Detecting, Monitoring and Preventing Database Security Breaches in Housing-Based Outsourcing Model*

T. K. Dang[1], T. T. Q. Nguyet[2], and T. Q. Chi[3]

Abstract: Outsourcing database services is emerging as an important new trend thanks to the growth of the Internet and advances in the networking technology. Therein, organizations can outsource their data management needs to external service provider(s), and thereby freeing them to concentrate on their core business. Basically, there are two popular methods of this outsourcing model: the *hosting* service and the *housing* service. In the former, the service provider provides servers and maintenance activities for the clients. Meanwhile, in the other method - housing service model, the servers are the property of the client and the client themselves installs the servers. In this case the outsourcing service provider only provides the *physical* security of machines and data, monitors (and if necessary restores) the operating condition of the client server. However, concerning security issues in the *housing* service business model, *soft* security-related aspects are usually ignored or understood that "the installed software (or the client) must be responsible for it". Therefore, the housing service provider needs to provide the client with means (e.g., tools/softwares) capable of detecting the database security flaws and visually and *securely* monitoring real-time activities of users having the managerial rights, especially with respect to the possible database security flaws. Besides, solutions to prevent abused database operations of malicious users at the service provider side must also be in place to guarantee the system reliability.

The focus of this paper is to propose an extensible framework for the system to make sure that all concerned security requirements are guaranteed. This system can help in addressing the problem of both *outsider* and *insider* threats. It is also well suited for the detection of *predefined* as well as *potential* security flaws. Our solution to the database security flaws detecting phase is inspired by the well-known *pentesting*- and data mining-based ones in network security. Moreover, the system administrator can also monitor visually and securely all activities of users who are accessing the database system in real time. By secure monitoring we mean that all concerned activities will be recorded despite the client-server network status. Based on the results of the detecting and monitoring phase, the system will be able to send warning messages or conduct proper preventing actions if it detects the risks which may violate the security policy. A prototype for Oracle based on the proposed framework has been implemented and empirical experiments have confirmed our theoretical analyses as well as shown the efficiency of our approach.

(*) This paper is partly financed by Mitani Sangyo Co., Ltd., Japan under contracts No. 010308/HCMUT-MITANI and 151008/HCMUT-MITANI.

[1,2,3] Faculty of Computer Science and Engineering, Ho Chi Minh City University of Technology
268 Ly Thuong Kiet Street, District 10, Ho Chi Minh City, Vietnam
{*khanh, ttqnguyet, tqchi*}*@cse.hcmut.edu.vn*