Compromising Privacy in Precise Query Protocols

Jonathan L. Dautrich Jr. and Chinya V. Ravishankar

Abhishek Srivastava
Student ID: 861307778

March 7, 2017
CS 236, Winter 2017

The problem:
The paper presents a privacy attack on the range queries encrypted using *Precise Query Protocols*(PQPs) which is mostly used in database as a service model. Author claims that if a partial order of encrypted tuples is identified it can be used to break the privacy of stored data on the servers without decrypting the data.

The contribution:
The authors proposed a novel algorithm to attack the privacy by identifying the partial order in query results of range queries encrypted using PQPs. The algorithm tries to identify encrypted records permissible position using PQ trees and results of queries on the range attributes. Which can then further used to infer the values of encrypted data. In this paper the hosting server is considered as main attacker and it uses the encrypted results of the query at its side so that client can be unaware of the attacks.

The method:
The Authors first presents the weakness of different kind of PQPs such as *Order preserving Encryption Scheme*, *Prefix-preserving Encryption*, *Encrypted B+ trees* etc. supported at servers end.

Author presented attack observes served range query results sets and identifies consistent etuple orderings among them. These ordering are called *Permissible permutations* and are stored in PQ-tree. Given an observed cluster its permutation can be a potentially correct ordering. As we observed more query results we can identify more clusters which can then used to exclude certain permutations which therefore refines partial ordering.

PQ-tree are designed to maintain permutations and is used in this paper to maintain the set of permissible permutations which is derived from the cluster set. PQ-tree starts by forming a universal tree which consists of possible permutations. Using a cluster from a query result we transform existing tree into new PQ-tree through reduction operation. After reducing PQ-tree with enough distinct cluster such that all leaves are children of a single Q-node.

Given a PQ-tree permissible loci can be identified of every tuple. By using tuple descendants, its type and its spread of its children we can identify etuple descendant of its children and using this in a recursive manner we can identify permissible loci of all the nodes.

Comments:
The paper presents a novel algorithm to compromise the privacy by identifying permissible loci of tuples. Authors did evaluation on how quickly can privacy of PQPs are compromised on different dataset using their algorithm.

However, there are some drawbacks of proposed algorithm:

- It does not work against few other kind of encryption techniques such as *MRQED*, *RASP*,*Hidden Vector Encryption* etc.
- It also only for 1-D data which is very impractical and this method can be extended to multi-dimensional queries as well.