

The people behind NICTA's seL4 research breakthrough.....

It took four years of hard work and the ingenuity of a dedicated team of 12 researchers and PhD students to transform an imaginative spark into a world-first research breakthrough in computer science. Here are some of the people who made it happen...

Dr Gerwin Klein - NICTA Principal Researcher and Project Leader



Dr Klein leads NICTA's formal verification research team, L4.verified. He joined NICTA fresh out of his PhD at Technische Universitaet Muenchen. Dr Klein is the chief architect of the proof and the seL4 verification project.

"It was incredibly lucky for me to join NICTA at such an exciting time five years ago," says Dr Klein. "It is rare that you get a challenging opportunity like this and the unique impact-oriented research culture at NICTA has helped us immensely. I've always liked to solve problems that other people say are impossible. Formally verifying a whole microkernel was precisely such a challenge and NICTA enabled us to bring together an outstanding team for solving it."

Dr Kevin Elphinstone - NICTA Senior Researcher & UNSW Senior Lecturer



Dr Elphinstone is a senior lecturer at the University of New South Wales. He is an operating systems researcher who also specialises in teaching operating systems at undergraduate and postgraduate level. He has been seconded to NICTA to work within the ERTOS group leading the seL4 operating system research team.

Dr Elphinstone's contribution has been central to the success of the seL4 proof. He is the chief architect of the seL4 microkernel itself. On the outset of the project, he recognised the challenges formal verification presented to operating system designers, and developed approaches and technologies that enabled prototyping secure operating systems that are much more amenable to formal verification.

"Constructing an operating system is immensely challenging due to its enormous complexity. Developing ways to reduce that complexity, while retaining performance and real-world applicability, was a key ingredient in the success of the formal verification. Our success in verifying seL4 will enable the creation of truly trustworthy systems in the future."

Professor Gernot Heiser - NICTA's ERTOS Group leader and UNSW John Lions Professor of Operating Systems



Professor Heiser is also Founder and Chief Technology Officer of NICTA's spin-out company Open Kernel Labs (OK Labs). The company develops and markets next-generation embedded operating systems and virtualisation technology. Its embedded hypervisor technology is in hundreds of millions of consumer devices worldwide.

According to Dr Klein, Professor Heiser is the visionary who made everyone believe in the project in the first place.

"When we started this project, not many people thought we could succeed, given that many prior attempts at OS verification failed, but we thought the time was right," Prof Heiser recalls. "What got us there in the end was an outstanding team with a truly unique combination of world-class OS and verification skills, a shared vision, and a strong will to 'kick ass'!"

What the experts are saying....

INRIA

Dr. Xavier Leroy
Senior research scientist at INRIA in France

"The verification of the seL4 kernel is a major milestone in the area of formal methods. By inventing novel verification techniques of the highest scientific interest and applying them all the way to the actual source code, the NICTA team achieved unprecedented levels of assurance for a software component as complex and security-critical as an operating system kernel."

Cambridge

Lawrence C Paulson
Professor of Computational Logic
Computer Laboratory, University of Cambridge

"It is hard to reply without resorting to cliches. Proving the correctness of 7500 lines of C code in an operating system's kernel is a unique achievement, which should eventually lead to software that meets currently unimaginable standards of reliability. This work goes beyond the usual checks for the absence of certain specific errors; instead, it verifies full compliance with the system specification."

The project has yielded not only a verified microkernel but a body of techniques that can be used to develop other verified software."

Yale

Zhong Shao, Professor of Computer Science at Yale University.

"Making operating system kernels truly dependable is one of the major challenges facing today's embedded systems community. The ERTOS group has successfully verified the

functional correctness of all the C code in the seL4 microkernel. The verification is done using a highly reliable proof assistant and comes with explicit machine-checkable proof objects that can be validated by independent third-parties. This is a remarkable achievement. It makes a significant advance toward building fully verified system software with meaningful dependability guarantees.”