Lecture 10 - 10/08/2019

Database Security

Data is the most valuable asset and is the one thing that must be protected at all costs.

RBAC for databases

Role-based access control eases administrative burden

Inference

Inference is a user getting making a legitimate query and using some outside knowledge to infer some sensitive data that they should not have access to.
E.g. getting an average salary and being able to infer the salary of an individual.

Tracker Attacks

If a user can only select a certain amount of values, they can select two sets of that size and infer a small set from those two larger sets.

Inference Prevention

Data Swapping

Shuffle data around so that the original rows no longer line up. This can be useful so the statistics are still valid but the attacker can not access what he used to be able to access.

Perturbation

Give data that is similar to the real answer but is different enough so that an attacker can not get the exact data and infer sensitive data from it.
https://en.wikipedia.org/wiki/Perturbation

Database Encryption

- The database is typically the most valuable
- Encryption often implemented with particularly sensitive data
- Encryption can be done in transit or with resting data