Customer Data Leakage Prevention

Goals

Protecting sensitive customer information from unauthorized disclosure is a major concern of every company. Since the company’s employees need to access customer information, customer data leakage prevention is a very complex task.

Description

In this research we reviewed state-of-the-art commercial and academic data leakage prevention solutions. Then we developed and evaluated various data misuse detection methods which include:

- **Anomaly detection** using a novel supervised and unsupervised context-based data linkage algorithm that is used to derive normal access patterns and detect abnormal access patterns that may indicate customer data leakage/misuse incidents.

- **M-Score** – A Misuseability Weight measure that assigns a sensitivity rank to datasets accessed by employees which indicates the potential damage to the organization in the event that the data is misused.

- Employ the concepts of **honeytokens** for detecting data misuse incidents, and answering questions such as how to use the honeytokens effectively, how to generate reliable honeytokens, and how many to create.

- An improved **collaborative e-mail leakage prevention** method that analyzes the communication of groups of users.

In order to evaluate our proposed method we developed an evaluation environment and a detection system prototype.