  | x |  |  |
| Removing data due to compliance | x | x |  |  | x | x |  |
| Sensitive data is stolen |  |  |  |  |  | x | x |
| Deploys phishing test | x | x |  | x |  |  |  |
| Fails a course | x | x | x |  |  |  |  |
| Fails a test | x | x |  | x |  |  |  |
| Detecting mail as phishing mail | x | x |  |  |  |  | x |
| Credit card information is stolen |  |  |  |  |  | x | x |
| Personal information is stolen |  |  |  |  |  | x | x |

Class diagram

*Resulting class diagram*

With the Class event Table our final Class Diagram is as above. This encapsulates our events in an overview and makes it understandable how each class interacts with each other. We are omitting a direct event which would connect ‘Compliance’-’Personnel’, as we feel that the events are encompassed with their common association ‘Sensitive Data’ and ‘Education’.

[Figure 3] shows our process of creating the final Class Diagram. It shows our refinement on our Problem domain. As a new class ‘Access Control’ was added in Iteration-2, as a target for attack, but also as a way for ‘Owner’ and ‘Employee’ to be associated with the ‘Sensitive Data’. In the same iteration, the removal of ‘Compliance’ was done. As we went back-and-forward how to integrate ‘Compliance’ in the diagram.

Iteration-3 shows diagram structure where ‘Compliance’ is not only a crucial part of the Problem Domain, but also a part of the ‘App’ Cluster. ‘Access Control’ was removed as we re-worded our Event Table to simplify the association between the ‘Personnel’ and ‘Sensitive Data’.

Explanation of each Class/Interface in the Class Diagram:

**Attack**

This class pertains to external threats, with a primary focus on phishing attacks, as evident in the event table. The targets of such attacks can include sensitive data and personnel, contingent on the malicious intent involved. We see this class being instrumental in understanding the context of the Problem Domain.

**Personnel, Owner, and Employee**

Personnel serves as an interface encompassing both business owners and employees. This interface was established due to the frequent occurrence of shared events that are relevant to both parties – see class event table and picture of the iterations below. The distinction between the owner and employee is vital for a comprehensive understanding of the problem domain, specifically the context of small businesses. Personnel may or may not possess access to sensitive data, depending on the circumstances.

**Sensitive Data, Personal, and Credit Card Information**

Sensitive data remains a constant presence in the daily operations of small businesses, necessitating their preparedness for security breaches and regulatory changes. The ideal approach entails a commitment to preventive measures against potential attackers. Sensitive data encompasses various types, including personal and credit card information, offering insights into the kinds of data that could be targeted in a breach. While we considered other classes such as 'cloud drive,' sensitive data was deemed a more fitting classification for encapsulating the primary concern.

**Education, Course, and Test**

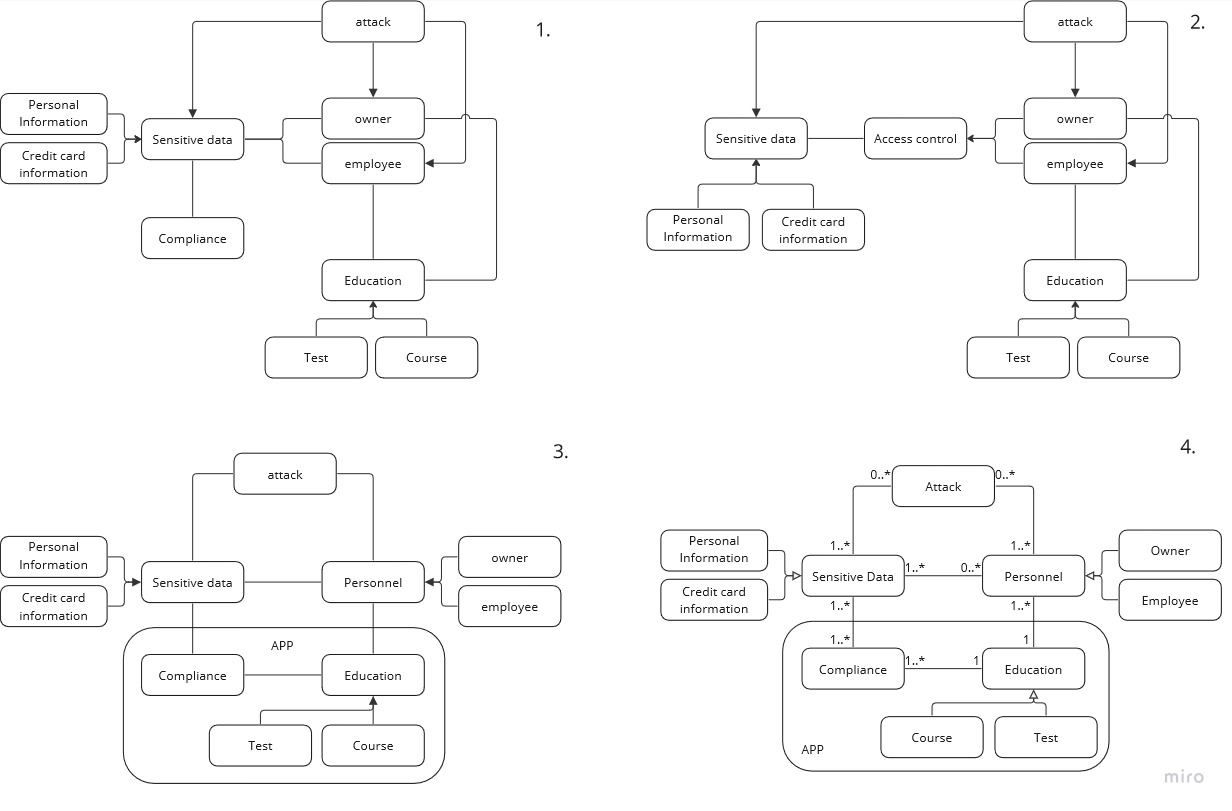
Education serves as a manifestation of the imperative need for awareness and information updates to ensure the safety of the business, its personnel, and customers. Our research underscores the significance of fostering awareness and providing educational resources. Within this context, 'Education' comprises various types, represented by objects such as 'Courses' and 'Tests.' These tools enable personnel to enhance their skills and adapt to new regulations or emerging threats.

**Compliance**

The compliance class functions akin to a regulatory body, influencing the operational practices of businesses. Compliance requirements significantly impact the education and training programs that personnel must undergo, as well as the procedures for handling and storing sensitive data. It is important to note that multiple compliance standards may apply to various pieces of sensitive data.

**Cluster App**

The completion of the class diagram enhances our understanding of the elements in the problem domain that are conducive to the development of an application, with a particular emphasis on the educational component. Additionally, we are exploring the possibility of implementing a system to monitor personnel's access to sensitive data.

*Construction of the class diagram: starting from first iteration 1 to 4 - the resulting diagram*