Securing Open Source Software Forum

The Role of AI in Securing Open-Source Applications

UNIVERSITY OF CANBERRA

OpenSI Open Source Institute

Red Hat

Innovation Central
A collaboration led by cisco

Supported by:

CANBERRA CYBER HUB

acs AUSTRALIAN COMPUTER SOCIETY

Foreword

The University of Canberra has a responsibility to expose its students, staff and industry partners to new technologies and their implications for the future labour market. The collision of open source, AI and cyber security is challenging old ways of thinking and doing. As is the case for all technology advancements, there are both risks and opportunities for economies, institutions, companies and individuals.

The forum organised by Innovation Central Canberra (ICC) together a range of perspectives on the topic of open source, AI and cyber security. This included consumers and users of open-source software, developers and integrators and researchers.

Representing the University of Canberra at the forum was Professor Frank den Hartog (Cisco Research Chair in Critical Infrastructure) and Associate Professor Carlos Kuhn (Research Chair in Open-Source Technology).

Some of the most provocative debate centred on potential risks at the intersection of AI, open source and cyber; particularly when you consider that the `contributors' to open-source software might also be potential cyber attackers.

The debate shifted from risk to opportunity during the panel discussion, with the broad conclusion that secure and AI-enabled open-source software had the potential to fundamentally change industries and accelerate adoption by improving transparency, collaboration and more rapid development.

Prof Janine Deakin

Executive Dean, Faculty of Science and Technology, University of Canberra

About the The Open Source Institute (OpenSI)

Established through a collaboration between Australia Capital Territory Government and the University of Canberra. The Open Source Institute (OpenSI) aims to lead as Australia's primary non-profit supporting open-source technologies in research, development, education, and implementation. OpenSI's vision is for open-source solutions to drive significant changes, foster collaboration, and empower individuals to shape a digital landscape that's sustainable and inclusive..

OpenSI bridges research and real-world application by developing innovative solutions within areas such as:

AI and machine learning

Cybersecurity and privacy

Quantum Technology

Open source business models

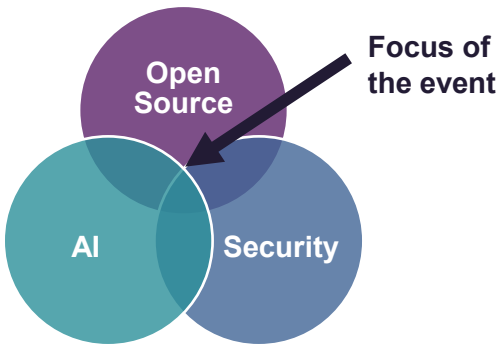
About the Event

Hosted by the University of Canberra on Ngunnawal land, the event attracted over 50 participants from industry, government, academia, and the not-for-profit sector. It was a collaboration between Innovation Central Canberra (ICC), Open Source Institute (OSI), aiming to deepen understanding of the opportunities and risks associated with Open Standards AI.

> "We have always believed in the power of open source development in driving innovation. Through collaboration, transparency and community-driven innovation, open source development models accelerate the pace of discovery, encourage experimentation and democratize access to cutting-edge tools and technologies. This leads to faster progress, greater innovation and vibrant ecosystems. AI is no different. In AI, where trust, security, and explainability are paramount, everyone — not just those with the deepest pockets or more extensive resources — should be able to participate."
>
> Matt Hicks, Red Hat CEO

By the end of this decade AI will have impacted almost every industry, organisation, process and system. It is shrinking development cycles, changing labour markets and enabling customisation at a scale never before imagined. Few users of software think about the potential impact AI is having and will have on how that code is written, including open-source software. Fewer still think about the potential cyber security implications associated with AI-enabled / developed code, including the potential threats it poses to those systems and institutions that materially impact our economy and society.

The convergence of open source, AI and cyber security is gathering momentum faster than industry can plan for it. Like in other AI domains, Australia's best chance of managing risks and capturing benefits is through targeted collaboration between industry, universities, developers and government.



"Code reviewing of open source is a form of giving back to the same community that produced the code."

