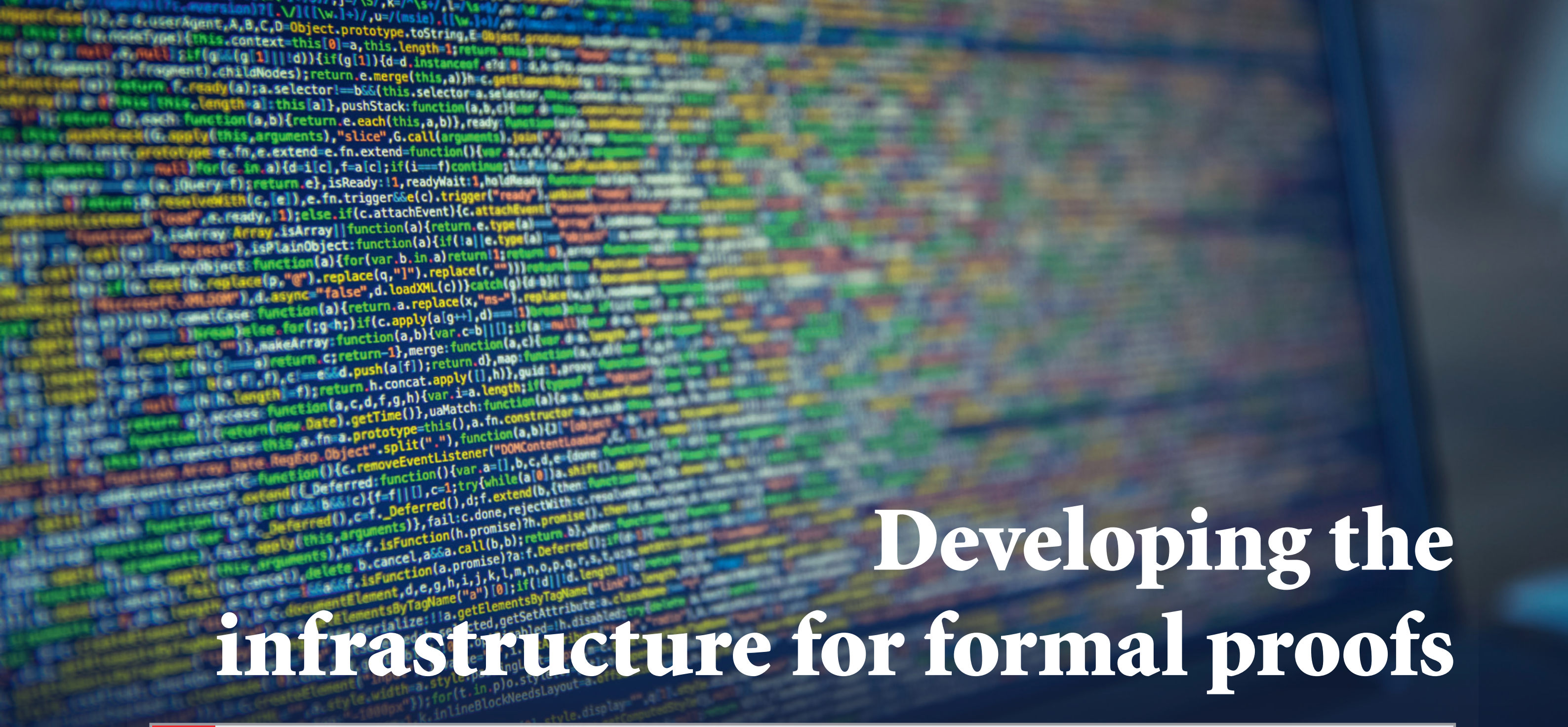


Developing the infrastructure for formal proofs

With computer systems playing an ever greater role in modern society, there is a growing need to establish their 'correctness' and their formal properties. We spoke to **Dr Dale Miller** about the ProofCert project's work in developing the foundations of a more accessible standard for formal proof, which could have significant implications in terms of software security

A vulnerability in a software system can be rapidly exploited, compromising the security of the computer systems we all rely on in everyday life, so it's increasingly important to establish their 'correctness'. However, the methods currently used to verify the formal properties of computer systems are splintered, says Dr Dale Miller. "Currently the world of formal methods is very fragmented. We use proof assistants to develop formal proofs – there are seven or eight major proof assistants," he explains. Based at the Inria Research Centre near Paris, Dr Miller is the Principal Investigator of the ProofCert project, an EC-backed initiative which aims to strengthen the foundations on which scientists can both prove mathematical theorems and establish the formal properties of computer systems. "The way it works today is that if you want to do a big proof you have to commit to using one of these proof assistants," he continues. "It may be very hard – if not impossible – to make use of results or tools from another community, another group of researchers."

