Data protection and security

Researches what is technically possible in terms of security: Prof. David Basin, Head of the Institute for Information Security at ETH Zurich.

Protection against cyber risks and protecting critical infrastructure against cyber criminality are of utmost strategic importance for the Federal Council. ETH Zurich has been actively engaged for years in the information security arena in both basic and applied research alike. The collaboration that has been established with industrial partners is especially valuable. It enables scientific insights to find their way quickly into commercial practice, with the added bonus that people in this field who leave ETH Zurich are exceptionally well trained.

The strategic objectives that the Federal Council adopted in its National Strategy for Protecting Switzerland against Cyber Risks in mid-2012 are unequivocal. At issue are the "early detection of threats and dangers in cyber space, increasing the resilience of critical infrastructure" and the "effective reduction of cyber risks, especially cyber criminality, cyber espionage and cyber sabotage."

ETH Zurich's "Zurich Information Security and Privacy Center" (ZISC) plays a key role in this respect. It was co-founded in 2003 with private sector companies. Today, Credit Suisse, Google, security technology provider Kaba and the Federal Department ArmaSuisse are partners in ZISC. Joint research projects are underway in fields such as cryptography, design methodology and network & system security. "The motivation for this collaboration originally came from industry," says Professor David Basin, who holds the Chair for Information Security at ETH Zurich. "This means that when it comes to security research, ZISC is able to play a dual role that is probably unique in the world." While the scientific perspective is concerned with basic research and proceeds according to the principle of what is possible in terms of security and what is not, the application of solutions focuses on engineering aspects such as the efficiency, cost, usability and maintainability of security systems. "This feedback between theory and practice is extremely valuable for both sides because in addition to collaborating with project partners, it is one of the prerequisites for bundling forces and thus increasing their impact, which is what politicians are calling for," says David Basin.

Joint research projects with industry

One of ETH's doctoral students spent two months working on site with ZISC partner company Google on the ongoing project "Monitoring and Supervision of Data Use" and an ArmaSuisse expert was involved with another project, also not yet concluded, on specific risks posed by the shared use of file servers. A number of projects, however, are also directly linked to everyday matters. One of these is the "Data Deletion" project launched in the autumn of 2011 in what was then ZISC's newly established Institute for Information Security. The issue here is whether and how data in Smartphones and Clouds can be deleted securely. In the process, the researchers not only encountered major gaps in security but also looked for ways and means of closing them. Ordinary deletion processes that are currently featured as standard on Smartphones offer no real protection. The ETH Zurich researchers therefore developed an application based on Android devices which ensures that the data both in the Smartphone's memory and on external storage media are completely overwritten. This application is now available to users free of charge.

Numerous IT applications are now unimaginable without cryptography such as in all instances where individuals need to be reliably identified and data safely transmitted. This is a complex problem: data are transferred between computers connected with one another in a computer network by means of so-called protocols which are being programmed in increasingly complex ways in order to satisfy more stringent security requirements. This, however, is a two-edged sword: increasing complexity also brings with it possible sources of error and this in turn produces new gaps in security. One way of preventing this may lie in reducing the protocols' complexity. ETH Zurich researchers are therefore working on modular data transfer solutions. "Cryptography needs to become a design discipline like many engineering disciplines such as automotive or software construction," says Ueli Maurer, Professor at the Computer Science Department and Head of the Information Security and Cryptology Research Group. "We hope in this respect to be able to bring about a fundamental paradigm shift in cryptography."

Industry supports new Chair

The industrial partners providing financial support to ZISC gain fruitful connections from this collaboration. Both sides benefit from the exchange of knowledge and gain insights into research work and practical applications. The partners also sometimes initiate scientific projects. The telecommunications group Swisscom, although not a ZISC partner, also provided start-up funding to support the establishment of a new Chair for Information Security. The telecommunications provider converted a loan of ten million Swiss francs to the ETH Zurich Foundation into a donation. In the autumn of 2012 this enabled ETH Zurich to make a direct appointment of Professor Adrian Perrig, one of the world's leading scientists in the field of system security. Professor Perrig is a former computer science student at EPFL and completed his doctorate at the Carnegie Mellow University in Pittsburgh, where since 2002, in addition to his professorship, he has also headed Cylab, one of the world's largest research centres for information and computer security.

This increases the number of professors in the information security field in ETH Zurich's Computer Science Department to four. "With the four professors, other colleagues and the high quality of its work, ETH Zurich is establishing itself as a leading centre for information security," says David Basin. This is also apparent in the fact that ETH Zurich now offers more than 15 courses in this advanced discipline. Graduates are specialists who are sought after by the private sector ZISC partners, industry in general and the public sector.