Anomaly Analysis Framework for Database Systems

Sokratis Vavilis, Alexandru Egner, Milan Petković and Nicola Zannone

Technische Universiteit Eindhoven University of Technology

Security Incidents in DBMS

Situation

- DBMS central role in organizations – Massive storage of data
- DBMS attractive for attackers
  - One of the most compromised assets [Verizon 2014]
- Strict data protection regulation in force

Anomaly Detection Systems (ADS)

- High number of alerts
- No insight on the security incident
- Difficult management & mitigation of damages

Security Analysis of Alerts

Alert Analysis should

- Provide insight / understanding on the alerts
  - Root causes, Attack information, Contextual Information (e.g. Time)
- Determine alert criticality
- Facilitate alert management

Existing Approaches

- Limited or no information of alerts
- Criticality – Partial view
  - Focus only on anomaly level
  - Focus only on data / content

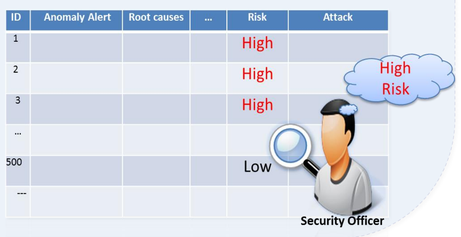
Proposed Approach

Objective

- Assist security officer in the analysis of alerts

Unified framework for analysis of alerts

- Risk-based Quantification of Alerts
- Feature-based Attack Classification
- Alert visualization - Analysis



Risk-based Quantification of Alerts

Risk based approach

- Anomaly Level
- Severity

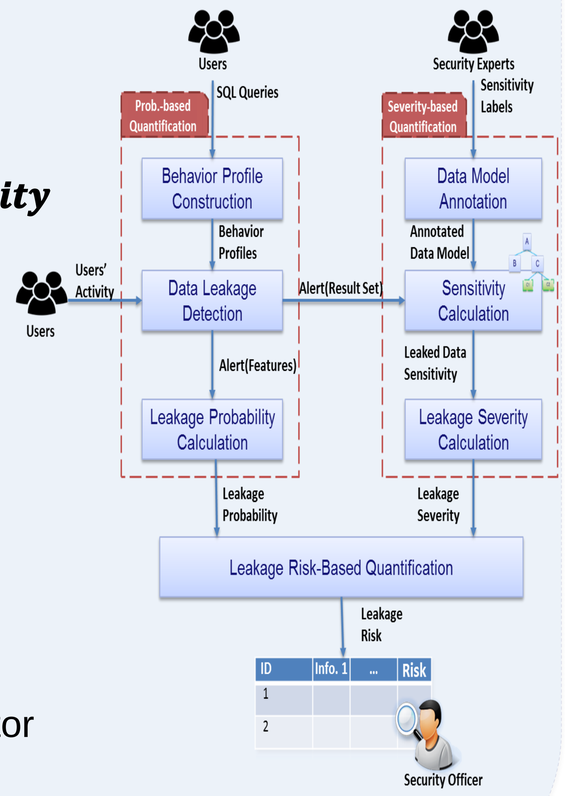
$$Risk = AnomalyLevel \times Severity$$

Anomaly Level

- Rich set of features
  - Behavior profiles
- Root causes of anomaly

Severity

- Data Sensitivity
- Data Quantity
- Data Subject Identifiability factor



Feature-based Attack Classification

Database Attacks

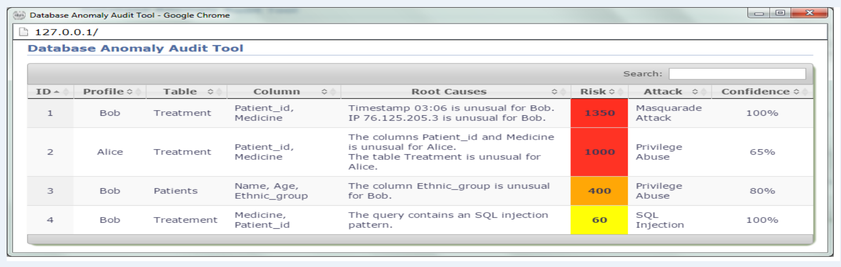
- Single Query
  - Privilege Misuse
  - Masquerade Attack
  - SQL Injection
  - Resource Consumption
  - Error-code analysis
- Multiple Query
  - Password Guessing
  - Query Flood

	Syntax-centric Features							
Attacks/Features	**Command**	**Column List**	**Table List**	**Search Space**	**Length**	**Malicious Patterns**	**Operators/ Functions**	**Syntax Error**
Privilege Misuse	Query	Query	Query	✘	✘	✘	Where	✘
Masquerade Attack	✘	✘	✘	✘	✘	✘	✘	✘
SQL Injection	NQ	Where	Where	✘	Query Where	✔	Where	✘
Resource Consumption	✘	✘	✘	# Tables # Columns # NQ	✘	✘	Where	✘
Error-code Analysis	Query	✘	✘	✘	✘	✘	Query	✔
Password Guessing	✘	✘	✘	✘	✘	✘	✘	✘
Query Flood	✘	✘	✘	✘	✘	✘	✘	✘
Inference Attack	✘	✘	✘	✘	✘	✘	Query	✘

	Context-centric Features				Result-centric Features			
Attacks/ Features	**IP Addr.**	**Timestamp**	**Issuer**	**# Queries**	**Result Set**	**Result Size**	**Response Code**	**Response Time**
Privilege Misuse	✘	✘	User Role	✘	✔	Records	✘	✘
Masquerade Attack	✔	✔	User	✘	✘	✘	✘	✘
SQL Injection	✘	✘	✘	✘	✘	✘	✘	✘
Resource Consumption	✘	✘	✘	✘	✘	Records Bytes	✔	✔
Error-code analysis	✘	✘	✘	✘	✘	✘	✔	✘
Password Guess	✔	✘	User	✔	✘	✘	✔	✘
Query Flood	✘	✘	✘	✔	✘	✘	✘	✘
Inference Attack	✘	✘	✘	✔	✔	✘	✘	✘

Legenda: ✔ Related Feature ✘ Unrelated Feature

Alert Visualization - Analysis

Assist security officer in handling alerts

- Provide insight on the alerts (e.g. root causes, attack type)
- Ranking / grouping based on different aspects
- User-friendly visualization