



Media Release
12 August, 2009

World-first research breakthrough promises safety-critical software of unprecedented reliability

The completion of the world's first formal machine-checked proof of a general-purpose operating system kernel was announced by NICTA, Australia's Information and Communications Technology (ICT) Research Centre of Excellence, today. This extraordinary milestone paves the way for a new generation of software capable of unprecedented levels of reliability.

There is now a way to mathematically prove that the software governing critical safety and security systems in aircraft and motor vehicles is free of a large class of errors – long before the plane takes off or the car's engine starts.

The Secure Embedded L4 (seL4) microkernel, designed for real-world use, has potential applications in defence and other safety and security industries where the flawless operation of complex embedded systems is of critical importance.

"It is hard to comment on this achievement without resorting to clichés," says Professor of Computational Logic at Cambridge University's Computer Laboratory, Lawrence C Paulson. "Proving the correctness of 7,500 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."

"Formal proofs for specific properties have been conducted for smaller kernels, but what we have done is a general, functional correctness proof which has never before been achieved for real-world, high-performance software of this complexity or size," explains NICTA Principal Researcher Dr Gerwin Klein, who leads NICTA's formal verification research team.

The proof also shows that many kinds of common attacks will not work on the seL4 kernel. For instance, the microkernel is impervious to buffer overflows, a common form of software attack where hackers take control of programs by injecting malicious code. "Our seL4 kernel cannot be subverted by this kind of attack," says Dr Klein.

The outcome is the result of four years' research by Dr Klein's team of 12 NICTA researchers, NICTA/UNSW PhD students and UNSW contributed staff. They have successfully verified 7,500 lines of C code and proved over 10,000 intermediate theorems in over 200,000 lines of formal proof. The proof is machine-checked using the interactive theorem-proving program Isabelle. It is one of the largest machine-checked proofs ever done.

"This is a remarkable achievement," said Yale University's Professor of Computer Science Zhong Shao, "It makes a significant advance toward building fully verified system software with meaningful dependability guarantees."

To reach this milestone, the NICTA team invented new techniques in formal machine-checked proofs, made advances in the mathematical understanding of real-world programming languages and developed new methodologies for rapid prototyping of operating system kernels.

"This work goes beyond the usual checks for the absence of certain specific errors," Professor Paulson notes. "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."

NICTA will shortly transfer its intellectual property to NICTA spin-out company Open Kernel Labs, whose embedded hypervisor software - also based on NICTA research - is in hundreds of millions of consumer devices worldwide.

“The NICTA team has achieved a landmark result which will change the game for security- and safety-critical software,” said OK Labs’ Chief Technology Officer and Leader of NICTA’s ERTOS Group, Professor Gernot Heiser. “It provides conclusive evidence that bug-free software is possible, and in the future nothing less should be considered acceptable where critical assets are at stake. OK Labs looks forward to taking this groundbreaking research to market.”

“NICTA’s completion of original ICT research of this calibre is a triumph,” said NICTA CEO Dr David Skellern. “The advances in knowledge made by the team reflect the outstanding talent of its members and the vision and tenacity of its leaders. It is also a tribute to the confidence the Australian Government has placed in us by securing NICTA’s continued funding in the recent Federal Budget.”

The scientific paper describing this research will appear in the 22nd ACM Symposium on Operating Systems Principles (SOSP) <http://www.sigops.org/sosp/sosp09/>. Further details about NICTA’s L4.verified research project can be found at <http://ertos.nicta.com.au/research/l4.verified/>.

About NICTA

National ICT Australia Ltd (NICTA), Australia’s Information and Communications Technology (ICT) Research Centre of Excellence, is developing technologies which will meet the current and future needs of the community in fields which will lead to large economic, social and environmental benefits for Australia. NICTA has five laboratories around the country. Since NICTA was founded in 2002, it has created four new companies, developed a substantial technology portfolio of patent applications and continues to supply new talent to the ICT industry through the NICTA-enhanced PhD program.

NICTA is funded by the Australian Government as represented by the Department of Broadband, Communications and the Digital Economy and the Australian Research Council through the ICT Centre of Excellence program. It was established and is supported by its members: The Australian Capital Territory Government; The Australian National University; NSW Department of State and Regional Development; and The University of New South Wales. NICTA’s partners include: the University of Sydney; University of Melbourne; the Victorian Government; the Queensland Government; Griffith University; Queensland University of Technology; and The University of Queensland.

For further information:

Dorothy Kennedy
Communications Specialist, NICTA
Ph: 02 9376 2098 or 0488 229 687