CityU
香港城市大學
City University of Hong Kong

電腦科學系
Department of
Computer Science

COMPUTER SCIENCE COLLOQUIUM

TransRelearn: When Software Vulnerability Discovery Meets Deep Neural Network

SPEAKER **Prof Yang XIANG**

Dean
Digital Research & Innovation
Capability Platform
Swinburne University of Technology
Australia

DATE 12 November 2018 (Monday)

TIME 10:30 am - 11:30 am

VENUE CS Seminar Room, Y6405
6th Floor, Yellow Zone
Yeung Kin Man Academic Building
City University of Hong Kong
83 Tat Chee Avenue
Kowloon Tong

ABSTRACT

Software industry has been empowering people and businesses worldwide. However, security vulnerabilities in software have been, and are continuing to be one of the most significant security threats.

The increasing number of disclosed vulnerabilities has proved that the speed of manual code inspection failed to keep up the pace of software being released. Therefore, machine learning (ML) techniques have been applied to speed up the detection of vulnerabilities. But, the potential of ML techniques is often severely compromised at the early stage of a software project, when we face a shortage of high-quality training data and have to rely on overly generic hand-crafted features. In this talk, we introduce a project: *Trans*fer *Re*presentation *Learn*ing for Vulnerable Function Discovery – *TransRelearn*, aiming to tackle this problem. Similar to the approaches by other world leading researchers, we apply a deep neural network for automated the extraction of rich features that represents both code semantics and syntactic information, at the same time guaranteeing that the features can be generalized across similar projects. The novelty of this project is that this enables us to utilize other software projects to learn useful knowledge which can be applied to the projects that have insufficient label vulnerability data. In other words, this knowledge relevant to vulnerabilities can be transferred from other software projects which have enough vulnerability data to remedy the shortage of the usable vulnerability data of a target project, while maintaining an optimal balance between feature richness and generalisability. The benefit is that the transferred knowledge helps to generate effective feature representations to enable early vulnerability detection even with a small set of training labels.

We found that many open source software projects hosted on Github repository have very limited vulnerability records (less than 100) on Common Vulnerabilities and Exposures (CVE) vulnerability database. Therefore, it is difficult to apply conventional ML techniques to train a statistically robust model for vulnerability detection on these software projects. Our method can solve this problem with comfortable effort. Our approach is one of the practical solutions that contributes to the active defense in cybersecurity.

BIOGRAPHY

Prof Yang Xiang received his PhD in Computer Science from Deakin University, Australia. He is currently the Dean of the Digital Research & Innovation Capability Platform, Swinburne University of Technology, Australia. His research interests include cyber security, which covers network and system security, data analytics, distributed systems, and networking. In the past 20 years, he has been leading the team developing active defense systems against large-scale distributed network attacks. His translational research has made significant impact to the real-world applications, such as AI-driven cyber security applications, malware applications, cloud and IoT security applications, and blockchain applications. His research was funded by the Australian Research Council (ARC) and industry partners. He has published more than 200 research papers in many international journals and conferences, such as IEEE Transactions on Computers, IEEE Transactions on Parallel and Distributed Systems, IEEE Transactions on Information Security and Forensics, and IEEE Transactions on Dependable and Secure Computing. He is the foundation Editor-in-Chief of the SpringerBriefs on Cyber Security Systems and Networks. He is the co-founder and the steering committee chair of the NSS, ICA3PP, CSS, SocialSec conference series. He served as the Associate Editor of IEEE Transactions on Computers, IEEE Transactions on Parallel and Distributed Systems, and the Editor of Journal of Network and Computer Applications. He is a Senior Member of the IEEE.

All are welcome!

In case of questions, please contact Dr Cong Wang at Tel: 3442 2010, E-mail: congwang@cityu.edu.hk, or visit the CS Departmental Seminar Web at http://www.cs.cityu.edu.hk/.