

Founded in 1425, the [Katholieke Universiteit Leuven](#) is a Flemish University of Catholic signature with an international orientation. It is the largest Belgian university with almost 35.000 students, of which 4.400 international students. With about 5.100 researchers in 2007, the research expenditures reached EUR 276 million. In the 2009 Times Higher Education Supplement (THES) university ranking, the K.U.Leuven was ranked 65th out of 200 world universities, making it the highest ranked university from Belgium as well as being the 21st highest ranked university in Europe. In a number of fields, including software security and distributed systems, the university aspires to a place among the centers of excellence in Europe and in the world. The Katholieke Universiteit Leuven is represented in this project by two research labs: the DistriNet Research Group of the Department of Computer Science, and the COSIC Research Group of the Electrical Engineering Department.

Research and networking expertise

With 50 members (including 3 professors and 10 postdocs), the [COSIC](#) team is one of the major European research groups in the area of security protocols and secure software/hardware implementations. COSIC has a track record of more than 20 EC sponsored projects (all of them with a substantial participation for key industry players), including the coordination of the IST Project NESSIE and the European FP6 NoE ECRYPT. During the past 20 years, COSIC has collaborated closely with industry and government on information security. Among others, COSIC is co-founder of LSEC, the Leuven Security Excellence Consortium (an association of 42 companies and research institutions in the area of e-security) and the industry security course SecAppDev. In addition, COSIC organizes the International Course on Computer Security and Cryptography on a yearly basis. Finally, COSIC is also active in international standardisation (ISO/IEC JTC1/SC27, IEEE, IETF, and OASIS). The research group SCD-COSIC (Computer Security and Industrial Cryptography) belongs to the Electrical Engineering Department of the Katholieke Universiteit Leuven. COSIC has contributed to the design and the evaluation the security of many practical systems (i.e. electronic identity card, electronic banking, electronic voting, UMTS). The Advanced Encryption Standard (AES), selected by the US government after an open competition has been designed by COSIC members and the hash function RIPEMD-160 is a joint design of COSIC and BSI (D). COSIC researchers have also obtained novel results in the areas of multiparty computation, privacy protection and interactive protocols. COSIC is one of the architects of the security infrastructure behind the electronic ID card in Belgium and is consulting regularly with FEDICT about the further development. The DistriNet research group is currently employing more than 60 researchers with approx. one fourth of these being post-doctoral researchers. The DistriNet research group has a strong track record of training and networking, mainly in three areas: (1) industrial training and technology transfer, (2) educational and training programs for bachelor and master students, and (3) academic training and networking. Firstly, DistriNet is actively involved in a broad range of industrial training and knowledge transfer programs. In the last

year, DistriNet co-organized several industrial security courses (SecAppDev and COSIC course), AOSD training workshops, as part of AspectLab, and the academic track at OWASP AppSec Europe. DistriNet also regularly disseminates research results at various industry-driven events, such as L-SEC, VSP, OWASP and Devoxx. DistriNet is also SANS' European partner for secure programming initiative. Secondly, for academic education and training, DistriNet supports both a bachelor and a master program in Computer Science, and recently started two new master programs on distributed systems and secure software. DistriNet also coaches yearly around 30 students during their MSc thesis. Thirdly, DistriNet has also rolled out a successful PhD framework, and 15 PhD students graduated in the last 3 years. To stimulate research discussion and cross-fertilization, DistriNet strongly supports the mobility of researchers (e.g., over 15 research visits in the last 2 years), and has actively participated in the ESF Scientific Programme MiNEMA, and European FP6 NoE on Aspect-Oriented Software Development. The DistriNet research group at Katholieke Universiteit Leuven is an internationally leading centre in software engineering research, with extensive expertise in secure software engineering and middleware for distributed software systems. DistriNet's research income is about 3.5M Euros per year. DistriNet is actively engaged in multiple national and international projects (e.g. over 40 national and 10 European projects started in the last 5 years) and is also part of the research institute IBBT. Experience has been accumulated in many application domains, often in close collaboration with industry (e.g. 100+ industrial partners in the last 5 years).

Key scientific staff

Wouter Joosen

Frank Piessens

Dave Clarke

Riccardo Scandariato

Lieven Desmel

Bart Preneel