Code breakthrough delivers safer computing

September 25 2009

(PhysOrg.com) -- Computer researchers at UNSW and NICTA have achieved a breakthrough in software which will deliver significant increases in security and reliability and has the potential to be a major commercialisation success.

Professor Gernot Heiser, the John Lions Chair in Computer Science in the School of Computer Science and Engineering and a senior principal researcher with NICTA, said for the first time a team had been able to prove with mathematical rigour that an operating-system kernel - the code at the heart of any computer or microprocessor - was 100 per cent bug-free and therefore immune to crashes and failures.

The breakthrough has major implications for improving the reliability of critical systems such as medical machinery, military systems and aircraft, where failure due to a software error could have disastrous results.

“A rule of thumb is that reasonably engineered software has about 10 bugs per thousand lines of code, with really high quality software you can get that down to maybe one or three bugs per thousand lines of code,” Professor Heiser said.

“That can mean there are a lot of bugs in a system. What we’ve shown is that it’s possible to make the lowest level, the most critical, and in a way the most dangerous part of the system provably fault free.”

“I think that’s not an exaggeration to say that really opens up a

completely new world with respect to building new systems that are highly trustworthy, highly secure and safe."

Verifying the kernel - known as the seL4 microkernel - involved mathematically proving the correctness of about 7,500 lines of computer code in an project taking an average of six people more than five years.

"The NICTA team has achieved a landmark result which will be a game changer for security-and-safety-critical software," Professor Heiser said.

"The verification 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."

Provided by University of New South Wales (news : web)