Research Associate – Security, Privacy and Machine Learning (MLSec, InfoSec).

THE ALAN TURING INSTITUTE

There has never been a more significant time to work in data science and AI. There is recognition of the importance of these technologies to our economic and social future: the so-called fourth industrial revolution. The technical challenge of keeping our data secure and private has grown in its urgency and importance. At the same time, voices from academia, industry, and government are coming together to debate how these technologies should be governed and managed.

The Alan Turing Institute, as the UK's national institute for data science and artificial intelligence, plays an important part in driving forward advances in these technologies in order to change the world for the better.

The Institute is named in honour of Alan Turing, whose pioneering work in theoretical and applied mathematics, engineering and computing is considered to have laid the foundations for modern-day data science and artificial intelligence. The Institute's goals are to undertake world-class research, apply its research to real-world problems, driving economic impact and societal good, lead the training of a new generation of scientists, and shape the public conversation around data and algorithms.

After launching in 2015 with government funding from EPSRC and five founding universities, the Institute has grown an extensive network of university partners from across the UK and launched a number of major partnerships with industry, public and third sector. Today it is home to more than 500 researchers, a rapidly growing team of in house research software engineers and data scientists and a business team.

BACKGROUND

The Defence & Security programme at the Turing is looking to expand a newly formed team of researchers working on real-world security and privacy challenges at the intersection of machine-learning and cyber security.

As a team, we aim to advance the state-of-the-art and publish cutting-edge research across both domains. Day to day, we collaborate with technical and subject matter experts from our partner organisations as well as academics, software engineers, and data scientists from across the Turing's research community. We present our work to a range of audiences including research colleagues, senior decision makers and non-technical stakeholders. For our models we use national clusters and cloud computing platforms to realise science and artificial intelligence research at scale.

We are a cross-disciplinary team and encourage applications from both generalists and specialists including those who self-identify as software engineers, computer scientists, machine learning practitioners, mathematicians, statisticians or more widely as data scientists or data engineers. Applicants focussed predominantly on either machine learning or systems/information security are most welcome.

The team practices an agile, experiment-driven approach and values a positive, supportive and collaborative environment in which 'radical candour' and 'lifelong learning' are encouraged. We embrace failure as a learning opportunity and necessary precursor to success. We are empowered to take ownership of our work and operate with a high level of autonomy in our roles, to deliver measurable impact to our partners.

ROLE PURPOSE

This role will sit within the new AI for Cyber Defence (AICD) Research Centre. The AICD is aiming to become a world-class research centre, at the Alan Turing Institute, focussed on delivering the science needed for developing autonomous and resilient cyber defence using reinforcement learning (RL) and other autonomous approaches to learning from interaction. This involves both the application of existing AI algorithms and techniques as well as fundamentally advancing AI where necessary.

The technical scope of this role includes:

- Identifying and advancing open security and privacy problems that might be solved with modern AI techniques. The areas we are working on include (but are not limited to):
    - Fully autonomous cyber operations and network defence.
    - Active attacks on anonymity networks.

  - Validating cryptographic ciphers, protocols and their implementations.
  - Systems security attacks and defences. Strengthening defences by discovering new adversarial techniques and models (e.g., vulnerability discovery, automated red teaming).
  - Adaptive fuzzing e.g., of web protocols, binary executables and hardware implementations.
- The application of modern AI techniques including (but not limited to):
  - Transformers and attention techniques for both episodic process memory and reduced action and observation spaces.
  - Multi-agent approaches such as swarms of specialised agents
  - Curiosity and related techniques for internally-generated reward signals.
  - Meta-learning and generalisability to novel environments.
  - Genetic techniques e.g., for improving RL algorithm performance and generalisability.
  - Adversarial approaches to RL policies as well as other AI systems.
  - Explainable RL (e.g., Bayesian networks).
- Relevant foundational research on AI including making improvements to existing techniques and proposing alternatives that advance the state of the art.
- Writing papers for submission to high quality peer review venues (e.g., USENIX, ACM CCS, AAAI, ICML, NeurIPS, IEEE S&P).

DUTIES AND AREAS OF RESPONSIBILITY

The research associate will work closely with the Centre Leads based at the Turing Institute to:

- Pursue collaborative research of high quality, consistent with making a full active research contribution in line with the research strategy outlined by the Centre Leads.
- Write or contribute to publications or disseminate research findings using other appropriate media.
- Attend and present research findings and papers at academic and professional conferences, and to contribute to the external visibility of the Institute.
- Ensure compliance with secure handling of data and health and safety in all aspects of work.
- Participate in and develop internal and external partnerships, for example to identify sources of funding, generate income, obtain projects, or build relationships for future activities.
- Contribute to the running of workshops to showcase early-stage research in the area.
- Participate in international research challenges and competitions.
- Contribute to the running of interactive events such as data study groups and capture the flag competitions.
- Establish regular ways to convene researchers such as with a seminar series, special interest and/or reading group(s).

