UNIVERSITÄT ZU LÜBECK

ETH zürich

Bachelor's/Master's Thesis Announcement

Privacy-Preserving Trustworthy Insurance Questionnaire Evaluation

Supervisors: Dr. Kari Kostiainen, ETH Zürich
Prof. Thomas Eisenbarth, Universität zu Lübeck
Prof. Esfandiar Mohammadi, Universität zu Lübeck

A typical cyber insurance product provides coverage against monetary loss caused by cyber attacks or IT failures. Many companies have an increasing need for such protection, and thus this insurance line of business is growing rapidly.

Compared to many other traditional areas of insurance, insurers still face challenges with respect to the cyber peril. The level of understanding of cyber risk, i.e. how to thoroughly assess risk, describe the risk, model the risk, is not on the same level as for a number of other risks. One major obstacle insurers are confronted with is the lack of trustworthy and structured data to describe cyber exposures and cyber losses.

Insurers address this problem today by collecting data from the insureds using detailed questionnaires that the customer needs to fill in. Such questionnaires typically include questions regarding security management and security practices of the company, for instance around the software patching process, remote access, backup and recovery practices. However, many customers are unwilling to reveal full details of their IT systems and security management. Customers are likely to be concerned that honest answers that indicate poor IT security practices could be used to discriminate against them, either at the time of cyber insurance pricing or possible claim handling.

The main goal of this thesis is to enable a trustworthy evaluation of the questionnaires in a protected environment (an SGX enclave) with limited computational resources. The task would be to adjust and implement privacy-preserving learning techniques to fit the insurance questionnaires. This task requires machine learning techniques that can learn small data sets and with limited resources. The expected output is an privacy-preserving approximation of a useful statistical inference (e.g., based on machine learning models, such as linear regression or a neural network).

Tasks:

1. Adjust and implement privacy-preserving for anwering questionnaires.
2. Research related work
3. Evaluate the accuracy of the statistics
4. Write down the results and hand in the implementation

Contact:

- Kari Kostiainen (kari.kostiainen@inf.ethz.ch)
- Prof. Esfandiar Mohammadi (esfandiar.mohammadi@uni-luebeck.de)