Machine Learning: Integrating Security Techniques in Curriculum

(Technical Report)

Front End Protection: How the GDPR Is Enforced

(STS Research Paper)

An Undergraduate Thesis Portfolio
Presented to the Faculty of the
School of Engineering and Applied Science
In Partial Fulfillment of the Requirements for the Degree
Bachelor of Science in Computer Science

by

Maclay Teefey

May 8, 2023

How can online private information be protected? Private information leaks cost businesses millions and can expose individuals to grave risks. Data security protection measures and enforced regulations are needed.

Machine Learning models have unique vulnerabilities that are not covered as part of UVA machine learning or cybersecurity classes at the University of Virginia. A new special topics course is therefore proposed. In it, students would study the security faults in machine learning models, including de-anonymization attacks, snapshot attacks, and data poisoning. Students would learn to detect and prevent such threats. The course would prepare students to manage current vulnerabilities. By improving students’ understanding of machine learning models, it would help them also thwart future attacks.

In 2018, the European Union enacted the General Data Protection Regulation (GDPR), a privacy standard for all member states, and established Data Protection Agencies (DPAs) for each member state. The agencies have issued 1500 fines totaling 2.7 billion euros. However, privacy advocacy groups and industry groups contend that too many companies do not comply with the GDPR. They seek stricter enforcement by pressuring DPAs to punish violators and by helping companies comply with the GDPR.