- Associate Professor Carlos Kuhn (University of Canberra)

Implications for Critical Infrastructure

Open-source software powers critical infrastructure across sectors—from healthcare to telecommunications to transportation—making its security a top priority. Approximately 70% of enterprises use a mix of open source and cloud-based software to power AI initiatives, including owners and operators of critical infrastructure.

Security vulnerabilities in open-source projects can have far-reaching consequences, particularly when you consider the kinds of infrastructure that could be impacted:

- Telecommunications networks
- Water treatment facilities
- Energy transmission and distribution plants
- Ports and road infrastructure

The risks associated with AI as it applies to open-source security are not just technical. There are challenges related to training of staff, monitoring and reporting of performance and the regulation of AI-driven tools.

Major Conclusions from the Discussion

The forum was anchored by an expert panel each with their own perspective and experience. The panel was facilitated by Miranda R., Malware Security: Manager and Cyber Security Consultant with a background in Defence.

The full list of panel members:

Shane Boulden, Principal Solution Architect, RedHat

Professor Frank den Hartog, Cisco Research Chair in Critical Infrastructure

Miranda R, Malware Security: Manager and Cyber Security Consultant

Associate Professor Carlos Kuhn, Research Chair in Open Source Technology, University of Canberra

Eric Nguyen, Industry Advisor, Open Source Institute, University of Canberra

What Made Open Source Successful

There are three major factors that contributed to the `mainstreaming' of open source :

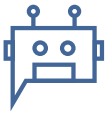
1. Critical mass; open source is routinely used in banks, government (including MyGov and critical infrastructure) and major corporates. It is now trusted as `enterprise grade'
2. Collaborative culture and community that allow issues to be navigated faster
3. Shared standards that anyone can build and run applications to / on

While none of the above is under immediate threat, the rise of generative AI code applied to open source is creating an inflection point. Layers of AI applied to software and hardware are making it difficult to guarantee trust and have potentially profound implications for data governance. Expert guidance and facilitation from industry (including players like RedHat) and communities of interest will be critical.

Major Conclusions from the Discussion

AI Does Not Solve for Security as a First Priority

Large Language Models (LLMs) are geared towards providing the consumer / user successful outcome. Experience has revealed to the panel members that LLMs will also tend to gloss over security (and prioritise functionality or performance). Security needs to be included specifically in the search prompts so AI tools will actively look for vulnerabilities in code and remediate them.



The Launch of DeepSeek Has Brought AI Security Into Mainstream Consciousness

DeepSeek, the Chinese AI company developing LLMs, launched an eponymous chatbot in January 2025 which quickly gained users and then scrutiny. Of specific concern was the potential for data ingested into the LLMs to be compromised. Some companies and government agencies immediately recognised the threat (particularly of employees uploading data into the DeepSeek LLM and making it pseudo-discoverable). The company claimed that it trained its V3 model for US$6 million compared to $100 million for OpenAI's GPT-4 in 2023, and approximately one-tenth of the computing power used for Meta's comparable model, Llama 3.1. If these economics are true, it will further democratise AI and truncate innovation cycles.

The Convergence of Open Source, AI and Security Exaggerates Old Tensions

There is a long history of technology developments forcing organisations to manage the tension between innovation and performance on one hand, and data security on the other. As innovation cycles speed up (propelled by AI) there is a risk that security is seen as an inhibitor to progress, not an enabler. But there are lots of lessons for how organisations can safely adopt open source. Specifically, there is a lot of interest in emerging concepts such as Instruct Labs, a novel methodology designed to overcome the scalability challenges in the tuning phase of large language model (LLM) training.

"Software ages like milk, not wine. It doesn't develop a nice floral bouquet as it ages, instead developing smelly CVEs. This applies to all code - open source and proprietary, and the difference is in how we manage fixes and provide vulnerability data transparently to software consumers."

