Roadmap for cyber security research

March 12 2019

Credit: CC0 Public Domain

In their secUnity roadmap, 30 renowned European IT security experts of the BMBF-funded secUnity collaboration outlined how digital threats on the European level can be responded to more efficiently in the future. Among these experts also are researchers from Karlsruhe Institute of Technology (KIT). Today, the secUnity scientists will present the

roadmap in Brussels and hand it over officially to the ENISA European Union Agency for Network and Information Security.

Information transmission, transport, industrial production, research, administration—hardly any area can manage without modern information and communication technologies. At the same time, the number of cyber attacks that become known is increasing constantly. Such attacks on digital infrastructures by criminals or state organizations threaten our prosperity, the security of our societies, and eventually, our freedom and democracy. At an evening event at the representation of the state of Hesse with the European Union in Brussels, secUnity scientists will discuss "Civil Cyber Security Research for Digital Sovereignty" with representatives of the European Parliament and European Commission. Then, the secUnity roadmap will be published officially and handed over to the European Union Agency for Network and Information Security.

"The hazard potential of cyber attacks in highly developed countries cannot be overestimated," warns Professor Jörn Müller-Quade, Spokesman of KIT's Competence Center for IT Security KASTEL. Within secUnity, IT security experts from all over Germany cooperate. Apart from the three national competence centers KASTEL, CRISP, and CISPA, specialists of the universities of Darmstadt and Bochum and of the Fraunhofer Institutes for Applied and Integrated Security (AISEC) and for Secure Information Technology (SIT) are involved.

Cyber security experts have long criticized that companies and public institutions are not adequately prepared for digital threats. On the contrary: due to progressing networking and digital trends, such as Industry 4.0, smart homes, or autonomous cars, potential points of attack by cyber criminals even increase. In the roadmap initiated by the secUnity collaboration and funded by the Federal Ministry of Education and Research (BMBF), more than 30 European authors now identify future challenges and potential solutions. Among the problems analyzed

are the security of embedded systems, machine learning, lacking awareness, and fake news. Then, measures to enhance security are outlined.

The experts strongly criticize the frequent use of hardware solutions without any IT security check. This threatens digital sovereignty of Europe. "This situation might be improved by European testing institutes that independently analyze the technology," says Professor Michael Waidner, Director of the National Research Center for Applied Cyber Security CRISP and of the SIT Fraunhofer Institute in Darmstadt. Moreover, open-source software and hardware solutions should be developed transparently in the EU.

But approaches to developing trustworthy European solutions are not sufficient to effectively protect interconnected systems, as they will continue to incorporate a large number of inexpensive, but insecure hardware and software components in the future. Using the smart home as an example, Professor Claudia Eckert, Director of the AISEC Fraunhofer Institute in Munich, says: "We need solutions to minimize the risks of such components and to operate the systems in a resilient way. Cameras, door openers, heating controls, any automatic device at home may be the gateway for big attacks. Secure gateways to connect insecure components ensure that sensitive information will not leave home and control components cannot be accessed from outside." Resilience in spite of uncalculable components has to be guaranteed in particular for critical infrastructures, such as healthcare and energy supply systems, as well as for public authorities and companies.

Development of quantum computers that is being pushed worldwide also entails major risks. Jörn Müller-Quade warns: "A quantum computer big enough to threaten the security of current cryptographic methods has not yet been built, but this might change quickly. Current progress in quantum technology is such that we have to take precautions today

already. We have to provide our complex interconnected systems with reliable encryption methods. These still remain to be studied in more detail."

Also artificial intelligence methods with their many new applications are associated with severe risks for IT security: machine learning processes can be attacked easily by specific manipulations during the learning and operation phases. "Before these technologies can be applied in critical areas or to improve the quality of life, trust in these processes and in their reliability will have to be placed on a scientific basis," Professor Thorsten Holz from Ruhr-Universität Bochum demands.

The new opportunities associated with the information society, such as smart grids that make everyday life more comfortable and help save energy, give rise to questions regarding the legal basis and in particular data security legislation. "In view of the fundamental risks caused by the digitization of entire industry sectors and of critical infrastructures, such as power and energy supply, we urgently need a harmonized legal framework for IT security in Europe," says Dr. Oliver Raabe of KIT's Center for Applied Legal Studies (ZAR). Legal standards as to which risks are acceptable and which security measures can be taken by companies still remain to be developed. The same applies to requirements relating to quality assurance and integrity of big data.

In addition, citizens who increasingly use complex communication systems have to be supported in protecting their privacy and IT security. "Research is therefore aimed at e.g. developing methods for a privacy advisor. When uploading photos or messages, such methods are to assess the risks and to reveal how much additional private information is disclosed by the publication. This would help citizens use social networks confidently," says Professor Michael Backes, founding director of the CISPA Helmholtz Centre for Information Security.

As data inventories are getting larger and larger, many companies will be given new possibilities of innovation, but there will also be the risk of losing an apparently secure market position in the digital era. "Data as such are not the petroleum of the 21st century. They will only come into value, if business models are developed that make them valuable. And valuables deserve special protection," explains Peter Buxmann, CRISP scientist and Professor of Information Systems and Information Technology as well as Director of the HIGHEST startup innovation center of Technische Universität Darmstadt. Citizens have to become aware of the value and protection needs of their data. On the other hand, use and further processing of data have to be transparent and fair price models of suppliers have to be implemented. "Politically speaking, we should therefore move away from the principle of data economy towards data sovereignty and we should request and support fair business models," Buxmann underlines.

"To master all these challenges, civil cyber security needs an interdisciplinary network of experts for civil cyber security research on EU level," summarizes secUnity speaker Jörn Müller-Quade.

More information: For further information, click here: it-security-map.eu/en/home/

Provided by Karlsruhe Institute of Technology