CS 6604 Hot Topics in Security and AI

Spring 2020

1 Course description

Advances in deep learning are significantly outperforming traditional ML systems in a variety of predictive and modeling tasks. As AI tools become commoditized, it is important to understand how this impacts the cybersecurity landscape. This course will cover advanced topics at the intersection of deep learning and security. This course is designed for students who are interested in learning data-driven security topics that are primarily based on methods from machine learning.

We will cover the following topics:

- **Deep learning for better security:** Understand how advances in deep neural networks including RNNs, CNNs, and GANs can be used to detect fraud and abuse online.
- **Threats against deep learning systems:** Understand vulnerabilities of deep learning systems (e.g., face recognition systems), and improve robustness of such systems.
- **Misuse of deep learning systems for attacks:** Understand new attacks enabled by deep learning tools, and defenses against such attacks. This includes deep learning powered techniques to break CAPTCHAs, generate fake reviews/news, control voice assistants, extract private information from collaborative learning systems, attack anonymity systems, and automate DoS attacks.

2 Reference materials

Most reading material will be drawn from research papers published at venues such as IEEE S&P, Usenix Security, CCS, NDSS, IMC, WWW, ICML, and NeurIPS.

3 Prerequisites

Students are expected to have a basic understanding of deep learning, and machine learning in general. Knowledge of a scripting language such as Python or Perl would greatly aid you in your work. Students who enroll for the course are expected to be highly motivated to learn and work hard and be ready to make up for any prerequisite deficiencies they may have.

4 Grading

Final grade will be based on the following components:

- Class participation
- Paper summaries
- Paper presentation
- Research project