A survey of Oblivious RAM

Minying Meng
10/27/2016
Outline

- Background
- Motivation
- Existing works
- My thoughts
- Reference
Cloud Computing
Cloud Computing

According to Gartner, Inc.

- Rapid development
- 17.2% increased
- $178 billion to $208.6 billion
Cloud Computing

- Reliability
- Sharing
- Convenience
- Isolation
- Compatibility
- Low cost
- High scalability
Security Issues

- Large attack surface (hundreds of servers)
- Infrastructure bugs
- Malware
- “Big brother”
- PRISM (surveillance program)
Access Pattern Leaked

- Which?
- When?
- Same data?
- Randomly or Sequentially?
- Read or Write?
Oblivious RAM (O-RAM)

- Formulated by Oded Goldreich in 1987
- Software protection
- An adversary can obtain nontrivial information about the execution of a program and the nature of the data that it is dealing with, just by observing the pattern in which various locations of memory are accessed during its execution.
Oblivious RAM

(a) ORAM functionality
Oblivious RAM

An **ORAM emulator** is an intermediate layer that protects any client (i.e., program).

ORAM will issue operations that deviate from actual client requests.

**Correctness:** If server is honest then input/output behavior is same for client.

**Security:** Server cannot distinguish between two clients with same running time.
Oblivious RAM

- Access pattern: generated by a sequence \((i_1, \ldots, i_n)\) with the ORAM emulator is the random variable \((j_1, \ldots, j_T)\) sampled while running with an honest server.

- ORAM emulator is secure if:
  - Same length of sequences
  - Access patterns are indistinguishable
My thoughts

- Simplify analysis
  - Sequential composition
  - Parallel composition
- Compare existing works
  - Performance
  - Security
Reference


Thank you!

Questions?