Encrypted Keyword Search Using Path ORAM on MirageOS

Rupert Horlick – rh572@cam.ac.uk

January 26, 2016

Threat Model

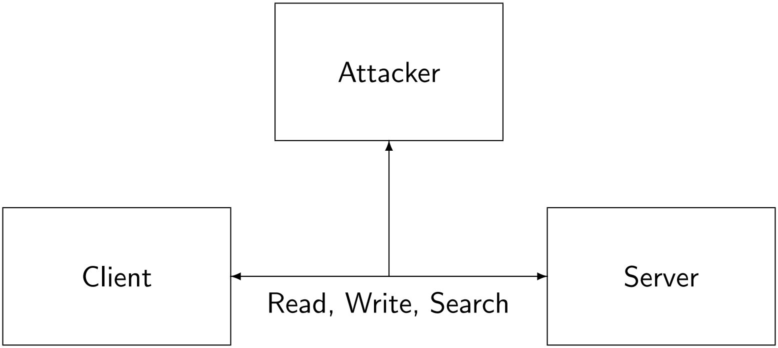

Figure: The Threat Model: The Attacker and Server are honest, but curious

System Architecture

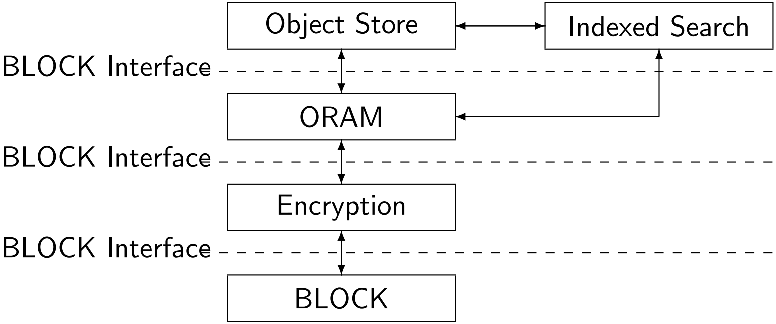

Figure: The Application Stack: We can use any underlying BLOCK implementation and we can add/remove ORAM, Encryption or Search modules as we please

Work Completed

ORAM as a functor with recursion and statelessness

File System based on inodes, with B-Trees for the index

Search using an inverted index and related search operations

Encryption by integrating an existing library

Write Up of preparation and implementation sections

Functional Testing using unit tests and randomised testing

Next Steps

Performance Testing using micro- and macro-benchmarks

Security Testing using statistical analysis

Write Up of evaluation section and conclusions

Redrafting based on feedback of supervisors

Extensions including optimisations and integrity verification