CASE STUDY

HARDWARE SECURITY

Background

Computations are not only performed in obvious devices such as smartphones, but most modern appliances are equipped with computing hardware. This includes cars, washing machines, thermostats, and even smoke alarms and pacemakers. Many of these devices connect to WiFi to perform services such as app integration or automated updates. By being online, these devices are however not only available to their intended user, but can also be found and controlled by malicious partners. This is problematic for essential devices such as pacemakers and cars, but also small everyday devices can be profitable to hack in order to steal personal data, spy in peoples' homes or send spam messages.

A secure Internet of Things (IoT) is therefore a research priority of computer security researchers. Devising secure everyday items comes with its own challenges. The solutions should be lightweight and cheap enough for consumer goods, easy to implement and should consume very little energy in order to minimize the carbon footprint of the IoT and to extend the battery lifetime for user comfort. A promising development is hardware security. In this approach, secure computation and communication are embedded within the hardware of the device, rather than in a software application ran by that device. This means that the device cannot be compromised by changing the software installed on it at a distance, which is the main attack mode of hackers. For instance, a device can be equipped with dedicated hardware that protects software from unauthorized modification or dedicated hardware to encrypt and decrypt data that are transmitted and received by the device.

Research approach

At LIACS, researcher Nele Mentens specializes in hardware security. She is professor of Applied Cryptography and Security in the Advanced Computing & Systems group. She investigates how to implement security in devices with limited capabilities, with special attention to security measures that are not fully baked into the device but can be configured remotely. Security in IoT devices requires careful balancing, as there are many requirements that the solution has to meet. In general, you might want to implement a solution that has a minimal energy use, but in some cases the security measures in the device might have to be heightened temporarily. This can be for instance in anticipation of an imminent attack or when performing a crucial task, such as the transfer of sensitive data. The solutions that Mentens proposes include the possibility of making small adaptations in the hardware that change its function, allowing for multiple security levels that can be chosen depending on the situation, or allowing secure remote upgrades of the hardware.

Impact

The work of Nele Mentens is a prime example of impactful research that arises from a strong core of computer science research, and comes to fruition through collaboration with other research fields and industrial partners. As she has a background in electrical engineering at KU Leuven, Mentens does not limit herself to devising protocols and mechanisms, but is also involved in actual design of hardware and chips. Her group translates the hardware security solutions they propose into working demonstrators. In cooperation with external partners, her security solutions have already been implemented in prototypes for drones (DroneMatrix) and medical wearables (several academic medical centres). There is a major interest in hardware security from industry, as the rise of IoT devices and their increased regulation create a demand for lightweight and flexible security solutions. There are public-private collaborations with industrial partners, such as STMicroelectronics, NXP, Airbus, Riscure and numerous smaller security and electronics companies.

Publications

S. Zeitouni, J. Vliegen, T. Frassetto, D. Koch, A. -R. Sadeghi and N. Mentens, "Trusted Configuration in Cloud FPGAs," In IEEE 29th Annual International Symposium on Field-Programmable Custom Computing Machines (FCCM), pp. 233-241, 2021.

M. Labafniya, S. Picek, S. E. Borujeni, and N. Mentens, "On the feasibility of using evolvable hardware for hardware Trojan detection and prevention," Applied Soft Computing, Volume 91, No. 106247, 11 pages, 2020. (research performed at KU Leuven)

M. M. Rabbani, J. Vliegen, J. Winderickx, M. Conti, and N. Mentens, "SHeLA: Scalable Heterogeneous Layered Attestation," IEEE Internet of Things Journal, Volume 6, No. 6, pp. 10240-10250, 2019. (research performed at KU Leuven)

Projects/grants

"PROACT - Physical Attack Resistance of Cryptographic Algorithms and Circuits with Reduced Time to Market"
Funding: Dutch Research Council, Dutch Research Agenda, Cybersecurity – Towards a Secure and Reliable Digital Domain
Budget: 1.8 million euro
Partners: Radboud University, Riscure
Role: coordinator

CASE STUDY

SAILS: AI IN ALL FACULTIES

Background

Leiden University has recognized artificial intelligence (AI) as a research priority for the entire university. To direct its investments and promote interfaculty collaboration, the university has launched the interdisciplinary programme SAILS in 2018. SAILS stands for Society, Artificial Intelligence and Life Sciences, and aims to create a university-wide network of researchers using AI. It does this by funding research chairs on AI throughout the university, bringing together researchers by organizing symposia, workshops and seminars, and also acting as a coordination hub for joint initiatives in AI research, education, and funding. To date, SAILS has funded seven Chairs within the university, and stood at the basis of many successful research projects involving all faculties of Leiden University (Archaeology, Governance and Global Affairs, Humanities, Law, Medicine, Science and Social and Behavioural Sciences).

