HUMBOLDT-UNIVERSITÄT ZU BERLIN

Humboldt-Universität zu Berlin | Unter den Linden 6 | 10099 Berlin

Mathematisch-Naturwissenschaftliche
Fakultät

Prüfungsamt

Prof. Dr. Lars Grunske
Lehrstuhl: Software Engineering

Datum:
11. Dezember 2019

Bearbeiter/in:

Geschäftszeichen:

Postanschrift:
Humboldt-Universität zu Berlin
Unter den Linden 6
10099 Berlin
Telefon: +49 30 2093-3150
Telefax: +49 30 2093-3067

grunske@informatik.hu-berlin.de
www.hu-berlin.de

Sitz:
Rudower Chaussee 25
Raum 4.417
12489 Berlin

Bankverbindung:
Berliner Bank
NL der Deutsche Bank PGK AG
BLZ 100 708 48
Konto 512 6206 01
BIC/SWIFT DEUTDEDB110
IBAN DE95 1007 0848 0512 6206 01

Gutachten zur Masterarbeit von Frau Laura Wartschinski mit dem Thema „Detecting Software Vulnerabilities with Deep Learning"

Sehr geehrtes Prüfungsamt,

Anbei mein englisches Gutachten für die Masterarbeit von Frau Laura Wartschinski mit dem Thema „Detecting Software Vulnerabilities with Deep Learning"

Summary
In this work, Laura Wartschinski has explored the topic of automatic detection of software vulnerabilities in python code. In particular, she has trained a Long-Short-Term-Memory (LSTM) network for this task. The main goal of the work was to develop a new technique and provide tool support.

In order to achieve these goals, Laura has collected a dataset of different code vulnerabilities from Github projects that contain Python code. This data set is a contribution by itself. Based on the large Python corpus a word2vec model was trained focusing on word embedding in a vector space. This is as far as I know also novel.

The code files used in the Python corpus where also classified into normal files and files that contain a vulnerability. As a result a machine learning algorithm could be used to classify the files based on the vectors (word2vec) of individual code tokens and their context. Specifically, Laura has used a Long-Short-Term-Memory network and has trained it based on the samples for each type of vulnerability to recognize features of vulnerable code and then applied it to detect unknown vulnerabilities in source code.

The approach is implemented in a tool called VUDENC (Vulnerability Detection with Deep Learning on a Natural Codebase) and an evaluation of the tool showed exceptionally good precision and

recall metrics for the identification of the different code-based security vulnerabilities.

In the evaluation, one outstanding feature is the systematic analysis of the parameter of VUDENC. Based on this analysis the reader could understand why the approach has worked and what the specific tunings of the machine learning algorithms are. Consequently, this work is not just a pure black-box application of a ML technique to a software engineering problem. The thesis in contrary, provides the required understanding of the application of the ML techniques to solve the vulnerability detection problem.

Evaluation

The research work is presented in a clear and professional matter, and the necessary concepts are explored completely and in a very organized manner. Laura Wartschinski explains in detail the underpinnings of the technique, and deftly explains why the ML building blocks are chosen and how they are interconnected to arrive to the final solution. The results found are positive and there is a good lookout section exploring possible future applications of the work, which shows good research forethought. The validation section of the work, especially the evaluation of the model in Section 6, shows great attention to detail both in the experimental setup as well as the results presentation. The thesis is clearly above the standard of what can be expected from a usual master thesis.

As a consequence of this analysis, I assign the following evaluation:

1.0 Very Good

HUMBOLDT-UNIVERSITÄT ZU BERLIN
Mathematisch-Naturwissenschaftliche Fakultät
Institut für Informatik
Prof. Dr. Lars Grunske
Sitz: Rudower Chaussee 25
Unter den Linden 6
10099 Berlin

Lars Grunske