Creating secure computing environments

By Bennie Mols Images Ivar Pel

GROUP PASSPORT

RESEARCH FIELD

Formal methods; cyber-physical system security (including hardware security); secure processor technology and key management; machine learning and security

EMPLOYEES

3 Professors
1 tenure track researcher
3 scientific programmers
5 PhD students

INSTITUTION

Centrum Wiskunde & Informatica (CWI) based at Amsterdam Science Park. CWI is part of the Institutes Organisation of NWO.

WEBSITE

CWI research group computer security:
www.cwi.nl/research/groups/computer-security

Dutch Secure Autonomous Cloud:
portals.project.cwi.nl/dutch-secure-autonomous-cloud/

Marten van Dijk

Modern computing environments can have many points of attacks from hackers. Proving that certain attacks can never be possible is the aim of the new CWI research group Computer Security.

After 18 years of working in the USA, Marten van Dijk returned to the Netherlands, where, in June 2020, he started to lead the new research group Computer Security at the Centrum Wiskunde & Informatica (CWI). 'Being given the opportunity to establish my own research group is a fantastic challenge', says van Dijk. 'I worked for many years at MIT's computer science and AI lab, CSAIL. The motto there was: shoot for the stars. I feel that we can do the same at CWI.'

Van Dijk's new Computer Security group is an extension of the CWI Formal Methods group, which has a long history. Van Dijk's aim is to use the same rigorous style of thinking that characterises formal methods to create secure computing environments. Van Dijk: 'Let's say you want to fill in your tax papers on a virtual desktop that runs in the cloud. Then you want to be sure that by running it in the cloud, you don't create any extra security risk.'

As tests can never prove that a computing environment is secure, rigorous analysis is needed. It's just much harder to apply it to a complex computing environment, which has many possible points of attack, then to a cryptographic protocol. That's the big challenge of the Computer Security group. Apart from the Formal Methods subgroup, the new research group has three other subgroups: cyber-physical system security, secure processor technology and key management, and machine learning and security. Van Dijk himself has worked in all these fields. 'My expertise is new for the Netherlands', he says. 'And what we do at CWI is also complementary to what happens at the Dutch universities.'

One of his ambitions is to create a Dutch Autonomous Secure Cloud (DUSAC), for which he is already collaborating with academics from the computer security and computer systems community in the Netherlands. Van Dijk: 'Europe depends too much on American tech companies. It's vitally important that we develop our own secure computing environment in the Netherlands. I hope that in five to ten years DUSAC will be a reality, and that we will have managed to make it interdisciplinary by incorporating legal, policy and economic aspects of computing security. People from academia and businesses who want to join are welcome to contact us.'

Protect land against water

Leader of the cyber-physical system security subgroup is the Chinese tenure track researcher Chenglu Jin. 'In my research, I am interested in securing critical infrastructure systems, like the flood defence in Zeeland', says Jin. He did his PhD research with van Dijk in the USA and considered it a great opportunity to help build a new research group at CWI. Jin: 'Marten and I share the same security philosophy. Furthermore, the Netherlands has top researchers working on critical infrastructure systems protecting land from water.'

Chenglu Jin

Farhad Arbab

Cyber-physical systems are systems in which a digital system controls a physical system. The physical systems typically contains all kind of controllers, sensors and actuators. Applications vary from simple smart home devices to complex industrial control systems, power grids and flood defence systems. 'In my work, I formally model especially the interactions between various devices in cyber-physical systems', states Jin.

As Jin started his job last October in the middle of the pandemic unfortunately, he hasn't met any of his colleagues in real life yet. 'But every Friday we have an informal virtual coffee meeting, and every second Tuesday, we have more formal virtual discussions in which one group member presents his or her research.'

New dimensions

Having worked in the formal methods subgroup for some thirty years, Farhad Arbab is a kind of grandfather of the group. Although officially retired, he happily continues to do research and to inspire new talent. 'What I like about the new group is that it adds new security dimensions that we had not previously addressed', he says.

Arbab works on building new protocols and languages for the interaction between active entities in a computer system. Arbab: 'Increasing the number of agents or cyber threats rapidly leads to an exponential explosion of the number of interactions. At present, we only have low-level languages to reason over such interactions. It's like having to write a non-trivial Java program in assembly code. I try to develop higher level languages that make it easier to formally analyse the security of such systems.'

Expansion of the formal methods group to address security concerns allows Arbab to more widely apply his experience. 'One of the new projects I am working on is in cyber-physical systems. Take the example of a drone that has to survey crops. We want to diagnose exactly what can go wrong and why, and ultimately prevent it from happening or take compensatory actions.'

Creating a group culture without the opportunity to meet in person hasn't been easy over the last year, but Arbab is surprised how well the new collaborations have taken off: 'In spite of the pandemic and no face-to-face meetings, we have found a lot of common ground in all our virtual meetings.'