Goals

Our goal is to create a comprehensive and systematic list of cybersecurity risks in medicine as well as potential measures that are known so far that may address these risks that will be published in an Opinion Paper that is work in progress.

Residual risks that cannot be mitigated need to become a part of the mandatory information a patient receives from the medical personnel before a treatment. Our analysis will also account for the fact that the usability and security requirements in the medical field are different from business and military applications and that healthcare is associated with specific ethical and legal requirements for which cybersecurity should account as well. One goal is to develop new security paradigms that account for these differences and help implementing a non-intrusive security approach that does not endanger the successful treatment of patients by reducing usability, speed and availability of the supporting ICT systems. Special emphasis will be given on outlining ethical conflicts that addressing these risks may have. This serves as a basis for a follow-up research project intending to empirically assess how these conflicts are perceived among stakeholders.

Another goal may be to outline what would need to be done on an international level in order to achieve a common understanding that digital medical infrastructures are never a legitimate target and that every party has the responsibility to avoid collateral damage during operations in the cyber space. In that sense, the workshop also touches upon issues of international humanitarian law. This is why we also involved experts from the WHO

Major disciplines represented

- Health Anthropology/Health Law

- Bioethics

- Epidemiology

- History of Philosophy

- Political Science

- Sociology

- Epidemiology

List of the speakers

Endre Bangerter (organizer & chair), Bern University of Applied Sciences, Switzerland
Alessandro Blasimme, University of Zurich. Switzerland
Gabriella Cattaneo, E-Sides Project, IDC European Government Consulting, Italy
Markus Christen (organizer & chair), University of Zurich, Switzerland?
Jens Clausen, Freiburg University of Education, Germany
Martin Denz, Swiss Association for Telemedicine and E-Health, Switzerland

Josep Domingo-Ferrer, Universitat Rovira i Virgili, Tarragona, Catalonia
Patrick Dümmler, Health Tech Cluster Switzerland and Avenir Suisse, Switzerland
Kherif Ferath, CHUV Lausanne / Human Brain Project, Switzerland
Dominik Herrmann (organizer & chair), University of Hamburg, Germany
Reto Inversini, Swiss Reporting and Analysis Centre for Information Assurance
David-Olivier Jaquet-Chiffelle, University of Lausanne, Switzerland
Bonnie Kaplan, Yale University, USA?
David Krieger, University of Lucerne, Switzerland?
Hannes Molsen, Drägerwerk AG & Co. KGaA, Germany
Kathrin Noack, SecUnity Project, Germany?
Nicola Orlandi, Novartis, Switzerland?
Bart Preneel, KU Leuven, Belgium?
Andreas Reis, World Health Organization, Switzerland
Marc Ruef, Scip AG Zurich. Switzerland?
Marcel Salathé, EPFL Lausanne, Switzerland?
Bernd ?Carsten Stahl, De Montfort University, United Kingdom
Mariarosaria Taddeo, University of Oxford, United Kingdom
Yung Shin Van Der Sype, KU Leuven, Belgium
Ahmed Walid, Federal Office of Public Health, Switzerland
Karsten Weber, OTH Regensburg, Germany?
Harald Zwingelberg, Unabhängiges Landeszentrum

Outcome

Brocher meeting summary (the Opinion Paper is work in progress and will be submitted later this year).

The meeting was instrumental to obtain inputs to better think about the ethics of cybersecurity in the health care and to discuss some emerging issues. Although the presentations were divided into three sections (systems, devices and information), there were significant overlaps among the presentations in the different slots. By combining the different inputs, the following problem landscape emerges:

Requirements and desiderata for health systems: Health care industry is in an early phase where the problem is being recognized step by step. Other industries went through the same cycles and are partly still in it. It is the responsibility of all participants to support these efforts. Many attacks are not special to healthcare and so are many countermeasures. However care must be taken as the potential damage of attacks as well as of unwanted side effects of security measures are very high. Good technical security needs to be considered in every development phase, starting with the training of personnel, during the requirements phase, the design phase, development, testing and also during operations. Technical Security measures should be lightweight and as unintrusive as possible. If they interfere with the daily work of personnel, it is likely that they cause side effects or that they are bypassed. It is important to have a balanced approach that integrates all aspects of IT security in order to avoid building high protection on one side and allowing the attacker to easily gain access on the other side. The security of medical devices cannot be defined without looking at the whole environment where they are running (systems they connect to, systems for configuration, persons that connect to, their awareness, etc.) It is important to accept that attacks can happen and will happen. This means that health care must build up detection and reaction capabilities in order to minimize the damage.

Ambitions of future information and communication technology in health: The recognition of cyber-security challenges

and the optimization of cyber-security defenses must consider several evolving features of the social and economic landscape around data. First of all, health-relevant information can potentially be inferred from a variety of new sources. Reconstructing a person's overall health situation and prospects from the myriad of facts represented in her "digital phenotype" is necessary to preserve the holistic view of the person at the center of medicine. Second, each source of data can be made available for different uses (e.g. health, wellness, philanthropy, public health) and each use comes with specific cybersecurity and privacy risks attached.

Challenges and new developments: Cybersecurity is a technological arm race between socio-technical weapons and defenses. The increasing amount, capacity, and heterogeneity of connected systems steadily generate new vulnerabilities, forcing affected stakeholders to renegotiate the existing level of cybersecurity constraints. Different decision-makers and affected stakeholders must be coordinated in order to generate, and make socially acceptable, an adequate level of economic investment and unavoidable sacrifices of usability and privacy. Without an appropriate coordination of stakeholders, cybersecurity strategies risk becoming ineffective, or worse, backfire. Achieving such coordination is itself a new socio-technical challenge for which new forms of governance should be developed.