The mission of the Institute for Computing and Information Sciences (ICIS) is to improve the fundamentals of software development via formal, mathematically founded theories, methods and tools that support the specification, design, analysis and evaluation of computer-based systems. Research aims include improving the quality of software, with an emphasis on enhancing reliability, security, systems architecture and system alignment. Work at the Institute is inspired by problems encountered in society – and in other disciplines. The applicability of the methods and tools is validated by tackling these problems. In 2008 research was concentrated within three research themes, each with its own specific focus and aims.

Computer systems now influence virtually every aspect of our lives. Sometimes these systems appear in an easily recognizable form, as in eCommerce sites such as Amazon, and pocket calculators, but they are also increasingly hidden inside public transport cards (OV chip), television sets, multimedia devices, mobile phones, cars and washing machines, for example. This trend is known as ambient computing. However, while computing is becoming increasingly pervasive, there are growing problems with software in terms of security (breaches of information access restrictions or privacy), reliability (the system behaves erratically), safety (use of the system is harmful), trustworthiness (low reliability of system services), efficiency (the system is unable to handle problems of a particular size) and conformity with requirements. The inherent complexity of computer-based artifacts - together with the slow pace of software development, high costs and strong competitive pressures - further complicates the search for solutions.

**Model-Based System Development (MBSD)**
Exploring various formal methods for model construction, implementation, testing and validation with the explicit aim of bridging the gap between theory and practice through collaboration with stakeholders from industry and other application areas.

**Digital Security (DS)**
Developing theories and formal methods for analyzing and improving security in the digital world. This involves on the one hand investigating the security and correctness of software (and other systems), and on the other, issues related to identity-centric security and privacy, i.e. developing approaches and protocols for managing and protecting digital identity.

**Intelligent Systems (IS)**
Developing and applying intelligent systems that are capable of learning and reasoning. The long-term research goal is to align computer-based intelligent systems with the needs of their users, answering questions such as how best to combine knowledge from human experts with measurement data, how to enable users to guide computerized proof 'assistants' and how people can profit most from a large repository of structured knowledge.
Awards

- Bernard van Gastel, Leonard Lensink, Sjaak Smetsers, and Marko van Eckelen together received the Best Paper Award at the 'Formal Methods for Industrial Critical Systems' conference.
- Rinus Plasmeijer received an honorary doctorate and professorship from ELTE University (Budapest, Hungary).
- The NAF Architecture Award was awarded to the ArchiMate team, which includes Erik Proper, Stijn Hoppenbrouwers, Nivea Ferrelra and Arjen Hommersom.
- Peter Lucas received the Best Paper Award at RNAIC'08.
- Research at ICIS on the Mifare Classic chip cards was awarded the I/O Media Award 2008. This is a national award by the Netherlands Organisation for Scientific Research (NWO) for bringing ICT research-related issues to the attention of the general public. The professional journal InformationWeek also featured it as one of the Top 10 Security Stories of 2008.
- The media interest surrounding the OV (Dutch public transport) chip card also helped Prof. Jacobs win the annual Franz Duyvestee Award, which is awarded to the member of staff at the University who received the most media attention in the previous year.
- Roel Verdult, a student who did his Masters thesis in the Digital Security group and became a member of the group after finishing his MSc degree, won the national 'Student of the Year' award issued by the student unions LSVb, ISO and ScienceGuide.

Collaboration

International cooperation is essential in the work done at ICIS, because developments in computing take place around the globe. Partners include MIT Computer Science & Artificial Intelligence Laboratory (USA), Ministry of Internal Affairs, ST Microelectronics (France and Belgium), University of Grenoble (Fr), RWTHA, Aachen (D), Cap Gemini, Makerere University Kampala (Uganda), INRIA Microsoft Research Lab Paris, ETH Zurich, ASML and Océ Technologies.

Research results

The most prominent result achieved in 2008 by the Digital Security section was undoubtedly the work on Mifare Classic RFID tags. This is a type of contactless chip card used as public transport and building access card in many places around the world, including
the Dutch OV (public transport) chip card and the Radboud University personnel card. This work, which started as two Master's thesis projects, has so far resulted in two scientific publications, at ESORICS and CARDIS. In research on software security and correctness, the paper 'Reentrant Readers- Writers' describes the combined use of theorem proving and model checking to verify a concurrent C program, an approach known as software surgery.

In the context of our research on brain-computer interfaces the Intelligent Systems section developed and tested new methods for extracting relevant features. In collaboration with GnuReads, new methods for personalizing hearing aids were developed and tested. The overview book (600+ pages) on Type Theory by Prof. Henk Barendregt and Dr Wil Dekkers has been completed and published in 2009. The Surf project 'Web Deduction' with the VU Amsterdam has led to a successful tool (www.prover.cs.ru.nl), which students can use to learn logic through a web-based system. The Web Deduction systems have also been extended with a 'certified calculator', which permits the certified computation of real values with arbitrary precision using the Coq system.

The Model-Based System Development section continued its work on model checking, a technique for automatic exploration of large state spaces. A framework for compositional abstraction of timed automata models makes it possible to check a complex Internet protocol for a random number of hosts, whereas previous methods could only handle three hosts. MBSD researchers succeeded in applying the Uppaal model checker to analyse models of the data path in copier machines. To develop embedded control systems in a multidisciplinary way, a 'lightweight' approach was developed that allows co-simulation of VDM++ and bond-graph models. In the BSIK/BRICKS project B-Screen, researchers at MBSD were able to develop and validate a Bayesian network model that combines information from different mammograms of the same patient. This resulted in improved cancer detection.

Societal impact
The Institute's impact is evident in various industrial projects designed to improve the quality of software, for instance in the medical domain (decision-support systems in the context of breast cancer screening – testing 'mindfulness') and with Ooe®, and ASML.
Bayesian techniques developed at ICIS are being used to combine data with background knowledge, for instance to localize sources in the brain and to improve the performance of brain-computer interfacing. The Digital Security section is regularly asked to examine security issues, including commercial contract research through LaQuSo, the Laboratory for the Quality of Software. In the past year the group investigated the Dutch e-passport, the new government personnel pass, the Rieti internet voting system used for Waterschapsverkiezingen (Water Board elections) in a joint project with TU Eindhoven, access control for the Electronisch Patiënten dossier (Electronic Patient Dossier, EDP), and smart electricity meters for Nuon. The group also investigated road pricing (kilometerheffing) and was contracted to develop a proof-of-concept test of the new electronic driving license. The ICIS continued to run CoDeYard, an innovative project set up to interest and involve high school students in the Netherlands and Belgium in computer science.

Future research
Within the Model-Based System Development section research will continue on the European FP7 project Quasimodo the NWO project ARTS and the ESI project Octopus (with Occ as the leading industrial partner). Within the Digital Security section research will focus on identity-centric security, which includes identity management and software security. Identity management involves investigating the policies and protocols used for identity management, mechanisms such as smart cards, RFID tags (e.g., in public transport), and the biometrics that can be incorporated, as well as the impact of this new technology on privacy and anonymity. Research on software security involves examining the role that software plays in the one hand in providing security and on the other as a source of security vulnerabilities. In collaboration with the Center for Neurogemonics and Cognitive Research at the VU in Amsterdam, the Intelligent Systems section will start a new project called GenetUSS (Gene Networks Underlying Synaptic Signalling). The aim of this project is to develop dynamic models of neurotransmitter vesicle release. The MathWiki system project, which will start in 2009, is geared to making formalized mathematics available through a web interface that provides both high-level (standard mathematical style) and low-level (proof code) access — for reading and for joint cooperative developments.