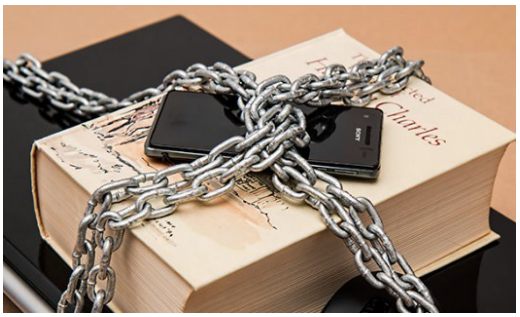

Security Lancaster | Lancaster University

Institute Seminar

Defending Deep Learning Infrastructure Against Model Stealing

Dr Peter Garraghan
Lancaster University

Date: April 1st, 2022
Time: 14:00-15:00
Teams Link: Join Seminar (We'd appreciate if you could optionally register to join our mailing list)

Abstract:
Growing demand for Deep Learning (DL) has driven the formation of specialized cloud and edge infrastructure dedicated to provision DL tools and services. Given the commercial value and competitive advantage offered by DL, there is strong incentive for organizations to protect their proprietary DL model design and trained cognitive/intellectual property against information leakage. Preventing such leakage is challenging given extraction attacks can extract, reverse engineer, and reproduce DL models from collecting a subset of test data, model architecture, and parameters. Whether such extraction attacks are exploited to identify model vulnerabilities to stage more disruptive attacks or successfully 'steal' DL models, such leakage is damaging given the significant investment and mission criticality in designing and operating DL models. In this talk we will discuss the challenges of defending against DL model extraction attacks, its threat within the context of both commercial and defense espionage, and our vision/roadmap to combat these issues towards creating secure Deep Learning infrastructure.

Please contact Jennifer for any Teams connectivity issues: j.mcculloch@lancaster.ac.uk