Project proposal

Project title	Big Data Analytics in Security
First Supervisor	Dr — Dimitris Tsaptsinos
Second Supervisor	tbc
School	Computing and Information Systems
Other member of supervisory team (no more than three KU supervisors in total)	
Specific requirements beyond 2:1 degree	

Project summary

(max 4,000 characters)

Big data analytics aid the drawing of conclusions (prediction, clustering or classification) in areas of marketing and finance amongst others. To achieve such conclusions very large databases are employed and existing, restructured and new algorithms are implemented to analyse the huge data. Datasets are increasingly "big" either in the number of observations (rows) or the number of attributes describing each observation (columns). The spectrum of algorithms techniques are employed ranging from simple analytics (standard statistical concepts, SQL) to advanced analytics (machine learning).

In the field of information security the quantity of data collected from the running networks is growing exponentially and this proposal provides an exciting groundwork opportunity for a cross- discipline collaborative project using computational foundations of machine learning interweaved with the fundamental statistical issues of data analysis.

The fundamental question to be addressed is “how do we analyse the tons of collected data and tell the existing security tools (firewalls, intrusion prevention systems, etc.) of what types of things to look for that are indicative of security threats and vulnerabilities and can we detect or predict future attacks?”