Role of LIACS

As research institute for computer science and AI, LIACS has a major role in the initiation and execution of SAILS. The programme was a bottom-up initiative, launched by Professor in Data Science Aske Plaat in 2018, who also was the first head of the programme. LIACS recognized the need for a more united approach with regard to AI, and convinced the university to create an interdisciplinary research programme for AI. Plaat was succeeded as programme director of SAILS in 2020 by Joost Batenburg, who joined LIACS in that year as the second SAILS Professor.

According to Batenburg, SAILS is a fruitful initiative that unites AI activities within Leiden University. 'The large possibilities of AI have caused a proliferation of AI-related initiatives in nearly all domains of scientific research. SAILS prevents a fragmented situation where faculties are separately investing in multiple small-scale AI initiatives.' Through SAILS, it is easy for domain experts to get into contact with AI experts at LIACS and elsewhere, and work together. And vice versa, SAILS monitors developments on a national and international level, and approaches researchers with new research initiatives whenever it sees an opportunity. 'This fulfils a clear need for researchers throughout the university, as can be seen from the active participation by all faculties involved.', says Batenburg.

Successful collaborations

Participation in SAILS has resulted in collaborations between LIACS and all faculties of Leiden University. Some take the form of internal projects, while others have attracted external funding and/or involve external partners. Examples of research projects are:

- **Hybrid, semi-supervised Deep learning for advanced image segmentation and annotation;** Collaboration between LIACS (Dr. Daniel Pelt), LUMC (Dr. Oleh Dzyubachyk; SAILS), and Archaeology (Dr. Tuna Kalayci; SAILS) with applications for cell segmentation in microbiology and detection of archaeological sites in satellite data.
- **Socially embedded AI systems for natural machine learning and human-machine interaction;** Collaboration between **LIACS** (Dr. Tessa Verhoef), **Psychology** (Dr. Roy de Kleijn), and **Leiden University Centre for Linguistics** (Prof. Stephan Raaijmakers) on the emergence of intelligent interaction in groups
- **Artificial Intelligence for Drug Discovery;** Collaboration between **Leiden Academic Centre for Drug Research** (Prof. Gerard van Westen; SAILS), **Chemistry** (Prof. Mario van der Stelt), **LIACS** (Prof. Joost Batenburg; SAILS, Prof. Thomas Bäck and others).
- **AI for Decision Making in Public Governance;** Collabiration between **Leiden Institute of Governance** (Prof. Bram Klevink; SAILS), **eLaw** (Dr. Francien Dechesne), and **LIACS** (Dr. Joost Broekens).

More information:

SAILS website

CASE STUDY

CLAIRE

Background

In 2018, AI researchers Holger Hoos (LIACS), Morgen Irgens (Oslo Metropolitan University) and Philip Slusallek (German Research Center for AI) noted that Europe was starting to fall behind in AI research. AI was quickly developing into a game changing technology with major implications for industry, politics and society, with large tech companies such as Google, Microsoft and Facebook and government-funded research institutes in America and Asia at the front. While Europe historically has a strong AI community, efforts are fragmented and scattered over hundreds of research institutions. As a result, there is no coordinated European effort to provide guidance to the EU and the individual countries with regard to policies and investments.

Hoos, Irgens and Slusallek realized that, if Europe wanted to keep technological sovereignty, there needed to be one European AI community speaking with one voice. They drafted a vision document on a Confederation of Laboratories for Artificial Intelligence Research in Europe (CLAIRE) and started to approach colleagues to invite them to join the initiative. In June 2018, CLAIRE launched with 600 supporting researchers and stakeholders.

The focus of CLAIRE is on trustworthy AI. It believes that the development of new technologies should not be left to large companies or individual governments to be used for their own ends. It promotes and supports the development of new technologies focusing on addressing major societal challenges to the benefit of all. AI should reflect the European realities, needs and values.

