Keynote Talks 1

Lions OS: Towards a Truly Dependable Operating System

Gernot Heiser

Abstract

The formal verification of the seL4 microkernel, completed almost 15 years ago, was a major step towards making a truly dependable OS a reality, but not more than a first step. While seL4 has now been deployed in a number of defence and civilian projects, and cars running an seL4-based OS will be on the road this year, the sad reality is that there are probably more failures than successes in seL4 deployment. We have to conclude that it is not sufficient to provide an open-source microkernel and hoping the community will build practical systems around it. Coming up with a good design of an seL4-based system, including re-use of legacy services, requires far too much expertise. The Trustworthy Systems Group at UNSW has therefore embarked on a project to design, implement and verify a complete seL4-based OS, Lions OS (named after the author of the Lions Book that taught Unix to generations of programmers). The name is program: we aim to make the project feasible by applying some of the core principles of Unix: simplicity and clean design. In addition we are restricting ourselves (for now, at least) to systems with a static architecture, i.e. the set of components and (the ceiling of) the communication channels connecting them are fixed at system build time. This restriction is compatible with at least the vast majority of cyber-physical, IoT and other embedded systems. Specifically, our aim is to build an OS that is (a) provably secure and reliable, (b) performing comparably to insecure mainstream systems such as Linux, and (c) adaptable to a wide range of use cases within the target domain. A core ingredient for making end-to-end verification scale to a complete OS is the Pancake language, a new systems language with a verified compiler which we will use to implement at least part of Lions OS. We have just released a first, open-source version of Lions OS. While still rudimentary, our experience so far is that a highly modular architecture, if done well, can result in a well-performing system, while keeping modules simple enough to verify them with automated techniques. Our roadmap for Lions OS includes end-to-end correctness and security proofs, formal reasoning about timeliness of mixed criticality systems, and provable elimination of information leakage through microarchitectural timing channels.

Short Biography

Gernot Heiser is Scientia (distinguished) Professor and John Lions Chair of Operating Systems at UNSW Sydney, where he leads the Trustworthy Systems research group. His research interest are in operating systems, real-time systems, security and safety. His research vision is to completely change the cybersecurity game from playing catch-up with attackers to systems that are provably secure and safe. With his team he pioneered the large-scale formal verification of systems code, specifically the design, implementation and formal verification of the seL4 microkernel; seL4 is now being used in real-world security- and safety-critical systems. Heiser's former company Open Kernel Labs, acquired by General Dynamics in 2012, marketed the OKL4 microkernel, which shipped on billions of mobile wireless chips and is deployed on the secure enclave of all iOS devices. He presently serves as Chief Scientist of Neutrality, and Chairman of the seL4 Foundation. Gernot is a Fellow of the ACM, the IEEE, Engineers Australia, the Australian Academy of Technology and Engineering (ATSE) and the Royal Society of New South Wales (RSN) and a Member of the German Academy of Sciences Leopoldina. He is also an ACM Distinguished Lecturer and an IEEE Distinguished Visitor.

Keynote Talks 2

Verifying the Results of Complex Elections

Vanessa Teague

Abstract

Elections are a special security problem because it is not good enough for systems to be secure and results correct - they must also be verifiably so. In this talk I'll discuss a setting increasingly common in the US, Australia and elsewhere: citizens vote privately on paper, then the votes are digitized and counted electronically. Risk Limiting Audits, invented by Philip Stark, provide rigorous statistical guarantees of an accurate election result in this situation, but were originally designed only for the relatively simple electoral processes used in the USA. I'll explain our techniques for auditing instant-runoff (IRV) elections and other complex social choice functions, including recent and future practical deployments in the USA. I'll conclude with important open problems, particularly for the single transferable vote (a.k.a. Australian Senate voting). Based on joint work with Michelle Blom, Andrew Conway, Alexander Ek, Philip B Stark, Peter J Stuckey and Damjan Vukcevic.

Short Biography

Teague's research focuses primarily on cryptographic methods for achieving security and privacy, particularly for issues of public interest such as election integrity and the protection of government data. She was part of the team (with Chris Culnane and Ben Rubinstein) who discovered the easy re-identification of doctors and patients in the Medicare/PBS open dataset released by the Australian Department of Health. She has co-designed numerous protocols for improved election integrity in e-voting systems, and co-discovered serious weaknesses in the cryptography of deployed e-voting systems in New South Wales, Western Australia and Switzerland. She lives and works on Wurundjeri land in Southeastern Australia (near Melbourne). In 2023 she founded Democracy Developers Ltd, an Australian not-for-profit that builds open-source software for supporting democracy.

Keynote Talks 3

Critical Technologies and Cybersecurity Research: The Next 10 Years

Surya Nepal

Abstract

Current approaches to cybersecurity are reactive. This means that we only start addressing problems when they occur. However, this approach is no longer sufficient in the context of emerging technologies, such as AI/ML, Quantum, 6G, AR/VR/XR, and Digital Twins. These technologies will significantly speed up digital transformation while also providing more opportunities for cyberattacks. Unfortunately, cyberattacks are becoming increasingly sophisticated, complex, adaptive, and non-deterministic. To defend our critical assets effectively, we need a proactive approach to cybersecurity. We must anticipate future vulnerabilities and opportunities associated with emerging technologies. This keynote talk will explore the cybersecurity research challenges and opportunities at the intersection of these emerging technologies. It will also highlight some of the relevant projects being undertaken at CSIRO's Data61.

Short Biography

Dr. Surya Nepal is a senior principal research scientist at CSIRO Data61. He has been with CSIRO since 2000 and currently leads the cybersecurity and quantum systems research group comprising 70 staff and 50 PhD students. His primary area of research focuses on the development and implementation of technologies in distributed systems, with a specific emphasis on security, privacy, and trust. Dr. Nepal has over 250 peer-reviewed publications to his credit. He currently serves as the Interim Editor-in-Chief of IEEE Transactions on Service Computing and is a member of the editorial board of ACM Transactions on Internet Technology. Additionally, Dr. Nepal holds the position of Deputy Research Director at the Cybersecurity Cooperative Research Centre and is also a Conjoint Professor at UNSW.