Data is Social: Exploiting Data Relationships to Detect Insider Attacks

PIs: Oliver Kennedy, Varun Chandola, Shambhu Upadhyaya, Hung Ngo (UB), Long Nguyen (UMich)

http://odin.cse.buffalo.edu/research/insider-threats/index.html

CNS-1409551, CNS-1409303

Project Objectives

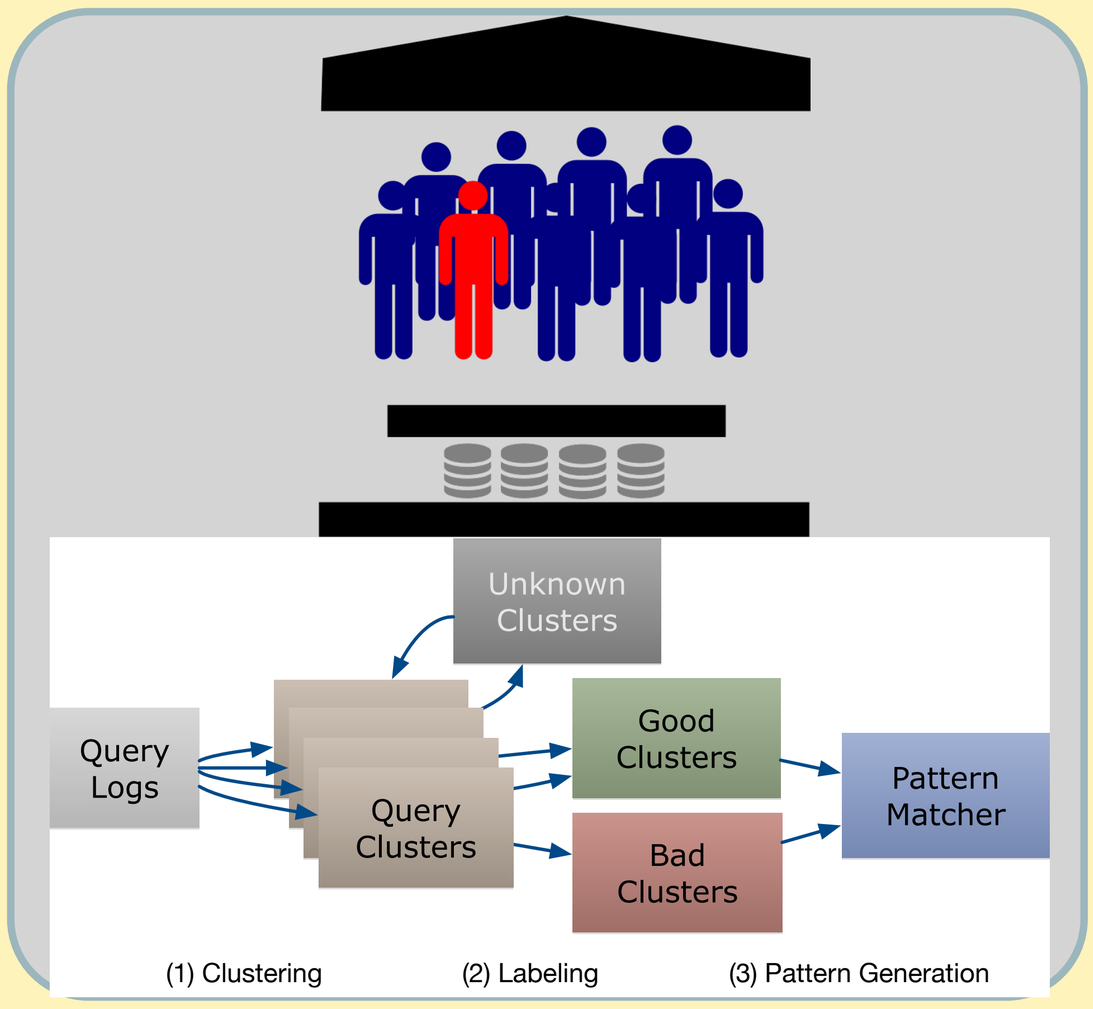
Develop methods to understand and identify insider threats posed by malicious insiders within large organizations.

Insider attack is an extremely serious and pervasive security problem. For obvious reasons, an insider attack has the highest damaging potential for an organization.

Handling insider threat is challenging, both in terms of defining the insider threat and distinguishing between normal and malicious behavior of authorized actors within an organization.

- Data access patterns reveal query semantics.
- We have developed a system, **Ettu**[1], a system that uses query intent modeling as a way to flag potential insider attacks.

[1] Ettu is derived from the last words of the Roman emperor Julius Caesar, "Et tu, Brute? " in Latin, meaning "You, too, Brutus?" in English to emphasize that this system is meant to detect the unexpected betrayals of trusted people.



Approach

- Develop a cyber ontology for modeling insider threats in the financial sector
- Use the intent to develop profiles for members of the organization
- Develop methods to detect deviations from user profiles as potential insider threat
- Develop novel approaches to compute query similarity for modeling intent
- Develop new tools for hierarchical clustering and statistical inference for complex structures such as queries

Query Log Exploration

- Surveyed various query similarity detection techniques
- Tested against realistic workloads obtained from a financial organization
- Created a benchmark for query similarity assessment.

Topic Modeling

- Developed a geometric algorithm for topic learning and inference
- Built on the convex geometry of topics in order to navigate through large logs and archives, and estimate related topics.

Threat modeling

- Created an insider threat ontology aiming to model the insider threat in the financial domain.
- Potential to integrate the ontology with other commonly used upper ontologies

Publications and Products

- G. Kul, D. Luong, T. Xie, P. Coonan, V. Chandola, O. Kennedy, and S. Upadhyaya, Ettu: Analyzing query intents in corporate databases, in Proceedings of the 25th International Conference Companion on World Wide Web, 2016, pp. 463–466.
- G. Kul, D. Luong, T. Xie, P. Coonan, V. Chandola, O. Kennedy, and S. Upadhyaya, Summarizing large query logs in Ettu, ArXiv 2016..
- G. Kul and S. Upadhyaya, Towards a cyber ontology for insider threats in the financial sector, Journal of Wireless Mobile Networks, Ubiquitous Computing, and Dependable Applications, 6 (2016), pp. 64–85.
- M. Yurochkin and X. Nguyen, Geometric Dirichlet Means algorithm for topic inference, NIPS, 2016.
- EttuBench – A SQL Query Similarity Metric Benchmark, https://github.com/UBOdin/EttuBench
- The UB Exam Dataset - http://odin.cse.buffalo.edu/public_data/2016-UB-Exam-Queries.zip

Interested in meeting the PIs? Attach post-it note below!