Background
Multipath TCP extends TCP in order to enable support for concurrent use of multiple paths between peers in a TCP/IP session. While it has been designed to be backwards compatible with the currently deployed TCP versions, the ecosystem of middleboxes deployed throughout network infrastructures is a major barrier to its adoption. Therefore, there is a need to further analyze the behavior of multipath TCP in the presence of TLS accelerator clusters and propose a solution to enable multipath TCP flows with TLS accelerator clusters and speed up TLS-protected communication.

Objectives
SICS Security Lab has a background in developing security mechanisms to strengthen the security of communication protocols and cloud infrastructure. Earlier efforts included analyzing the behavior of multipath TCP (MPCTCP) with TLS accelerator clusters, which are often used in enterprise networks and cloud infrastructure in order to terminate TLS connections.

Several important issues have been identified, such as the incompatibility of multipath TCP in the presence of TLS accelerator clusters, load-balancing MPTCP connections, handling failures of serving accelerators, etc. Furthermore, a set of high-level solutions has been identified.

The thesis consists of the following items:
1. Prepare a background study of TLS support in MPTCP;
2. Review the already identified limitations and identify further limitations of TLS support in MPTCP.
3. Based on the work done so far, design a solution to enable MPTCP over TLS accelerator clusters.
4. Analyze how the identified solution behaves under the defined adversarial model.
5. Implement a practical solution that enables MPTCP over TLS accelerator clusters, addresses load-balancing aspects and spurious failures of TLS accelerators.
6. Perform a vulnerability analysis of the approach based on the defined threat model and compare it with the current state of the art.
7. Evaluate the performance of the approach.
8. Provide a written report on the findings.

Competence
We are looking for one bright MSc student in Kista (Stockholm) who meet the following requirements:
1. Development skills in C (advanced knowledge is a plus) and comfortable use of Git, SVN.
2. Some knowledge of the TCP stack.
3. Knowledge in operating system architectures and network communication.
4. Good spoken and written English

A successful candidate will have the opportunity to contribute to a research paper and an important open-source project.

Applications
Applications should include a brief personal letter, your CV with your education, professional experience and specific skills and recent grades. In your application, make sure to provide examples of previous programming or other projects that you consider relevant for this position. Candidates are encouraged to send in their application as soon as possible, in paper form or via e-mail. Suitable applicants will be interviewed as applications are received.

About SICS
SICS Swedish ICT is a leading research institute for applied information and communication technology in Sweden. We are a non-profit-distributing organization with main offices in Kista outside Stockholm and smaller offices in Uppsala and Lund. SICS employs approx. 140 researchers, including 45 PhDs, and hosts another 30 researchers from KTH, consultants and students working on their Master Thesis.

Contact:
Nicolae Paladi (nicolae@sics.se)

https://www.sics.se/groups/security-lab-sec