Please note that job descriptions cannot be exhaustive, and the postholder may be required to undertake other duties, which are broadly in line with the above key responsibilities. This job description is written at a specific time and is subject to changes as the demands of the Institute and the role develop.

The Alan Turing Institute

PERSON SPECIFICATION		
Skills and Requirements Post holders will be expected to demonstrate the following:	**Essential (E)** **Desirable (D)**	**Tested at application (a)** **Tested at interview (i)**
Education/Qualification		
PhD or an equivalent qualification/experience in cyber security, machine learning or a closely related discipline.	**E**	**A**
Eligible for UK/NATO security clearance, e.g., by nationality or 5+ years NATO residency	**E**	**A**
Knowledge and Experience		
General machine learning knowledge.	**E**	**A/I**
Familiarity with reinforcement learning or related control techniques.	**D**	**A/I**
The ability to initiate, develop and deliver high quality research aligned with the research strategy indicated by the Centre Leads and any industrial stakeholders and to publish in peer reviewed conferences and journals.	**E**	**A/I**
Experience of working in a team and interacting professionally within a team of researchers and students.	**E**	**I**
Able to collaborate with experts across domains and teams	**E**	**A/I**
Ability to organise working time, take the initiative, and carry out research independently (e.g., planning, execution, work to meet deadlines), under the guidance of the PI.	**E**	**A/I**
Publication record in peer reviewed international conferences or journals.	**D**	**A/I**
Experience in frameworks such as NumPy, Tensorflow, PyTorch, Ray/RLLib, Stable Baselines.	**D**	**A/I**
Prior experience developing software in a scientific computing context, ideally in Python.	**D**	**A/I**
Experience in development suites, systems and versioning products (e.g., Git, IDEs, Linux).	**D**	**A/I**
Communication		
Excellent communication skills with the ability to adapt to different audiences, as appropriate	**E**	**I**
Ability to present research papers in academic and industrial venues	**E**	**I**
Project Delivery		
Proactive approach to managing stakeholders and their requirements and identifying opportunities for collaboration.	**E**	**A/I**
Adapts services and systems to meet stakeholders' needs and identifies ways of improving standards. Learns from issues and takes action to resolve them.	**E**	**I**
Decision Making		
Ability to make independent decisions which are low risk and that mainly affect themselves or a small number of people and are guided by regulation and practice	**E**	**A**

Work with others to make collaborative decisions that may be operational or strategic and impact immediate team or work area.	**E**	**A&I**
Recommend and advise on available options for decisions that affect operational processes, taking into account any risks.	**E**	**A&I**
Initiative and Problem Solving		
Uses judgement to analyse and solve problems and take action to prevent recurrence of problems.	**E**	**I**
Consider possible solutions to identify those which offer wider benefits and obtain evidence to support thinking.	**E**	**I**
Analysis and Research		
Ability to plan and implement rigorous analysis plans.	**E**	**I**
Identify and use a range of standard sources to gather and analyse routine data and produce reports that can be interpreted by others.	**E**	**I**
Understand when additional data is required and identifies appropriate sources. Produces reports that identify key issues and findings.	**E**	**I**
Other Requirements		
Commitment to EDI principles and to the Organisation values	**E**	**I**

The Alan Turing Institute

OUR VALUES

The Alan Turing Institute is committed to equality diversity and inclusion and to eliminating discrimination. All employees are expected to embrace, follow and promote our EDI Principles and Our Values.

APPLICATION PROCEDURE

If you are interested in this opportunity, please click the apply button below. You will need to register on the applicant portal and complete the application form including your CV and covering letter. If you have questions about the role or would like to apply using a different format, please contact us on 020 3970 2148 or 0203 862 3340, or email recruitment@turing.ac.uk.

CLOSING DATE FOR APPLICATIONS: 21 February 2023 at 23:59

TERMS AND CONDITIONS

This full-time is offered on a fixed-term basis until March 2025. The annual salary is £40,850 - £46,200 plus excellent benefits, including flexible working and family friendly policies, https://www.turing.ac.uk/work-turing/why-work-turing/employee-benefits

**Candidates who have not yet been officially awarded their PhD will be appointed as Research Assistant at a salary of £38,236 per annum.*

Successful candidates will need to undergo a security check by DSTL's security team.

EQUALITY, DIVERSITY AND INCLUSION

The Alan Turing Institute is committed to creating an environment where diversity is valued and everyone is treated fairly. In accordance with the Equality Act, we welcome applications from anyone who meets the specific criteria of the post regardless of age, disability, ethnicity, gender reassignment, marital or civil partnership status, pregnancy and maternity, religion or belief, sex and sexual orientation.

We are committed to making sure our recruitment process is accessible and inclusive.
This includes making reasonable adjustments for candidates who have a disability or long-term condition. Please contact us at adjustments@turing.ac.uk to find out how we can assist you.

Please note all offers of employment are subject to obtaining and retaining the right to work in the UK and satisfactory pre-employment security screening which includes a DBS Check.

Full details on the pre-employment screening process can be requested from HR@turing.ac.uk***.***