Quality of Protection Modeling Language: Models

DB SIMULTANEOUS CLIENTS

December 14, 2014

Contents

QoP-ML Model: DB Simultaneous Clients

1.1 General Information

Model Name:	DB Simultaneous Clients
Authors:	Damian Rusinek, Bogdan Ksiezopolski
Authors' E-mail Addresses:	damian.rusinek@gmail.com bogdan.ksiezopolski@acm.org
Requires:	AQoPA 0.8.2
Analysed In:	
Date:	

1.2 Model Description

Model analyses different configurations and scenarios of protocol retrieving and searching informations in encrypted database. Model examines the server load, depending on the number of concurrent client connections.

One can imagine that database stores the details of company customers while employees use devices (e.g. smartphones) with thin clients to obtain information about particular customers.

The whole database is encrypted in order to protect it against data theft and leakage. However, server must have access to the plaintext when executes searching operations. We assume that server can temporary (for the time of one searching operation) obtain encryption key from Secure Keys Storage to decrypt the data and select subset of records.

The decryption of whole database may take a long time therefore we assume that database is indexed and divided into small parts of data (e.g. customers are divided based on the first letter of the last name). However, on the other hand database cannot be too much detail indexed, because an attacker may distinguish records according to the indexing informations (e.g. there may be only one customer on the particular street).

In the analysis process we prepare different scenarios for searching and retrieving data from the private database. The differences in scenarios come from different configurations of security mechanisms and assuring different sets of security attributes. Each scenario is tested for 100 simultaneous clients.