Intelligent Malware Detection Utilizing Novel File Relation-Based Features and Resilient Techniques for Adversarial Attacks

Challenge:

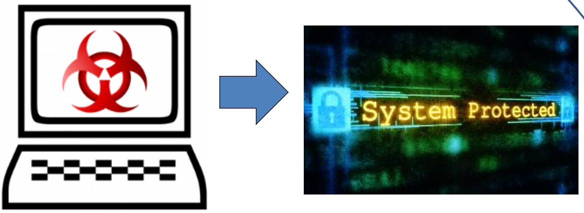
- Driven by considerable economic benefits, both the sophistication and the quantity of malware have significantly increased.
- Can we develop much more powerful methods which are capable of protecting the users against new threats, and are more difficult to evade?

Solution:

Create a resilient platform against adversarial malware attacks:

- Design newly novel relation-based features for malware representations;
- Develop a semi-supervised learning framework for malware detection;
- Develop resilient techniques against adversarial attacks on machine learning or data mining based models.

How secure is your computer?



Our goal is to design and develop intelligent and resilient solutions against malware attacks.

http://www.csee.wvu.edu/~yaye/

Scientific Impact:

- Provide an effective way to identify different threats to trustworthiness caused by malware;
- Create a resilient platform at both feature and model levels against adversarial malware attacks;
- The developed techniques are designed to be arms race capable so that they can also be used in other security domains.

Broader Impact:

- Benefit the society at large by making cyberspace more secure and resilient to cyber-attacks.
- Robust outreach efforts to K-12, general public, undergraduate, graduate, minority, and women in cyber security.

Award #: CNS-1618629, **PI: Yanfang Ye** (WVU), Co-PI: Katerina Goseva-Popstojanova (WVU), Contact: yanfang.ye@mail.wvu.edu