Announcement: Student job (HiWi) in cooperation with Fraunhofer AISEC, Garching

Extension of Searchable Encryption Tool

Motivation
Searchable Encryption (SE) is a relatively new topic in cryptography. SE protocols allow a client to search over encrypted data on a server without revealing to the server the query nor the result of the query. Though, during search some information is leaked to the server. The application of SE protocols to real-life applications requires to find a compromise between security and performance of the searches.

Job Description
We currently have an opening for a research assistant position. The position includes familiarization with Apache Lucene and Searchable Encryption (SE). The task involves the development and testing of a prototype based on Lucene that incorporates SE techniques. The monthly working time is 40 hours, but can be increased on request. Tasks include:

- Analyzing Lucene’s index structure
- Research on SE index structures and their applicability to Lucene’s index structure
- Development of features in a SE prototype

Existing in-depth knowledge of the topic is not required. Generation of own ideas is desired and creative work is encouraged. If desired and applicable a follow-up thesis topic can be provided.

Requirements

- Programming skills in Java
- Interest in Search Engines, Searchable Encryption, Cryptography
- Ability to work self-directed and systematically

Contact
Fraunhofer Institute for Applied and Integrated Security (AISEC)
Mark Gall
Email: mark.gall@aisec.fraunhofer.de
Phone: +49 89 322-9986-124

Published: 6. Oktober 2017