Storage Encryption for the Cloud

We are trying to make the Cloud a safer and saner place to live. To do so, we have writing a full operating system in OCaml, dubbed "MirageOS" [3] which compiles complex applications to single, sealed, hyper-specialized and self-contained virtual machines (or "unikernels") that can be easily deployed on any Public Cloud. These unikernels are safer than usual Virtual Machines based on standard application stacks (such as LAMP: Linux+Apache+Mysql+PHP), as they are written in a high-level language with strong static typing guarantees, with lots of whole-program analysis and optimizations done at compile-time – and they are as efficient as their counterparts as the small penalty of using a high-level language is balanced by the removal of all the legacy layers embedded in more standard operating systems.

An other important part of Cloud applications is the storage layer. For such applications, user's data needs to move back and forth from the user's edge devices to untrusted computing nodes located in datacenters. This causes *(i)* bandwidth and *(ii)* privacy issues: we already started to address *(i)* by designing "Irmin" [2], a database library to control precisely the synchronization of data between distributed nodes, using the same design principles as distributed version controlled systems such as Git.

The goal of this internship is to focus on *(ii)*, the privacy issues. Recent related work [1] on convergent encryption for Cloud storage will be the starting point of the work, but the candidate is expected to actively propose, evaluate and implement other approaches as well. Part of this work is related to the "User Centric Networking" project. [1]

Profile

The successful candidate will have a background in Computer Science, with a strong interest in Functional Programming and/or Operating Systems and Security. A working knowledge of OCaml and a taste for writing software would certainly be a plus.

Duration and Location

The duration of the internship will be of a minimum of five months, starting date negotiable. The internship will take place at OCaml Labs, in the Computer Laboratory of the University of Cambridge, UK. For any question, please contact `thomas.gazagnaire@cl.cam.ca.uk`.

References

[1] Jonathan Anderson. Privacy engineering for social networks, Chapter 4, 2012.

[2] B. Farinier, T. Gazagnaire, and A. Madhavapeddy. Mergeable data-structures. In *JFLA*, 2015.

[3] A. Madhavapeddy, M. Mortier, C. Rotsos, D. Scott, B. Singh, T. Gazagnaire, S. Smith, S. Hand, and J. Crowcroft. Unikernels: library operating systems for the cloud. In *ASPLOS*, 2013.

[1] http://usercentricnetworking.eu/