International Journal of Innovative
Computing, Information and Control
Volume **6**, Number **3(B)**, March **2010**

ICIC International ©2010 ISSN 1349-4198
pp. **1313–1324**

NOVEL METHODOLOGIES TO DETECT COVERT DATABASES

Keun Gi Lee, Joon Ho Choi, Kyung Soo Lim, Seokhee Lee and Sangjin Lee

Digital Forensic Research Center
Korea University
Anam 5ga, Sungbuk gu, Seoul, Republic of Korea
{ lifetop; reaper9; lukelim; gosky7; sangjin }@korea.ac.kr

Received December 2008; revised June 2009

Abstract. *Companies have substituted paper based systems with IT systems, such as DBMS (Database Management System), EDMS (Electronic Document Management System), and ERP (Enterprise Resource Planning) system. We should focus our attention on discovering sensitive information in a database server, since the majority of corporations use DBMS. However, concealment is difficult to observe and detect, because perpetrators do their best to hide their illegal activities. In particular, we need to consider the case of a covert database server.*

This paper proposes methodologies to detect covert database servers that would be helpful to forensic investigators. Therefore, we describe an example of a covert database server and suggest several detection techniques. Finally, we provide an investigation scenario that applies our methodology in the real world.

Keywords: Digital forensic, Database, Hiding, Network searching

1. **Introduction.** Corporations organize their information using database management system infrastructures, such as Oracle Database, Microsoft SQL Server, MySQL, IBM DB2, IBM Informix, Sybase SQL Server and PostgreSQL. Current database technology is based on distributed network and administration automation. Improving database technology minimizes data redundancy, whilst maximizing data integrity, secure data sharing and advanced security. However, it is difficult to discern a database system among many systems during an incidence response. In addition, a corporation might not operate correctly by concealing their database server. Thus, investigation might be deterred. Although the accomplices could intentionally hide the database system, investigators must demand computer data submission based on reliable electronic evidence.

For the purposes of this paper, we have collected live data and network information using network search technologies. This paper is organized as follows. First, we provide background knowledge, giving examples of hidden database systems. Second, we illustrate a scenario with covert database systems. Finally, we outline a suitable methodology to find databases in several investigation environments.

2. Background.

2.1. An example of hidden system.

In the work of [1], Figure 1 illustrates a situation where clients usually have access to the normal database server through the main server system that manages the database server. However, they are unaware of the existence of the covert database server. The specific client usually has access to the normal database server or the covert database server through their main server system. This client can also directly access the covert database server to conceal confidential information. If a forensic