CLAIRE in 2021

CLAIRE has rapidly grown into a major player in European AI research and policy. The launch attracted a lot of press coverage, including the Dutch, German and Belgian national news, and attracted new stakeholders to the network. With over 400 associated labs, it unites the majority of AI researchers in Europe. CLAIRE has developed into a non-profit organization with 23 staff members and 8 offices throughout Europe. It organizes events, conferences and webinars where researchers can meet and discuss topics related to AI, advises the European Commission on policies and investments on AI through advisory groups and coordinates a network of centres of excellence on specific topics funded by the EU. During the corona pandemic, CLAIRE proactively launched a special taskforce to advice governments on the use of AI in addressing the pandemic. The work of CLAIRE has recently been recognized: the network was awarded the prestigious German AI Prize 2021, together with colleagues at ELLIS.

CLAIRE has even bigger ambitions for the future. It is working on expanding the network with industrial partners within Europe, thereby becoming the world's largest player in trustworthy AI. To this end, CLAIRE wants to set-up a lighthouse centre for AI, a major European research institute comparable to CERN or ESA to which all European countries contribute. By providing critical mass for investments, their effect can be maximized when compared to a large number of small projects by multiple institutes.

The role of LIACS

The early work on CLAIRE has mainly been the voluntary work of the three founders. They form the Board of CLAIRE, currently with Hoos as chair. The network was realized within a few months, which Hoos was able to do with full support from the management of LIACS. He was provided with administrative and financial support, and freed of his duties. This is a clear example of how LIACS works: an agile and flexible management, devoted to support the initiatives of its researchers.

The benefits for the institute are clear: LIACS has become a major player at the forefront of AI in Europe, with direct access to the vast network and funding of CLAIRE, and an influential role in advising on European AI policy. In the first round of European seed funding for AI, amounting to 50 M€, LIACS has become involved in two centres of excellence, on the foundations of trustworthy AI (Ai4Media) and on human-centred AI (HumaneAI Net).

Further information:

https://claire-ai.org/

CASE STUDY

EVOLUTIONARY COMPUTING WITH INDUSTRY

Background

Designing a powerful car with low fuel consumption, minimal docking time of ships in harbours without queues in case of delays: finding an optimal solution requires a careful balance of many different factors. Thomas Bäck, head of the Natural Computing research group at LIACS, investigates whether AI can be used to find optimal solutions for complex optimization problems. This can be many different problems, ranging from the best way to design ships to predicting the condition of an aircraft based on its performance. His cutting-edge research generates substantial interest from industry.

Research approach

Bäck's expertise is evolutionary computation: a computational method that use the principles of reproduction, mutation and selection to evolve into versions of themselves that are better adapted to the specific circumstances. These algorithms can be done on simulated data in design processes, but also on operational data. They weigh up different aspects and suggest the best option.

An important question is how different factors contribute to the optimal result. For instance, a long and slim ship will have less hull resistance and will require more steel to build compared to a shorter and wider ship with the same cargo capacity. What shape and design will be the more fuel efficient and sustainable? In the life-time of a large ship, small differences in such aspects can have a major influence on the environmental impact of the design. Another application domain is the optimal maintenance schedule for vehicles. Ideally, maintenance should be scheduled before wear and tear can cause damage, so the out-of-service time of the vehicle is minimized. The algorithms developed by the group aim to predict what the optimal time for maintenance is, and how this can be predicted from operational data.

Sometimes major gains can be found in unexpected aspects. In a recent research project with industrial partner C-Job Naval Architects, one of LIACS's PhD students, Roy de Winter, discovered in operational data that one of two identical ships, was over 30% more fuel efficient than the other. Upon inspection, one of the ships has just been cleaned, and the other was still coated in algae and barnacles. This shows that cleaning of ships is a very influential factor and should not be cut back on when looking for gains.

