Starting shot for Quantum Engineering

The foundations of quantum research are there now it should go for application. The University of Saarland offers from next winter semester the interdisciplinary bachelor study programme "Quantum Engineering". Also ETH Zurich educates from spring quantum engineering which should serve the query for skilled personnel. They will work between the disciplines electro technique and quantum science (previously known under physics). At least from the name itself quantum engineering has the potential to be the new "Rocket Science".

Gravitational Force and Light

Physics: A picture should bring forth the first, experimental proof of Einstein's "Relativity Theory". For this Sir Arthur Stanley Eddington waited for total solar eclipse on 29 May 1919 on the Prince Island in the Gulf of Guinea with a camera. Why? The Relativity Theory indicates that gravitation is in a position to diffract light. This hypothesis, the British astronomer mathematician and physicist could only verify when star light fell past on the earth very close to the sun and through the diffraction the position of the star appeared changed. While in back light of the sun however no star is to be recognized. Eddington travelled to Africa for the next total solar eclipse. Here he pressed on the trigger at the right moment and fixed on the generated snapshot. The position of the star appears in fact shifted compared to a photo, which was generated one and a half years before in the night. With that the exactness of the relativity theory as claimed by the British physicist was proved. The extremely small deviation led again and again to doubt to the Eddington's reasoning, however, it was insignificantly corrected in 1979 by a new measurement.

VDI nachrichten, 7 June 2019, Nr. 23, Seite 3

Anil Kumar Ghosh

Hacker vis-à-vis Medical Professionals

IT Safety: The careless treatment with safety measures in hospitals and physicians' consultancy rooms causes main targets of cyber attack. Stolen incoming data are the gateway in any concern and the cause of most thefts of sensitive pieces of information. Before April 2019 the United Association of Insurance Economy adopted some serious study to this effect. It investigated how clinics and physicians' consultancy rooms with password turn around with alarming results.

The authorized IT specialists in the framework of the study found in darknet 60% of the incoming data of the German clinics as also one of ten physicians' consulting rooms. Many doctors apparently are lacking the consciousness for IT safety. 9 out of 10 physicians utilized easy to guess password regarding treatment or their own names according to the study.

Easy booty (spoil): The safety of the patient data is inadequate. The analysis of the e-mail server of around 1200 settled down doctors showed that only 5 observed standing of technique of the Federal Office of Safety in the information technique (BST).

As in the USA & Germany previously no mentionable theft of patient data has been known to which the complete differing structures of the insurance system and health insurance is indebated. Safety deficiency in clinics and physicians private chambers can change that. Many medical practitioners were an easy spoil with cyber attacks – the investigation discovered. In every second the coworkers opened a potential damaged mail, 20% clicked rather on a link or opened the appendix. Markus Holzbrecher Morys of German Hospital Association (DKG) knows management stimulating example: Coworkers have fear probably to open virus affected Emails in house. Instead of that they open in hospitals, while they are of opinion that IT professionals are there in service and it cannot happen there.

If an attacker first once in physician's chamber or clinical network has penetrated, the attacks start on most differing systems also on medical equipment. Through that life threatening dangers generate for the patients. A safety researcher succeeded in it with a laptop to bring under his control an anesthesia instrument and in the meantime still control further vital functions besides respiration. On hacked up insulin syringe or injection syringe the attackers could change the prescribed medication doses which may cause death to patients.

Previously we have not seen any targeted cyber attack on medical equipment – says Heidenreich in conversation with the VDI nachrichten. However it comes to that the doctors could pull the data plug as nodelay measure and in spite of that work further. The function of medical instruments is also without network guaranteed through that however the course of work is delayed while nearly patient data must be manually written off.

"Quick changes at these installations of equipment are not possible" Heidenreich cries out. When a patch comes from Microsoft we require in individual case three to four weeks before that is tested by us, then the reliability of the apparatus may not be impaired through an update.

Modernization is possible: The manufacturers of medical equipment are aware of increasing danger. They increase the cyber safety of their products particularly with which they must calculate, with safety leakage to be taken into account strongly in future.

They faced the problem that the equipment in hospitals and physicians' private chambers are managed some years, there, however, may old systems are to be seen. Moreover it deals with some apparatus with small internet of things components which arrange for a few storages and weak processors.

In spite of that suitable measures can increase the safety on behalf of the management. "It gets a firewall added in order to protect sensitive components "clarifies Heidenreich. So also different clinical areas get isolated from each other. Generally we recommend a separation from normal work place – PCs and medicine apparatus from that place a network segmentation is meaningful he advises each area (domain) practically in one's own network and communicate only on special gateways with other departments.

More Protection: Additionally the manufacturers mobilize the saleable protection measures. Whitelisting is such a possibility with those working implements really only function which is important for the assignment, reports Heidenreich. Whitelisting prevents the other processes starting up. The security specialist mentions further steps. New medicinal apparatus are set in container and virtual machines. In that a separate management system runs only for the medicinal special application. In future a cloud connection of special medicinal apparatus may be planned and the components can be better protected.

Anil Kumar Ghosh

VDI nachrichten, 3 May 2019, No. 18,
Sicherheit, Seite 9 von UWESIEVERS.