Project Progress Report

Name:	**Rupert Horlick (rh572@cam.ac.uk)**
Project Title:	**Encrypted Keyword Search Using Path ORAM on MirageOS**
Supervisors:	Dr. N. Sultana & Dr. R. M. Mortier
Director of Studies:	Dr. B. Roman
Overseers:	Dr. M. G. Kuhn & Prof. P. M. Sewell

Work Completed

Up to this point, all parts of the implementation have been completed, to a degree that they can usefully form part of the evaluation. Path ORAM has been implemented, including recursion and statelessness. An analysis of the effect of block size on the performance was carried out and an optimal block size was selected (this will be included in the evaluation). A file system was built on top of ORAM, which includes an implementation of B-Trees to form the basis for an inode index. An indexing and search module was then built on top of this, which constructs and updates an inverted index, and allows simple keyword search, including phrase search. During implementation, areas that could be revisited for optimisation or extension were noted and these will form an extension of the project.

The dissertation chapters Preparation and Implementation have been written, with only a few small subsections left to work on before a full first draft of these sections can be submitted to the supervisors for review.

Evaluation is now underway, with the evaluation strategy thoroughly devised. The first part of evaluation consisting of functional testing, through unit tests and randomised testing, is nearing completion. The next steps following this are evaluations of performance and security, followed by the write up of the evaluation process and the conclusion.

At this point, a full draft in its entirety would be submitted to the supervisors.

Depending on the timing of this submission, work would begin on extensions to the project, with a focus on the aforementioned optimisations and possible implementation of an integrity verification scheme.

Comparison with Work Plan

This is all in accordance with the work plan from the project proposal, although there has been a minor reshuffling of work. The encryption module of the project turned out to require less work than expected, so was moved forward to be performed before the evaluation. This then allows the evaluation, which will take slightly more time than anticipated, to extend into the freed time. Hopefully some of this time will still be left over and the project will completed ahead of schedule. Based on the speed of writing so far, the write up of the evaluation will also take less time than allocated in the proposal, so there will be more time to redraft and implement extensions to the project.