Formal proofs

This fragmentation has consequences in terms of the way mathematicians prove theorems and establish the specific properties of computer systems. While established methods are still relevant in some situations, mathematics and computing has of course developed significantly over the last century or so. "Today we want to do formal proofs of very complex mathematical concepts and very complicated software systems, so it's really now a matter of scale. What worked long ago on much smaller systems doesn't always work so well today," explains Dr Miller. The project aims to develop standardised methods of defining a formal proof in the form of proof certificates; this holds interest in terms of both software development and more abstract mathematical research. "Some researchers have done a formal proof in a theorem prover called Coq of the famous mathematical theorem called the four-colour theorem. This is a theorem about how many colours are required to colour a geographic map," says Dr Miller. "The formal proof of that theorem was hard to achieve – a computer assisted proof was first achieved 40 years ago, but some mathematicians weren't convinced they could trust it. The more recent Coq proof is far more convincing."

There is a long history of research into these kinds of abstract questions, with mathematicians, logicians and philosophers all contributing to the development of the proof theory field, the study of the structure of mathematical proofs. While mathematicians like Gentzen, Church and Turing could not have anticipated the pace of future technological development, their papers

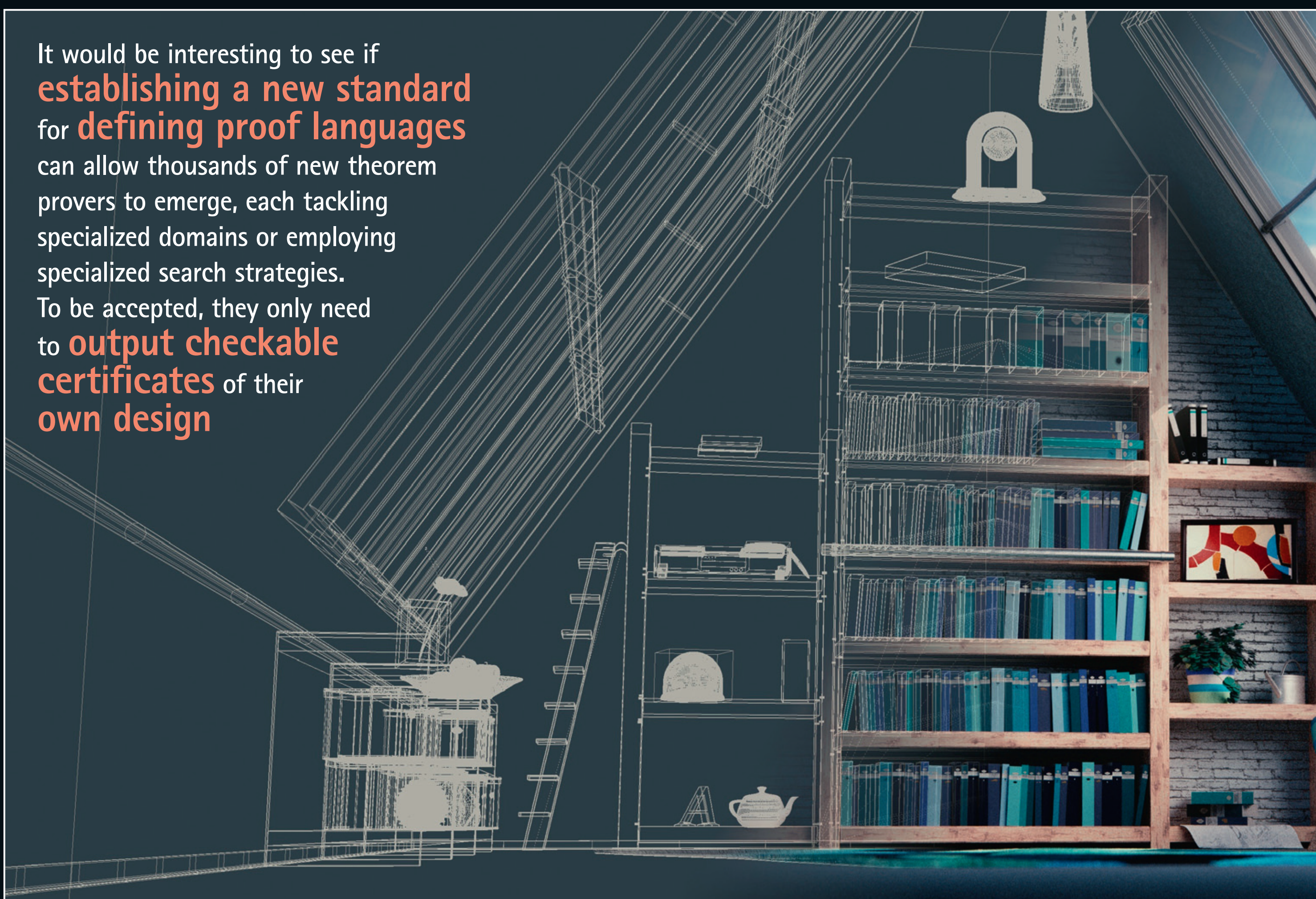
and ideas remain relevant in research; now Dr Miller and his colleagues are looking at them again. “We’ve been taking this old literature, dating back 70-80 years, and improving it. In a way, we’ve been trying to make it more computer science friendly,” he explains. Researchers aim to build on this earlier work by using the core elements of existing inferences to develop bigger inferences, which could help put in place the building blocks of enhanced software and hardware security. “It would be very interesting to eventually develop tools that could help us tackle security problems and assess whether a programme is correct. This could help prevent the emergence of bugs and problems in programmes that people could then exploit later,” continues Dr Miller.

