University of Zurich[UZH]

Department of Informatics

University of Zürich
Department of Informatics
Binzmühlestr. 14
CH-8050 Zürich
Phone. +41 44 635 43 11
Fax +41 44 635 68 09
www.ifi.uzh.ch/dbtg

UZH, Dept. of Informatics, Binzmühlestr. 14, CH-8050 Zürich

Prof. Dr. Michael Böhlen
Professor
Phone +41 44 635 43 33
Fax +41 44 635 68 09
boehlen@ifi.uzh.ch

Zürich, 10. Mai 2017

BSc Vertiefungsarbeit
Topic: Detecting Anomalous Access Patterns in Role-Based Relational Databases

Attacks on relational database systems are a severe security threat to many enterprises. The most common attack vector are SQL injections carried out on vulnerable webpages. Another threat that is more difficult to detect and prevent are insider attacks; in this scenario employees that already have access to a database try to tamper with the database (steal, manipulate or delete data).

Kamra et al. [1] propose an intrusion detection (ID) system for relational databases that mines the audit log of the database to find a set of allowed queries per *role*. In a role-based access control (RBAC) database every user is assigned to one or many roles. The ID-system builds a classifier that automatically decides if an incoming query is anomalous for the role(s) of the user. If the query is anomalous, different actions can be taken, e.g. the query can be silently dropped and/or a database administrator can be notified.

The goal of this project is to study and understand the ID-system proposed by Kamra et al. [1]. In particular, the student should understand the complete pipeline starting with (i) a query entering the system, (ii) the feature extraction phase into quiplets, and (iii) the classification of the query with a Naive Bayes Classifier.

Tasks

1. Study and understand the intrusion detection system presented in [1] with a focus on role-based anomaly detection.
2. Describe an example workload that leads to malignant queries being classified as benign and vice versa.
3. Summarize your work in a short report (approximately 10 pages)

Optional Task

1. Implement role-based anomaly detection [1].
2. Evaluate your implementation on a synthetic dataset.

References

[1] A. Kamra, E. Terzi, and E. Bertino. Detecting anomalous access patterns in relational databases. *VLDB J.*, 17(5):1063–1077, 2008.

Supervisor: Kevin Wellenzohn (wellenzohn@ifi.uzh.ch)

Start date: 9 May 2017

End date/Oral exam: 27 June 2017, 15:00

University of Zurich
Department of Informatics

Prof. Dr. Michael Böhlen
Professor