Senior Verification Researcher

Company: Kry10 UK Ltd, subsidiary of Kry10 (https://kry10.com/)
Location: UK, Remote or Hybrid
Department: Kry10 UK + Europe
Reports to: Chief Scientist / VP UK + Europe
Employment: Permanent, full time
Salary: £100k (with some flexibility for exceptional candidates) + Pension + ESOP + relocation if required within UK

About Kry10

Kry10 is a software and security company creating exceptionally resilient systems for mission-critical devices. Our work spans multiple sectors including critical national infrastructure, industrial control systems, defence, healthcare, telecommunications, automotive, and AI infrastructure. With a focused team of 35 people, we're scaling rapidly and already have global reach with offices across the UK, US, NZ, and Australia.

Technology & Innovation

At the heart of what we do is the Kry10 Operating System (KOS): a platform that delivers mathematically proven security through strong isolation and tightly controlled communication. Formal verification isn't adjacent to what we do, it's foundational to it. Our team includes some of the most experienced contributors to seL4 and its verification ecosystem, and we build on that work every day.

This role sits at the frontier of that expertise: producing machine-checked guarantees for real security applications, using AI-accelerated formal methods workflows, on properties that until now could only be assured by architecture and hardware separation.

About the Role

We are seeking a UK-based Senior Verification Researcher to lead the verification research for Kry10's part of a collaborative project on browse-down security (“verifiable ephemeral computation for cross-domain"). This project is funded under ARIA's Safeguarded AI programme and delivered by a consortium of PentenAmio, Kry10, and Galois Inc.

The project will deliver machine-checked guarantees for two components of a single-chip cross-domain security appliance. Galois leads the verification of the video codec path. **You will lead the verification of the other target: verified ephemerality of the untrusted virtual machine.** That means producing a formal, machine-checked argument that when a session ends (or on a defined reset event), the low-side VM is torn down and all its capabilities revoked, and that each new VM session is built to a known-good state, such that no information can leak

© Kry10 UK Ltd. All rights reserved.

from one session to the next. Any compromise of the untrusted side is therefore provably non-persistent.

You'll own the verification problem end to end, from formal specification of the ephemerality property, through proof development, to a defensible statement of assumptions. To be clear, you are not expected to build the solution itself: partner organisations are leading the solution architecture and much of the low-level embedded engineering, and you'll work alongside a dedicated senior software engineer at Kry10. You will work with those engineers to specify and prove properties about the architecture: to understand it deeply, model it faithfully, and deliver machine-checked arguments about its security properties. You won't have direct reports, but you won't be working alone either: you'll collaborate closely with Kry10's verification researchers in the UK and Australia, with Galois on the AI-enabled proof toolchain, and with PentenAmio as they integrate the results into deployed products for customers.

Proofs sit at the centre of this role, but the assurance case spans mechanisms as well as models. Building on the seL4 behavioural model, the specification is expected to cover correct capability revocation (including its correct invocation from the high side), correct invocation of external device resets, construction of each new VM session from an immutable, read-only source image, and cryptographic signing of the VM image and boot process, for example via a software TPM. You'll help shape the precise specification and how these elements combine into a single, coherent assurance argument.

We take a pragmatic view of what verification means here. Building a formal model of the system's behaviour and proving properties of that model is a valuable and legitimate outcome, even where the model is not fully connected to the final implementation. Tightening the connection between model and implementation throughout is part of the research agenda, not an entry requirement for the work to count.

AI-assisted verification is key in this project. You'll use and evaluate AI tooling for drafting specifications, generating invariants and proof scripts, and accelerating proof engineering, with the proof assistant as the ground-truth oracle throughout. Your findings on where AI helps (and where it doesn't) will feed directly into the programme's central research question.

Key Responsibilities

- Own the ephemerality verification target. Define the formal security specification for VM teardown and rebuild over the seL4 / KOS behavioural models, spanning capability revocation, device resets, immutable source images, and signed boot, then develop the proofs and carry them through to completion. You'll decide what the proof needs to say and how to get there.
- Make the trust story explicit. Produce a clear, rigorous account of the threat model, proof assumptions, and trusted computing base, and work to minimise

© Kry10 UK Ltd. All rights reserved.

it, building on seL4's proven revocation mechanisms and integrity theorem. The value of this work depends on the honesty and precision of its claims.
- Combine proofs with cryptographic assurance. Specify and evaluate the cryptographic elements of the target: signed VM images and boot processes (e.g., via software TPM), anchored to an immutable source image, ensuring the formal proofs and deployed cryptographic mechanisms form one mutually reinforcing assurance case.
- Work hand-in-hand with the engineers building the system. Partner with Kry10's senior software engineers and PentenAmio's embedded engineering team so that the formal model faithfully reflects the architecture, the verified design and the shipped system stay aligned, and the proof artefacts become a native, proof-carrying capability of the KOS platform. They build it; you prove things about it.
- Put AI to work on real proofs. Use AI-assisted workflows for the full proof lifecycle: specification drafting, invariant and lemma generation, and proof script development, in collaboration with Galois's toolchain work, and report on what it does or doesn't contribute to each sprint.
- Engage with the Red Team. The project runs in 8-week sprint cycles with independent adversarial review. You'll respond to Red Team findings, harden the proofs and specifications, and help select the next verification targets.
- Represent the work. Participate in regular meetings with ARIA and consortium partners, contribute to progress reports and the final published outputs, and help tell the story of what verified ephemerality makes possible.

