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 artefacts – together with the slow pace of software development, high costs and strong competitive pressures – further complicates the search for solutions.

The Institute for Computing and Information Sciences (iCIS) was established 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, architectures and system alignment. The quality of the research remains very high, resulting in many Netherlands Organisation for Scientific Research (NWO) grants in 2013, including three NWO Venis for Dr Alexandra Silva, Dr Peter Schwabe and Dr Sicco Verwer, an ASPASIA for Dr Lejla Batina and a TOP grant for Dr Elena Marchiori. Work at the Institute is inspired by problems encountered in society as well as by issues arising in other disciplines.

Members of the Institute advocate open source software as well as (digital) security by design and openness (in contrast with security through obscurity). In the same spirit, iCIS promotes a culture of openness when dealing with scientific integrity. Work in progress (papers, research proposals and research methodology) is discussed.
regularly in small meetings within the institute, which are open to every iCIS member. Software and data are made freely available whenever possible. Security weaknesses that have been spotted are first reported to the companies or authorities involved before they are made public.

Research within iCIS is organized within three themes:

**Model Based System Development (MBSD)**
The approach used is to explore 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, in other application areas and in companies.

**Digital Security (DS)**
Researchers develop theories and formal methods, which they use to analyze and improve the security of the digital world. The scope of the research includes software and hardware (in particular smartcards and RFID), identity management, security protocols, applied crypto, quantum computation and legal aspects.

**Intelligent Systems (IS)**
The aim here is to develop and apply intelligent systems that are able to learn knowledge and reason with it. The long-term research goal is aligning computer-based intelligent systems with their users, answering questions such as how to optimally combine knowledge from human experts with measurement data, how to enable users to guide computerized proof assistants and how to let humans profit optimally from this large repository of structured knowledge.

**Collaboration**
International cooperation is an essential part of the work done at iCIS, because developments in computing take place around the globe. Partners include the Dutch Ministry of Internal Affairs for a project on business process reengineering (BPR), the University of Grenoble Joseph Fourier, France (Tarot), KU Leuven (EU project FutureID, ESF Cost network TRUDEVICE), IBM Research Zurich (EU project FutureID), Makerere University Kampala, Uganda (NUFFIC), TNO Delft, the Netherlands, Aalborg University, Denmark (Artiste) and Océ Technologies, Venlo, the Netherlands (Octopus), the Dutch Foundation for Internet Domain Registration (SIDN), the Dutch Banking Association (NVB, Amsterdam), Radboudumc (ParkinsonNext project), Thales and TNO-ESI, Eindhoven (Metsis) and TILT (University of Tilburg).

**Research results**
Prof. Herman Geuvers’ team has worked on a variety of methods and tools relating to proof assistants. They have redefined dependent type theory in a ‘context free’ fashion, which is important for implementations of type theory as a proof assistant. The MathWiki system was developed further, leading to a first prototype called ‘Agora’. The group has also obtained a variety of results on coinduction and coalgebra, notably providing coalgebraic descriptions of language equivalence and studying language determination. Prof. Barendregt – working together with Profs. Dekkers and Statman – finalized the handbook ‘Lambda Calculus with Types’ (833 pp), which was published by Cambridge University Press.

Prof. Heskes’s Machine Learning group is involved in three EU projects that are designed to reveal the causal mechanisms behind complex diseases. Within these projects, the Machine Learning group’s task is to develop new techniques for data fusion and causal analysis that make use of all available data to obtain a better understanding of the aetiology of the disease and to derive putative biomarkers. The group continued the successful line of research on causal discovery. In causal discovery, the goal is to learn the structure of causal processes (‘smoking causes ‘cancer’) from observations (‘correlation between smoking and ‘cancer’). Tom Claassen’s PhD thesis, on a logical approach towards causal discovery, received a cum laude distinction. In collaboration with researchers at the...
Donders Institute for Brain, Cognition, and Behaviour, Heskes’s group developed novel probabilistic methods for inferring brain networks from diffusion-weighted magnetic resonance imaging (DWI) as well as resting state functional magnetic resonance imaging (fMRI) time series.

In collaboration with the Microbiology group at the University, Dr Marchiori’s team developed a method for improving the retrieval of anammox bacterial genome from metagenomes. Furthermore, in collaboration with the Netherlands Brain Bank group, the team analyzed brain data from donors with multiple sclerosis, using machine learning techniques in order to reveal associations between brain lesions and gender. The results indicated the presence of significant associations between brain lesions and gender in multiple sclerosis. Dr Marchiori’s team continued to perform research on methods for the study of complex systems described by means of networks.

