Announcing the Final Examination of Mohammed Abuhamad for the degree of Doctor of Philosophy

Time & Location: June 1, 2020 at 11:00 AM in Virtual Defense https://ucf.zoom.us/j/6673083892
Title: Towards Large-Scale and Robust Code Authorship Identification with Deep Feature Learning

Successful software authorship identification has both software forensics applications and privacy implications. However, the process requires an efficient extraction of quality authorship attributes. The extraction of such attributes is very challenging due to several factors such as the variety of software formats, number of available samples, and possible obfuscation or adversarial manipulation. We focus on software authorship identification from three central perspectives: large-scale single-authored software, real-world multi-authored software, and the robustness assessment of code authorship identification methods against adversarial attacks. First, we propose DL-CAIS, a deep Learning-based approach for software authorship attribution, that facilitates large-scale, format-independent, language-oblivious, and obfuscation-resilient software authorship identification. DL-CAIS incorporates learning deep authorship attribution using a recurrent neural network and identifying programmers using ensemble random forest. We demonstrate the effectiveness of DL-CAIS under different experimental settings and scenarios for identifying programmers of both source code and software binaries. Second, we propose Multi-X, a fine-grained multi-author identification system of programmers in single code files. Multi-X incorporates code segmentation, code representation, authorship verification, code integration, and authorship identification. We evaluate Multi-X with several Github projects (Caffe, Facebook's Folly, TensorFlow, etc.) and show remarkable accuracy. We examine the performance of Multi-X against multiple dimensions and design choices, and demonstrate its effectiveness. Finally, we propose Author-SHIELD to examine the robustness of six state-of-the-art code authorship attribution approaches against adversarial examples. We define three adversarial attacks on attribution techniques---confidence reduction, a programmer imitation, and evasion attacks---and realize them in targeted and non-targeted adversarial code perturbation. Our experiments demonstrate the vulnerability of current authorship attribution methods against adversarial attacks.

Major: Computer Science

Educational Career:
Bachelor's of Computer Science, BS, 2007, Islamic University of Gaza
Master's of Artificial Intelligence, MS, 2013, The National University of Malaysia

Committee in Charge:
David Mohasien, Chair, Computer Science
Paul Gazzillo, Computer Science
Murat, Yuksel, Electrical Engineering and Computer Science
Sung, Choi, Health Management and Informatics

Approved for distribution by David Mohasien, Committee Chair, on May 18, 2020.

The public is welcome to attend.