Required Qualifications

- Substantial hands-on experience with an interactive theorem prover such as Rocq, Isabelle/HOL, or Lean, developing significant proofs and verification artefacts relating to real-world software. Our internal verification work uses Rocq and Iris, so our expectation is that this project will too. Experience with separation logic (Iris or comparable) is strongly preferred.
- Experience verifying (or formally specifying) systems-level properties: e.g., operating systems, hypervisors, memory management, or similar low-level software.
- The ability to take an informally stated security property and a real system architecture and turn them into a well-posed formal model and specification, with a precise account of assumptions, abstraction choices, and trusted computing base.
- Strong written communication skills: able to produce clear technical documentation for a mixed audience of proof engineers, systems engineers, red team members, and programme stakeholders.
- Comfortable working in a distributed, collaborative team across time zones and organisations.
- Self-directed and able to lead a research workstream through sprint-based deliverable cycles with minimal supervision.

© Kry10 UK Ltd. All rights reserved.

Preferred Qualifications – some / any of:

- PhD or equivalent research experience in formal methods, programming languages, or a related area
- Familiarity with the seL4 ecosystem, particularly its capability model, revocation mechanism, and integrity/isolation theorems (very useful, but not a prerequisite)
- Some familiarity with the seL4 ecosystem
- Familiarity with applied cryptography for platform integrity: image signing and verification, attestation, measured or secure boot, software TPMs
- Experience with AI / LLM-assisted formal methods, whether from research, tooling, or direct use
- Experience with virtualisation, VM lifecycle management, or hardware state modelling
- Contributions to open-source proof repositories or formal methods tooling

We recognise that candidates will bring different technical strengths and experiences, and selection will be based on overall suitability, aptitude, and interest rather than a single technical profile. If you're unsure about applying, please reach out to us anyway.

We welcome applications from exceptional early-career researchers, e.g. those finishing a relevant PhD; the seniority of the role can adapt to the candidate.

What We Offer

- Proofs that ship. Your verification work becomes a native part of a commercial operating system and a deployed security appliance used by critical-infrastructure customers: this work has a direct route to deployment.
- A genuinely hard, genuinely novel target. Verified ephemerality on real hardware, against capable adversaries, with a realistic assurance story.
- A team that takes formal methods seriously. You won't need to justify why this work is hard or important: our engineers and researchers have been doing seL4-based verification for more than a decade.
- World-class collaborators. Day-to-day research collaboration with Galois and PentenAmio, and engagement with ARIA's Safeguarded AI programme, including its Red Team.
- A permanent home for this work. This is a permanent role. The project is the starting point, but verified ephemerality and AI-assisted verification are strategic to Kry10 well beyond it.
- Flexible, with a home base if you want one. Remote or hybrid working within the UK, with a mild preference for candidates able to be based at or near our Gloucester office. A relocation package is available. We're a collaborative, low-bureaucracy team. Decisions get made quickly.

© Kry10 UK Ltd. All rights reserved.

- Good salary, pension, and participation in Kry10's employee share option plan.

How to Apply

- Please submit your CV and a short covering letter to recruitment@kry10.com with the subject line "UK Senior Verification Researcher - [Your Name]".
- We want to know why you're interested in this role.
  In your covering letter please tell us:
  - What draws you to this project specifically
  - Which proof tools you have the most hands-on experience with, and your exposure (if any) to Rocq and Iris
  - Your perspective on AI-assisted formal verification (even if your experience is limited)
- Please send any questions about this role or the application process to recruitment@kry10.com
- We'd like the successful candidate to start as soon as practical; we understand notice periods and academic commitments. Our process is typically a couple of calls with researchers in the UK and Sydney, and an in-depth technical conversation on-site in Gloucester.

Kry10 is an equal opportunity employer. Applicants must have the right to work in the UK. We welcome applications from candidates of all backgrounds. All qualified applicants will receive consideration for employment. This role is subject to security, export control and/or contractual restrictions: appointment will be conditional on the successful candidate being able to meet these requirements, including eligibility to work in the UK. Any security or export control requirements will be assessed fairly and in accordance with applicable law.

We welcome applications from disabled candidates and are happy to discuss reasonable adjustments at any stage of the recruitment process.

© Kry10 UK Ltd. All rights reserved.

Our Culture & Values

Founded in New Zealand, our core values guide everything we do:

Tūturu Rangatira kī Tahi (Authentic Leadership with Accountability)
We act and do what we say. We are accountable for our actions and the promises we make to others.

Raru ki uta, Raru ki tai (Know What Problem You're Solving)
We tackle the most important problems first and understand what problems our customers have.

Mata-tika (Fair and Reasonable)
We are fair and reasonable with ourselves and others in all dealings. We value diverse perspectives and foster respectful dialogue.

Rangi rāua ko Papa (Planet Enhancing)
We prioritize projects and partners that actively protect our planet and seek efficient ways to lessen negative environmental impact.

Inu wai, Kai Rona (Drink Water, Then Eat the Moon)
The Kry10 platform is a massive undertaking built through iterative excellence. Each release reflects ongoing client feedback and our commitment to ambitious goals.

Kaitiaki (Guardianship)
As guardians, we bring great care and attention to work, treating it as our own. We ensure knowledge and work are passed on to future guardians.

Mana Tahi, Mana Tini (Individual and Collective Success)
We celebrate individuality and expertise while recognizing that collective success is the only way to achieve the Kry10 mission.

Moumou te Huruhuru (Don't Waste the Feathers of the Bird)
We use resources efficiently and ensure our people have the right tools to do the job well.

© Kry10 UK Ltd. All rights reserved.