In 2012 Prof. Rinus Plasmeijer’s team introduced a new programming paradigm called Task Oriented Programming, which should make developing distributed web-enabled multi-user systems much easier. In 2013 this team continued working on an implementation of this idea, the iTask system, in order to be able to develop more realistic applications in collaboration with industry partners. Practical applicability has been investigated in two areas. The Dutch Coast Guard uses the iTask system to design a new prototype for ‘coordinating ‘Search and ‘Rescue’. And TNO has been using the iTask system to investigate new ways of working on Navy Vessels in the hope that these can be operated with a much smaller crew. TNO has decided to use the system as a standard tool for this type of investigations.

The research in Prof. Frits Vaandrager’s team on automata learning is highly relevant in the security setting, as it makes it possible to obtain models of the behaviour of malware (botnets, for instance) and to discover security vulnerabilities in the communication protocols that are used in for instance bank cards. Significant funding has been obtained to continue research in this area through an NWO Veni grant for Dr Sicco Verwer, an NWO Free Competition proposal ALSEP, and a project LEMMA that was funded in the context of NWO’s Cyber Security programme.

The research in Prof. Peter Lucas’ team on eHealth continued in collaboration with clinical partners from Radboudumc. The aim of this research is to empower patients while improving the quality of health-care and reducing its costs. Patients are supported by smartphones equipped with an intelligent reasoning engine that can interpret signs, symptoms and sensor data (blood pressure, lung function and the results of biochemical lab tests) and offer feedback on their health status. The new concept of a multi-level Bayesian network, introduced by iCIS in 2012, offers useful tools for exploring the temporal evolution of disease interaction in very big healthcare datasets. This research was done in close collaboration with NIVEL. In addition, an NWO Free Competition grant was awarded to explore our new idea of state-based Bayesian network structure learning. Work on new frameworks of probabilistic logic also continued, both at the fundamental level and in the context of surveillance applications (in collaboration with Thales).

Research on privacy-friendly authentication using attributes under the name IRMA (I Reveal My Attributes; see irmacard.org) led to several publications, not only about the mathematical foundation of anonymous credentials and efficient implementation on smartcards, but also about the eco-system for attribute-based authentication. This eco-system is now being tested in a small student pilot among students doing the Kerckhoff Security Master’s programme. Research on embedded security under the supervision of Dr Lejla Batina in new STW and NWO projects has led to the establishment of a security lab for side-channel analysis. Dr Peter Schwabe was awarded an NWO Veni grant to investigate super-fast safe crypto.

The ERC advanced grant ’Quantum Computation, Logic, and ‘Security’ started in 2013. Three new PhD students and one postdoc, together with Prof. Bart Jacobs as Principal Investigator, have begun work on this new field. Robert Furber MSc and Prof. Bart Jacobs published a paper at CALCO’13 showing that the category of commutative C∗-algebras with positive unital maps can be described as a Kleisli category of a monad. This result is interesting as it connects the mathematical work on C∗-algebra in quantum and probability theory to categorical notions such as monads (as in program semantics).

Research on ’Privacy by Design’ carried out within the Privacy & Identity Lab identified eight privacy design strategies, which were presented at the Privacy Law Scholars Conference at Berkeley and published in the journal Computer Law & Security Review. These strategies can be used to take privacy into account from the early stages of designing new information systems.

The paper ’Dismantling Megamos Crypto: Wirelessly Lockpicking a Vehicle ‘Immobilizer’ by Flavio Garcia, Roel Verdult, and Baris Ege was accepted for the USENIX Security Symposium, but had to be withdrawn from publication following legal proceedings in the UK.

Research on applying state machine learning to security analysis – in collaboration between the DS and MBSD groups – was successfully applied to automate the security analysis of EMV bank cards and of smartcard readers used for Internet banking.