This is not an immediate objective for the project however, and the current focus is more on laying the foundations for the next stage of development in formal methods. Within the project, researchers are concentrating on the fact that nowadays it is machines that build proofs, then communicate it to another machine that will check it. “ProofCert is a completely machine-to-machine project. These proofs are usually very complicated, and it’s inconceivable that a single person would be able to fully check it or that we would trust a human checker. But we still want to be able to check a proof now, and if doubts are raised at some point in the future, then they’d like to be able to re-check it again,” says Dr Miller. Many mathematical ideas are subject to re-examination; while abstract questions remain an important part of the wider agenda, Dr Miller says he often draws inspiration in research from issues around the ‘correctness’ of computer programmes. “To prove the correctness of a programme, you need to have a statement that says; ‘this programme should do the following...’ Then you state that as a proposed theorem, and look to prove that this programme does what it’s supposed to,” he outlines.

This programme might be the computer’s operating system for example, or a search engine. Establishing whether a programme is correct depends to a large degree on understanding and describing its purpose, yet Dr Miller says it can be difficult to state this formally. “Take the google search bar for example. It’s very difficult to state its purpose formally – it’s supposed to be useful of course, but defining that in a mathematical sense is a complex challenge,” he points out. A well-considered, systematic way of thinking about what a specific programme should be doing and its formal purpose is essential to verifying whether it’s correct; this starts right from the early stages of development. “When a programmer is asked to perform a task they’re typically given a specification. Usually, that’s in a natural language, not all of the details are fully filled in, and also it usually relies on other programmes that aren’t fully mathematically defined either,” explains Dr Miller. “Today it is a major challenge to formally show that a program satisfies all or even some of the properties expected of it.”

Formal proof

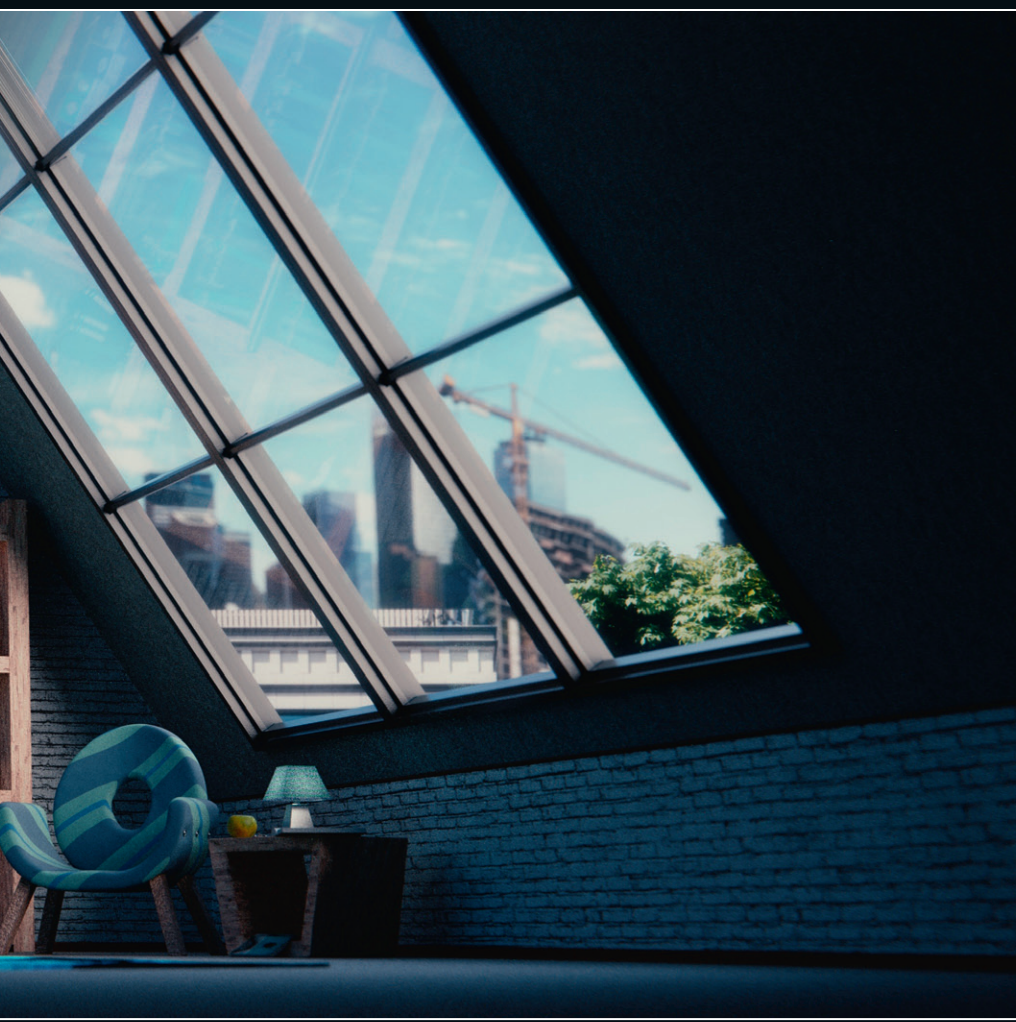
The wider goal in this research is to make proof universal, to standardise proof systems through proof certificates, an



