J. Irvine Secure Software Development

Faceted Data

Read Schmitz et al (2016) article about faceted data.

- Do you think this is a good approach to protect systems from data leakage? What are the pros and cons?

Faceted data is a technique used to protect systems from data leakage by breaking up sensitive data into smaller pieces or facets. Each facet contains only a subset of the original data and is stored separately from the other facets. This makes it more difficult for an attacker to gain access to the entire dataset if they are able to compromise one facet.

The main advantage of faceted data is that it provides an additional layer of security for sensitive data. By breaking up the data into smaller pieces, it reduces the risk of a complete data breach if one facet is compromised.

However, there are also some disadvantages to using faceted data. One disadvantage is that it can be more difficult to manage and maintain than traditional data storage methods. Another disadvantage is that it can be more difficult to query and analyse the data when it is stored in multiple facets.

Faceted data can be an effective way to protect sensitive data from leakage, but it should be used in conjunction with other security measures such as access controls and encryption.

Schmitz, T., Rhodes, D., Austin, T.H., Knowles, K. and Flanagan, C., 2016, April. Faceted dynamic information flow via control and data monads. In International Conference on Principles of Security and Trust (pp. 3-23). Berlin, Heidelberg: Springer Berlin Heidelberg.

- Create a basic outline design of how you would create such a system in Python.

To create faceted data programme in Python you would:

- Identify any sensitive data that needs to be protected (GDPR).
- Breakdown any sensitive data into smaller pieces or facets.
- Use access controls or encryption to safely store facets. (GDPR)
- Manage and maintain facets in a database or file system.
- Use a data analysis tool to query and analysing the facets