- Shane Boulden, RedHat

Major Conclusions from the Discussion

Critical Infrastructure security can suffer from rush to cost reduction

The privatisation of critical infrastructure has created a paradigm where infrastructure performance has been traded off for cost. The rush to open source and AI has been driven by commercial factors (productivity savings) rather than performance improvement. This has created a gradual erosion of performance over time. Future development of open source software needs to look at AI as a performance improver, not just a cost saver. It also needs to more consciously direct AI and LLMs towards solutions that are secure by design so that vulnerabilities are actively anticipated and responded to.

The Next Wave of Convergence Will Make Open Source More Consumable

Privileging security is a pre-cursor to making available an AI consumable. Without trust from users Open Source AI will struggle to progress fast enough.

"We need to harness open-source AI innovation, and balance it with our goals for security and safety."

- Eric Nguyen, Industry Advisor, Open Source Institute, University of Canberra

The response needs to include a focus on areas such as:

1. Active code review (with a focus on vulnerabilities and protecting against rogue or degraded code)
2. Validation of developers' knowledge and understanding
3. Provenance inspections to determine if software is up to date – including looking at the inter-dependencies of different pieces of codes and will they compromise security of the code
4. The role of people as both enablers and as a potential source of risk

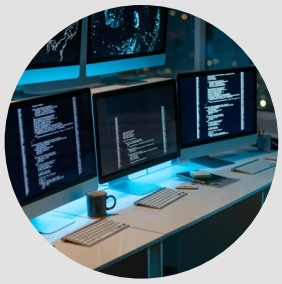
"When it comes to open-source you have to remember that sometimes the contributors to open-source code are actually the attackers and actively engaged in data poisoning,"

- Professor Frank den Hartog

Opportunities Emerging From the Discussion

De-risking Adoption by Industry

Industry adoption of AI-driven open-source software must be supported by clear, universally accepted data standards and baseline implementations. An example of this is the AI Readiness framework, an open-source project created by the Fintech Open Source Foundation (FINOS). The goal of the FINOS AI Readiness project is to develop a governance framework that manages the on-boarding, development of, and running AI-based solutions within financial services organisations - allowing us all to unlock the potential of this disruptive technology in a safe, trustworthy and compliant way.



New Research Frontiers

Strengthening academia-industry collaboration is vital for accelerating innovation. Initiatives like Canberra Cyber Hubs' upcoming event, Forging Successful Research Partnerships (June 2025), strategically support researchers and industry in building impactful, sustainable partnerships as part of the broader Partnerships of Innovation series.

Building Future Skills

Equipping the workforce with the skills necessary to navigate AI, open source, and cybersecurity convergence is essential. Industry-academia partnerships, such as those through the Cisco Networking Academy, offer opportunities to co-develop and deliver targeted training. An example is the University of Canberra's short course, "The AI Advantage: Fundamentals for Government & Business", designed to rapidly build essential AI capabilities across industry and government.

Get Involved with Our Partners

Collaborative partnerships are critical to innovation in cybersecurity and open-source technology. Connect with our partners below to explore opportunities, engage in collaborative projects, and stay at the forefront of industry developments.

OpenSI Open Source Institute

OpenSI advances the adoption and integration of open-source technologies through research, collaboration, and education, fostering trusted and secure software solutions.

Connect with Linkedin

Red Hat

Red Hat leads in enterprise open-source solutions, supporting secure digital transformation with innovative technologies and collaborative community-driven approaches.

Connect with Linkedin

Innovation Central

A collaboration led by cisco

ICC connects industry with researchers to accelerate innovation, particularly through applied technology solutions in areas like cybersecurity and AI.

Connect with Linkedin

CANBERRA CYBER HUB

Canberra Cyber Hub providing resources, networking, and knowledge exchange within Canberra's cybersecurity community,

Connect with Linkedin

acs AUSTRALIAN COMPUTER SOCIETY

ACS represents Australia's technology professionals, driving standards, innovation, and skills development in ICT to ensure a globally competitive tech workforce.

Connect with Linkedin

UNIVERSITY OF CANBERRA

The University of Canberra has a deep focus on cyber security, Defence and critical infrastructure in recognition of its location in Australia's capital and relationships with both government and industry

Connect with Linkedin