NSF Campus Cyberinfrastructure PI and Cybersecurity Innovation for Cyberinfrastructure PI Workshop

September 23 – 25, 2019 | Minneapolis, MN

NSF Program (either CC or CICI):

Program Area: CICI

Award Number: OAC-1940855

PI: **Yanfang Ye**

co-PIs: Xin Li, Brian Woerner

Project Title: CICI: SSC: SciTrust: Enhancing Security for Modern Software Programming Cyberinfrastructure

PI: Yanfang (Fanny) Ye
Associate Professor
Department of CDS
Case Western Reserve University
yanfang.ye@case.edu

Co-PI: Xin Li
Professor
Department of CSEE
West Virginia University
xin.li@mail.wvu.edu

Co-PI: Brian Woerner
Professor & Department Chair
Department of CSEE
West Virginia University
brian.woerner@mail.wvu.edu

NSF Campus Cyberinfrastructure PI and
Cybersecurity Innovation for Cyberinfrastructure PI Workshop
September 23 – 25, 2019 | Minneapolis, MN

Quad Chart for: CICI: SSC: SciTrust: Enhancing Security for Modern Software Programming Cyberinfrastructure

Challenge:

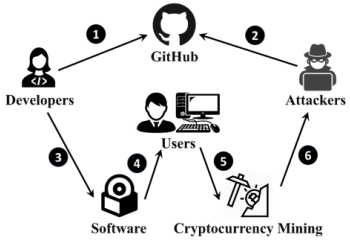
- Modern software programming CI, consisting of online discussion platforms (e.g., Stack Overflow) and social coding repositories (e.g., Github), has offered an open-source and collaborative environment for distributed scientific communities to expedite the process of software development.
- Despite the apparent benefits of this new social coding paradigm, its potential security-related risks have been largely overlooked - insecure or malicious codes can be easily embedded and distributed, which severely damage the scientific credibility of CI.

Solution:

Develop innovative techniques to detect insure or malicious codes on social coding platforms:

- Automatic detection of insecure code snippets on Stack Overflow.
- Automatic detection of malicious codes on GitHub.
- Development of user-friendly tools for scientific and engineering communities to enhance code security in modern software programming CI.

Can one trust the codes in social coding platforms?



Our goal is to advance capabilities of AI to enhance the security of modern software programming CI.

Broader Impact:

- Benefit the society at large by promoting the efficiency of cyber-enabled software development without sacrificing the security.
- Robust outreach efforts to K-12, general public, undergraduate, graduate, minority, and women in cybersecurity.
- The establishment of a cybersecurity lab through this project will enhance the cybersecurity training that will help build the national workforce in cybersecurity.

Metadata tag:

- **Yanfang Ye**, "CyberAI: Innovation, Research, Education for a Better world", ***IJCAI Early Career Spotlights***, 2019.
- Yujie Fan*, Yiming Zhang*, Shifu Hou*, Lingwei Chen*, **Yanfang Ye**, Chuan Shi, Liang Zhao, Shouhuai Xu. "iDev: Enhancing Social Coding Security by Cross-platform User Identification Between GitHub and Stack Overflow", *IJCAI*, 2019. (17.9% acceptance rate)
- Deqiang Li, Qianmu Li, **Yanfang Ye**, Shouhuai Xu. "Enhancing Robustness of Deep Neural Networks Against Adversarial Malware Samples: Principles, Framework, and Application to AICS'2019 Challenge". The AAAI-19 Workshop on Artificial Intelligence for Cyber Security (AICS), 2019. ***AICS 2019 Challenge Problem Winner***.
- **Yanfang Ye**, Shifu Hou*, Lingwei Chen*, **Xin Li**, Liang Zhao, Shouhuai Xu, Jiabin Wang, Qi Xiong. "ICSD: An Automatic System for Insecure Code Snippet Detection in Stack Overflow over Heterogeneous Information Network", *ACSAC*, 2018. (*20.1% acceptance rate*).

Contact: yanfang.ye@case.edu