> It would be interesting to see if **establishing a new standard** for **defining proof languages** can allow thousands of new theorem provers to emerge, each tackling specialized domains or employing specialized search strategies. To be accepted, they only need to **output checkable certificates** of their **own design**

objective which has historical parallels in the way text files evolved in the early years of the internet. Around 30 years ago, computers were distributed in small networks and it was relatively difficult for people to share text files, until Tim Berners-Lee and colleagues developed the HTML standard for creating webpages. "Now that those text files had a bit of extra structure, it was possible to build the worldwide web and things took off. So what was needed was standards," outlines Dr Miller. Researchers in the ProofCert project aim to develop an accessible standard for formal proof of the different documents that exist on different machines, work which could have significant implications in terms of hardware and software security. "Cybercriminals trying to break into computers have a very sophisticated network. They work together and sell each other malicious exploits," explains Dr Miller. "On the other side, in the formal methods community, we have different silos and we don't have an easy method of sharing our results."

A more systematic method of checking programmes, with dynamic and responsive formal methods, could help improve both the quality and security of software. Many aspects of software insecurity arise from programmes being incorrect, a context in which improved formal methods take on real importance, believes Dr Miller. "If we can improve the world of formal methods, developing proof certificates, then more people would use them, as more important programmes would be correct. By re-examining programmes with these sophisticated tools, the quality of software should improve," he says. The primary focus in research was developing a standard for interoperability between theorem provers, but with the project nearing the end of its funding term, Dr Miller is already looking towards new questions. "The next question I'd like to address is – how would we design a worldwide web of proof and how can we share, trust and learn from proofs?" he continues. "The general focus in my research community is on the generation of proofs. I'd like to add the additional focus of trying to make them permanent and useful once they have been found."



At a glance

Full Project Title
Broad Spectrum Proof Certificates (ProofCert)

Project Objectives
ProofCert has designed a universal framework for defining the semantics of the proofs exported by many of the world's theorem provers. Building on the mathematical theory of proofs, this framework provides a simple and declarative method for sharing and trusting proof evidence from a range of theorem provers. As a result, simple and trustable proof checkers can be built to check the correctness of the evidence within synthetized proof systems. Removing the need to formally trust theorem provers means that provers are free to evolve: they only need to output their proofs in formats that proof checkers can validate.

Project Funding
Funded by the European Research Council.

Project Partners
• Please see website for full details of collaborators and partners.

Contact Details
Project Coordinator, Dr Dale Miller
1 rue Honoré d'Estienne d'Orves
Bâtiment Alan Turing
Campus de l'École Polytechnique
91120 Palaiseau
T: +33 (0)1 77 57 80 53
E: dale.miller@inria.fr
W: https://team.inria.fr/parsifal/proofcert/

Focused labeled proof systems for modal logic by Dale Miller and Marco Volpe. The Proceedings of LPAR-20. November 2015. Springer LNCS 9450.

A framework for proof certificates in finite state exploration by Quentin Heath and Dale Miller. In the proceedings of PxTP 2015.

Dr Dale Miller

Dr Dale Miller is currently a researcher at Inria-Saclay and LIX/École Polytechnique after having been a professor in the USA and France. He has been the Editor-in-Chief of the ACM Transactions on Computational Logic and received the 2011 and 2014 Test-of-Time awards from the IEEE Symposium on Logic in Computer Science.

Parsifal

INVENTEURS DU MONDE NUMÉRIQUE