As a follow-up to earlier research carried out in the Laboratory for Quality Software (LaQuSo), which revealed security weaknesses in Blackboard Learn, a countermeasure was designed which was presented at NordSec2013. This countermeasure is also being tested to secure the University’s own Blackboard website.
which advises the Dutch Cabinet on cyber security issues and Dr Hoepman is a member of the Dutch commission on electronic voting “Electronisch stemmen in het stemlokaal” set up by the Ministry of the Interior. Further evidence of societal relevance and impact is the fact that the Dutch Banking Association (NVB, Nederlandse Vereniging van Banken) now funds a part-time chair in Information Security (Prof. Verheul). Bayesian techniques developed at iCIS are being used to combine data with background knowledge, for instance to localize sources of activity in the brain and to improve the performance of brain-computer interfaces. The iCIS ‘Web Deduction’ system (www.prover.cs.ru.nl) is used to teach logic in a number of courses at several universities.

Future research
Research on side-channel analysis and on fast and safe implementations of cryptography will intensify following the start of the new NWO and STW projects led by Dr Batina, the Veni grant of Dr Schwabe, and the European Science Foundation (ESF) COST network TRUDEVICE. A new EU project USEMP will start researching online social networks. USIMP will use legal, socio-logical and computer science techniques to provide transparency on the economic value of personal data. More research on the privacy and security of personal data, in particular medical data, will be carried out in the recently started ParkinsonNext project, in collaboration with Radboudumc, among others. PhD defences for two joint doctorates with the University of Leuven will take place early in 2014. Dr Marchiori’s team will continue to work on analysing complex systems represented by graphs. The focus will be on theoretical foundations of graph clustering and applications in life sciences and social and economic sciences. Multi-disciplinary research on e-health and bio-informatics will be further consolidated.

Societal impact
The Institute’s impact is evident in various projects that were designed to improve the quality of software. Examples include those in the medical field (developing new tools and techniques to analyse and describe clinical and pathological data which can be used to understand and improve the prognosis, diagnosis and treatment of several diseases, such as neuro-degenerative diseases, testing ‘mindfulness’, etc.) and model checking, together with Océ and ASML. A 2nd Phase STW Valorisation grant was awarded to Prof. Peter Lucas to move towards the market introduction of a smartphone app that will support COPD patients in detecting any worsening of their condition.

Cyber security and privacy are increasingly important in today’s information society. Public interest in these topics continues to grow, making headlines in the news almost on a daily basis. The Digital Security group not only addresses these concerns through its research, but also plays an active role in public debates on these issues. The group’s expertise is in heavy demand from both the public and private sector, on topics such as the smart grid (especially smart electricity meters and smart charging of electric vehicles), the security of web applications (including the Blackboard learning system, which is also used at this University), electronic payment systems, electronic voting, and identity cards. Many of these consultations happen through short-term contract research projects via LaQuSo. Moreover, TenneT, the national electricity transmission operator in the Netherlands and much of Germany now funds a PhD student in the group, and research has started on the privacy and security of medical data in a new collaboration with Radboudumc (the ParkinsonNext project). Prof. Jacobs is a member of the National Cyber Security Council, which advises the Dutch Cabinet on cyber security issues and Dr Hoepman is a member of the Dutch commission on electronic voting “Electronisch stemmen in het stemlokaal” set up by the Ministry of the Interior. Further evidence of societal relevance and impact is the fact that the Dutch Banking Association (NVB, Nederlandse Vereniging van Banken) now funds a part-time chair in Information Security (Prof. Verheul). Bayesian techniques developed at iCIS are being used to combine data with background knowledge, for instance to localize sources of activity in the brain and to improve the performance of brain-computer interfaces. The iCIS ‘Web Deduction’ system (www.prover.cs.ru.nl) is used to teach logic in a number of courses at several universities.
Key publications


Tom Heskes has been a professor since 2008, specializing in Artificial Intelligence, in particular Bayesian machine learning. Since 2007 he has been a Principal Investigator at the Institute for Computing and Information Sciences and an Affiliated Principal Investigator at the Donders Centre for Neuroscience. He won a prestigious Vici grant from the Netherlands Organization for Scientific Research in 2006 and is Editor-in-Chief of the journal *Neurocomputing*.

Through ongoing collaborations with Radboudumc, in particular within the Centre for Systems Biology and Bioenergetics. Several newly collaborations, with the Dutch brain bank (Alzheimer) and within the EU projects TACTICS (obsessive-compulsive disorders) and OPTIMISTIC (myotonic dystrophy), will support the development of data mining and machine learning algorithms to gain insight into disease progression and the causes underlying brain diseases. Further e-health research, including those on the self-management of chronic diseases, will move towards implementation in clinical practice. In collaboration with commercial companies, modelling workflows and active learning of software components will be taken to the next level, both in theory and in practice.