Jurnal Teknologi Maklumat & Multimedia **1**(2004): 73-89

New IV-Based Database Encryption Scheme Using TS Block Cipher

ZAILANI MOHAMED SIDEK, NORBIK BASHAH IDRIS & HARIHODIN SELAMAT

ABSTRACT

Current database security research classify four types of controls for the protection of data in databases: access controls, information flow controls, inference controls, and cryptographic controls. This paper covers the fourth type of controls, cryptographic controls in database security that provides security of data stored in commercial RDBMS like Oracle. The proposed database encryption scheme is based on TS Block and Stream Ciphers, and is capable of protecting data at the data element, row, and column levels using both block and stream encryptions. The design of the scheme's key generation and management system allows the controls of users' access to encrypted data in a multilevel fashion thus provide multilevel security. The scheme solves the problem of mandatory and discretionary access controls in a given organization. The security of the scheme is based on the fact that no cryptographic keys are stored in the database system. All encryption and decryption keys are stored securely in smartcards thus providing minimum cryptographic information to users. The design of the encryption scheme is based on the provably strong ciphers with 128-bit keys which is currently infeasible to be broken even by exhaustive key search. Implementation of the scheme has been conducted successfully in Oracle RDBMS and complements the Oracle encryption security available.

ABSTRAK

Penyelidikan masa kini dalam bidang keselamatan pangkalan data mengelaskan empat jenis kawalan bagi mengawal keselamatan data iaitu kawalan capaian, kawalan aliran maklumat, kawalan inferens dan kawalan kriptografi. Kertas ini menerangkan kawalan jenis keempat iaitu kawalan kriptografi yang dapat menyediakan keselamatan data bagi suatu sistem pengurusan pangkalan data hubungan komersial seperti sistem Oracle. Skema pengenkriptan pangkalan data yang di cadangkan ini adalah berdasarkan sistem-sistem sipher "TS Block" dan "TS Stream". Skema ini dapat memberi keselamatan data pada aras unsur data, baris dan lajur data menggunakan kaedah pengenkriptan blok dan "stream". Reka bentuk sistem penjana dan pengurusan kunci kriptografi dapat mengawal pengguna mencapai data yang telah di enkripkan secara berbilang aras. Ini dapat memberi ciri keselamatan data berbilang aras (multilevel security). Skema ini mendapat ciri keselamatannya berdasarkan atas fakta bahawa tiada kunci kriptografi di simpan dalam sistem pangkalan data tersebut. Oleh itu maklumat kriptografi yang minimum diberi kepada pengguna iaitu hanya kunci kriptografi mereka disimpan secara

selamat dalam kad-kad pintar. Reka bentuk skema pengenkriptan ini dibuat menggunakan sistem sipher yang terbukti kuatnya dan menggunakan kunci sepanjang 128 bit. Pada masa ini, kunci sepanjang ini tidak mungkin dapat di cari penyelesaiannya walaupun menggunakan kaedah pencarian kunci secara menyeluruh (exhaustive). Pelaksanaan skema ini dalam sistem pangkalan data hubungan Oracle telah di buat dengan berjaya dan ia dapat melengkapkan lagi sistem keselamatan pengenkriptan Oracle yang tersedia ada.