Fall 2016 Research Plan

1.) Write a brief outline of your research plan:

My research will focus on the relationship between machine learning and data security. In particular, the research will study how machine learning algorithms themselves are vulnerable to inadvertently revealing information in the data sets analyzed through deriving the data sets analyzed from the results of a machine learning algorithm. This research will also focus on investigating methods to prevent such an attack.

2.) What do you hope to learn and achieve by the end of the semester?

By the end of the semester, I hope to gain a deeper knowledge of the potential risks resulting from widespread use of machine learning, as well as ways to potentially mitigate or prevent the damage from such a data breach.