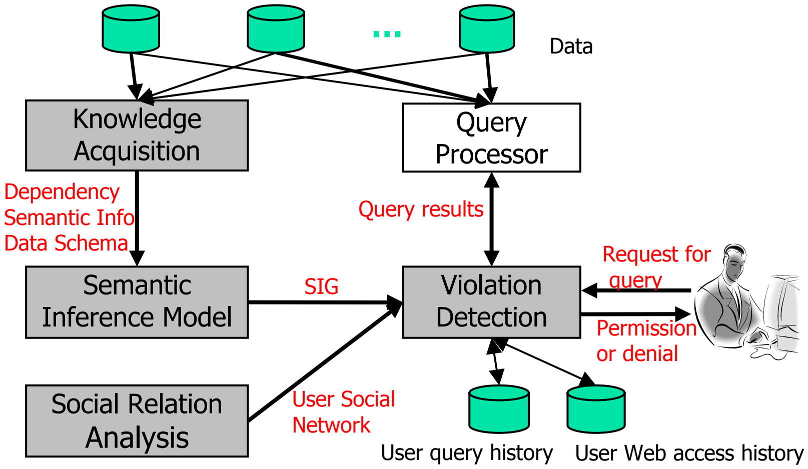
PROTECT DATABASE SECURITY VIA COLLABORATIVE INFERENCE DETECTION

Yu Chen and Wesley W. Chu
UCLA Computer Science Department

Introduction:

Malicious users can infer sensitive information from a series of seemingly innocuous data access. Thus, we develop an inference violation detection system to protect sensitive data content.

Methods:



Inference channels can be used to provide a scalable and systematic sound inference. Thus, we need to construct a semantic inference model (SIM) that represents all the possible inference channels from any attribute in the system to the set of pre-assigned sensitive attributes. The SIM can be constructed by linking all the related attributes which can be derived via attribute dependency from data dependency, database schema and semantic related knowledge. To reduce inference computation complexity, the instantiated SIM can be mapped into a Bayesian network. Thus, we can use available Bayesian network tools (e.g. SamIam [3]) for evaluating the inference probability along the inference channels. For a single user, when a user poses a query, the detection system will examine his/her past query log and calculate the probability of inferring sensitive information. The query request will be denied if it can infer sensitive information with the probability of exceeding the pre-specified threshold [1]. For multi-user, the users may collaborate with their query answers to increase the probability of inference sensitive information. We can construct a task-sensitive social network based on the users' profiles and questionnaire data [2], which can be utilized to derive *collaboration levels* among users. Collaborative inference from multiple users can be derived based on their respective *collaboration levels*, their corresponding query log sequences and the relationship with the inference channel (e.g. with or without overlap) for the sensitive information.

Conclusions:

We have developed a detection system that prevents single users from inferring sensitive information by a series of innocuous queries. We are currently extending the detection system for multiple collaborative users that is based on their query histories as well as their social relations.

[1] Y. Chen and W. W. Chu. "Database Security Protection via Inference Detection." *IEEE International Conference on Intelligence and Security Informatics*, May 2006.

[2] J. He, W.W. Chu, and Z. Liu. "Inferring Privacy Information From Social Networks." *IEEE International Conference on Intelligence and Security Informatics*, May 2006.

[3] SamIam by Automated Reasoning Group, UCLA. http://reasoning.cs.ucla.edu/samiam/