Impact

The research conducted by Bäck and his group is fundamental in nature. The idea to use evolutionary computation on complex optimization problems is relatively new, with many directions and methods still to explore. Nevertheless, Bäck has already found industrial partners to be willing to invest in this type of research. These partners see the potential gains of the approach and want to be involved in this cutting-edge research from the very start. Examples of projects are public-private partnerships with automotive industry (DAF Trucks, Honda Research Institute Europe, Volkswagen, BMW), air transportation (KLM), as well as production and manufacturing (TataSteel Europe, ASML). As such, evolutionary computing is a prime example of the research conducted at LIACS: firmly grounded in the foundations and methods of computer science, with a strong application orientation explored with external partners.

Papers

DE WINTER, R.; VAN STEIN, B.; DIJKMAN, M.; BÄCK, T. (2019), Designing ships using constrained multi-objective efficient global optimization, Machine Learning, Optimization, and Data Science, pp.191-203, Springer,
DOI: https://doi.org/10.1007/978-3-030-13709-0_16

CASE STUDY

PROGRAMMING EDUCATION

Background

Programming is increasingly being recognized as an essential skill for modern society. Not only do many careers require knowledge of coding, citizens interact with computer code on a daily basis, making it important to have at least a basic understanding of how programming works. This shift towards programming education for all requires a fundamental different approach. Traditionally, education was targeted towards adults, and required a deep dive into software jargon and syntax. Efforts to make programming accessible for children gave rise to visual click-and-pull block programming languages, such as Scratch. However, these languages are limited, and at some point the young programmers have to switch to a text-based language. This is often experienced as a large step, with many ways to mess up, leading to frustration. Felienne Hermans at LIACS works on bridging the gap between block and text-based programming languages to help young adolescents take this step.

Research approach

Programming education researcher Felienne Hermans is associate professor in Programming Education, and head of the Programming Education Research and Learning (PERL) group at LIACS. When noticing the difficulties high school students had in learning programming language Python, Hermans started to draw parallels with how pupils learn how to read and write. This is often learnt by first learning the letters, then words and full sentences, and only then the correct interpunction. This principle lies at the basis of programming language Hedy, that Hermans developed for high school students. Hedy gradually introduces the rules of correct programming by only introducing new elements when students have shown to master the previous elements. For instance, students can start by giving simple text commandos. When they are successful, other elements like loops are introduced. And only when these elements are grasped by the students, they are confronted with the correct syntax to give commands in Python.

Hedy is divided into 22 levels that students can complete in an average of 45 minutes. During a level, students work on small projects using the elements they just learned, such as creating an interactive story or simulating a simple dice game. If successful, they unlock the next level, motivating the students to continue with the programme. Hermans paid attention in Hedy to not only teach programming syntax, but also explain why these rules exist and what happens when the rules are applied incorrectly in helpful error messages. This adds to the understanding and prevents frustration.

Impact

The work on Hedy combines several of LIACS's strategic aims. It combines core computer science research with insights from educational sciences to create societal impact, and contributes to educating the next generation of computer scientist. To maximize impact, Hedy is available as free-to-use software, and available in 11 different (natural) languages, with more planned. Analysis of the programmes developed by the students is input for further research by the PERL group, as it shows how the kids interact with the programme and how their learning curve develops.

Hermans is a strong and visible voice in programming education. She aims to enthuse kids to learn to code, create equal opportunities for boys and girls in this and convince policy makers to invest in programming education at young ages. She was awarded with the Dutch Prize for ICT Research 2021, 'for her research into making computer science and programming accessible to a wide audience, as well as for her pioneering role in establishing a new direction within Dutch ICT research and education.'

Publications

- *Hedy: A Gradual Language for Programming Education.* Hermans, F.J. ICER '20: Proceedings of the 2020 ACM Conference on International Computing Education Research, August 2020 Pages 259–270
- *Gradual Programming in Hedy: A first user study.* Marleen Gilsing, Felienne Hermans, VL/HCC 2021, October 2021 (upcoming)

Website

https://www.hedycode.com/?lang=en
https://www.youtube.com/watch?v=EdqT313rM40&t=22s (Hedy introduction talk for general public)
https://www.youtube.com/watch?v=R2U9MEowYag (in-depth Introduction for Codeweek 2021)

CASE STUDY

QUANTUM AI

Background

The quantum computer radically differs from classical computers. It uses the quantum properties, usually detectable only at atomic scales, to realize a computing device whose advantages over conventional computers grow exponentially with the number of particles (quantum bits or qubits) used. Such devices hold the promise to perform computations that are simply impossible to do on classical computers. After large investments in quantum computing research in the past decade, prototypes with a small number of qubits have shown that the principle works and is technologically feasible. There is still a lot of work to do before quantum computers can be produced that are stable and can outperform classic computers on useful tasks. Yet experts are confident that within 10 years we will have quantum computers which perform various useful computations which are beyond the reach of any conventional supercluster.

