P.U.R.E. Research Plan Form

Mentee Information
Name: Xinmin Lin  Date: 2/9/2017
NetID: xlin32  Email: xlin32@illinois.edu  Year (F, S, J, Sr): S  Major: CompE

Mentor Information
Name: Wei Yang  Date: 2/9/2017
NetID: weiyang3  Email: doudang@uiuc.edu  Department: Computer Science
Faculty Advisor: Carl Gunter & Tao Xie

Spring 2017 Research Plan

1) Write a brief outline of your research plan:
   I plan to do the project "adversarial machine learning for malware detection". In the first few weeks I will learn to use some basics of tensorflow and read some literatures of adversarial machine learning. Then I will continue to study to use these techniques to test my ideas of what features might affect the malware classifier's misclassification rate to climb.

2) What do you hope to learn and achieve by the end of the semester?
   I wish I can learn the basics of machine learning and get more insights into the field of deep learning and security.