Schlussbericht / Resumee Breakout Session No. 2

Cybersecurity, Privacy and Ethics – Opportunities and Threats for a Digital Society

Edgar Weippl, Dominik Engel, Katharina Krombholz, Michele Loi, Matteo Maffei, Stefan Mangard, Joe Pichlmayr, Marjo Rauhala, Elisabeth Schludermann.

Security, privacy and free data exchange are in a quite contradictory relationship: on the one hand is a desire to exchange data freely and unhindered to take advantage of new opportunities offered by the "Internet of Things" and "Industry 4.0" - but on the other hand privacy and security are becoming increasingly important for data protection, system reliability, and safety. Technical solutions as well as combinations are manifold, but what is ethically justifiable? Many different aspects play an essential role - from cryptography to software design, from legal questions to ethics. As conclusion we pointed out necessary structures and measures for ethically-reflected research in Austria to remain a recognised gloabel player.

Designing instead of reacting

The growing complexity of today's digital world makes the understanding and enforcement of security and privacy properties a profound, long-lasting technical challenge, with an enormous societal, economical, and political impact. Companies are mandated by law (see, e.g., the new GDPR) to adopt state-of-the-art security and privacy technologies and to embed the so-called security and privacy by design principles in the design phase; authorities and public bodies are increasingly confronted with critical decisions related to the security of critical infrastructures and to the privacy of citizens; and end users are daily asked to explicitly or implicitly take security and privacy-relevant decisions without having the required technical background.

Highly integrated production plants, smart homes and autonomous vehicles: the Internet of Things is becoming an increasingly significant element of private and professional life. Linking the real world with the cloud delivers greater convenience and increased productivity – but also completely new threats. Cybersecurity has implications for all products and systems – from everyday objects to data centers – and represents a major challenge for our society.

Challenges of cybersecurity ethics

1. there are still many interesting and practically relevant ethical issues in the ethics of cybersecurity that wait to be discovered, or that are known to practitioners already but have escaped our reviews. To develop this blooming field, Austria absolutely needs the collaboration of cybersecurity practitioners. E.g. can the use of biometrics in border control be made more ethical? What would this entail?
2. cybersecurity scholars and practitioners are sometimes disconcerted and put down by the inability to reach agreed upon conclusions in ethical discussions. Ethical debates are sometimes more open ended. There is cultural resistance that needs to be considered and dealt with.
3. while some cybersecurity professionals are aware of the ethics issues, it is still challenging to optimize our way of teaching ethics (and our ethical framework themselves). Academic ethics needs to change and be adapted to be maximally usable in this field. This requires an interdisciplinary way to assess the quality of philosophical ethics, to generate new methodological ideas to pursue it in new directions, and how best to adapt it to be valuable in addressing the problems of these individuals.

Security and Privacy initiatives and activities in Austria

Most recently the Vienna Cybersecurity and Privacy Research Center (VISP), an inter-institutional initiative of IST, TU Wien, and Uni Wien, was established. It aims at addressing the aforementioned challenges by creating a worldwide leading research and educational center, making Vienna the place to be for students, researchers, industry, and stakeholders in the domain of cybersecurity and privacy.
Graz University of Technology founded recently the Cybersecurity Campus Graz together with SGS, the world's leading inspection, verification, testing and certification company. The campus is planned to host around 400 researchers and experts from industry upon full operation to create an unique environment for research and education.
The Austria IT Security Hub is a platform for an intensive and sustainable cooperation between a wide variety of companies and individuals in the cyber security environment and the education sector.
The aim is to set up these sustainable structures in order to implement the development of cybersecurity awareness at a broad national level, as well as basic and excellence programs in the field of education and training based thereon. The development of corresponding "security" base programs will not work without corresponding development of "digital skills" in broad sections of society as well as these should be striven for hand in hand in the education sector.

Future structures and support for ethical security research in Austria

- Possibilities to conduct and follow an interdisciplinary approach fostering genuine interdisciplinarity between security research, social sciences, humanities, and ethics
- Structures for research review and oversight that support researchers in competitive environments and are sensitive to particular aspects of security research
- Initiatives with a clear focus:
  We see three distinct types of initiatives that are essential to Austria actively shaping and supporting security research:
  1. Centers/Clusters of excellence with permanent funding to conduct basic research and attract high-potential/profile international researchers offering life-long career perspective. This is necessary to retaining a leading role for Austria in the international competition.
  2. Temporary centers that address a specific sub-topic. These centers are best established within an existing organization to minimize overhead. Currently successful examples are Christian-Doppler Labs, Josef-Ressel centers and – COMET modules.
  3. Centers that form a longer-term bridge between research and industry. These centers are best established as independent organizations with close ties to both industry and academia. Currently successful examples are COMET centers. Unfortunately, the funding stability of COMET centers is not comparable to German counterparts such as the Helmholtz institute CISPA in Saarbrücken, the Max-Planck-Institute in Bochum, CRISP in Darmstadt. Aside from the overall budget, these German research institutes can hire permanent staff (e.g., tenure track researchers) due to the permanent funding.
- Clear political commitment

Edgar Weippl, Dominik Engel, Katharina Krombholz, Michele Loi, Matteo Maffei, Stefan Mangard, Joe Pichlmayr, Marjo Rauhala, Elisabeth Schludermann.