To achieve advantages over classical computers, quantum computers need to run dedicated algorithms that are specifically designed to exploit their quantum features. Devising such algorithms is a major challenge, and is developing into a separate field of research where computer scientists and physicists work together to investigate what a quantum computer can actually do.

Research approach

LIACS is involved in quantum software research, and works on machine learning algorithms for quantum computers. Dr. Vedran Dunjko is one of the lead scientists in LIACS's quantum research. The domain of machine learning is a promising area where it is expected algorithms which can realize a quantum advantage could be found. In recent papers (see below), a team of researchers lead by Dunjko, have shown that quantum computers can perform reinforcement learning faster and in exciting new ways compared to classical algorithms. Furthermore, as a part of an international collaboration, they have shown quantum technologies of the type developed at QuTech can provide the basis for reinforcement learning speed-ups in a future quantum internet. Reinforcement learning is a machine learning technique that trains AI by learning from their trial-and-error efforts.

Unique to LIACS research is the hands-on, applied approach that the institute has with regard to quantum computing. According to Dunjko, the first quantum computer prototype has shown that a new paradigm is needed. 'The first generation of quantum computers will be error prone and have a limited number of qubits. Algorithms that have been developed over the 30+ years of quantum computing theory cannot be run on such devices. We need to find new classes of algorithms that work on the available and near-term systems.' To do this, LIACS works with the Leiden Institute of Physics (LION), and the Leiden Institute of Chemistry (LIC) on a full pipe-line approach in the applied Quantum algorithms (aQa) initiative. The process starts with defining the quantum computer that is actually available, and analyzing the system to find out what algorithms this particular machine would be good at. One possible approach is the cutting up of computations in smaller parts.

Dunjko feels that the open-minded character of LIACS has been instrumental in developing this research line. 'LIACS is extremely open to new ideas suggested by researchers, and has trusted and facilitated our group to develop our own approach. As the institute is very open to establishing relationships with other fields, boundaries are easily erased, so we are frequently working with physicist at LION and QuTech in Delft, that literally have their hands on a quantum device.' This has been very successful, and Leiden is developing into one of the national hubs for quantum research.

Impact

Quantum computing already attracts substantial interest from industry. LIACS is working with oil companies Shell and Total on the prediction of earthquakes, and the development of new tools for chemistry, and automotive company Volkswagen on various industrial challenges that can possibly benefit from quantum algorithms.

According to Dunjko, quantum computers will have a major impact in society and industry, but in which domains is far from certain. 'There are many promising research directions. Examples are the discovery of new materials and molecules, for instance for drugs and batteries, or the prediction of geoscientific or economic events and risks. It is impossible to say at the moment which efforts will succeed and which will not. But when there is a success, and I am confident that there will be successes within 5-10 years, it has the potential to be ground-breaking.'

Papers

- Quantum Enhancements for Deep Reinforcement Learning in Large Spaces. Sofiene Jerbi, Lea M. Trenkwalder, Hendrik Poulsen Nautrup, Hans J. Briegel, and Vedran Dunjko. PRX Quantum 2, 010328 , February 2021. https://arxiv.org/pdf/1910.12760.pdf
- Variational quantum policies for reinforcement learning. Sofiene Jerbi, Casper Gyurik, Simon Marshall, Hans J. Briegel, Vedran Dunjko, 10 March 2021, https://arxiv.org/pdf/2103.05577.pdf
- Quantum agents in the Gym: a variational quantum algorithm for deep Q-learning, 9 March 2021, https://arxiv.org/pdf/2103.15084.pdf
- Experimental quantum speed-up in reinforcement learning agents", V. Saggio, B. Asenbeck, A. Hamann, T. Strömberg, P. Schiansky, V. Dunjko, N. Friis, N. C. Harris, M. Hochberg, D. Englund, S. Wölk, H. J. Briegel, and P. Walther, Nature, 10 March 2021; DOI: 10.1038/s41586-021-03242-7