

Provenance, security & machine learning

Agenda

The British Library
96 Euston Road
NW1 2DB,
UK

The Alan Turing Institute is located on the first floor of the British Library (right hand side) and can be accessed via the main doors from 09:30 onwards. Please allow 15 minutes for queuing when planning your journey.

Monday 11 November 2019

| | |
|---------------|---|
| 09:45 – 10:20 | Registration |
| 10:20 – 10:30 | Introduction and welcome |
| 10:30 – 10:50 | Building a provenance-based IDS and the questions we ask ourselves – Thomas Pasquier (University of Bristol) |
| 10:50 - 11:10 | Tracking and analysis of causality at enterprise level – Gabriela Ciocarlie (SRI International) |
| 11:10– 11:30 | Visualization for provenance, security and machine learning – Nick Holliman (Newcastle University) |
| 11:30 – 11:50 | Refreshment break |
| 11:50 – 12:10 | Provenance, AI and proof in court – Steven McGough (Newcastle University) |
| 12:10 – 12:30 | Making Deep Neural Networks (DNNs) less susceptible to adversarial trickery – Katy Warr (Roke Manor) |
| 12:30 – 13:00 | Panel discussion |
| 13:00 – 13:45 | Lunch |
| 13:45 - 15:00 | Break out sessions phase I |
| 15:00 – 15:20 | Refreshment break |
| 15:20 - 15:45 | Break out sessions reporting and refocusing |
| 15:45 - 16:30 | Break out sessions phase II |
| 16:30 - 17:30 | Discussion, report planning and the next steps |