Fraunhofer

TRENDS FOR CYBER SECURITY

CONTENT

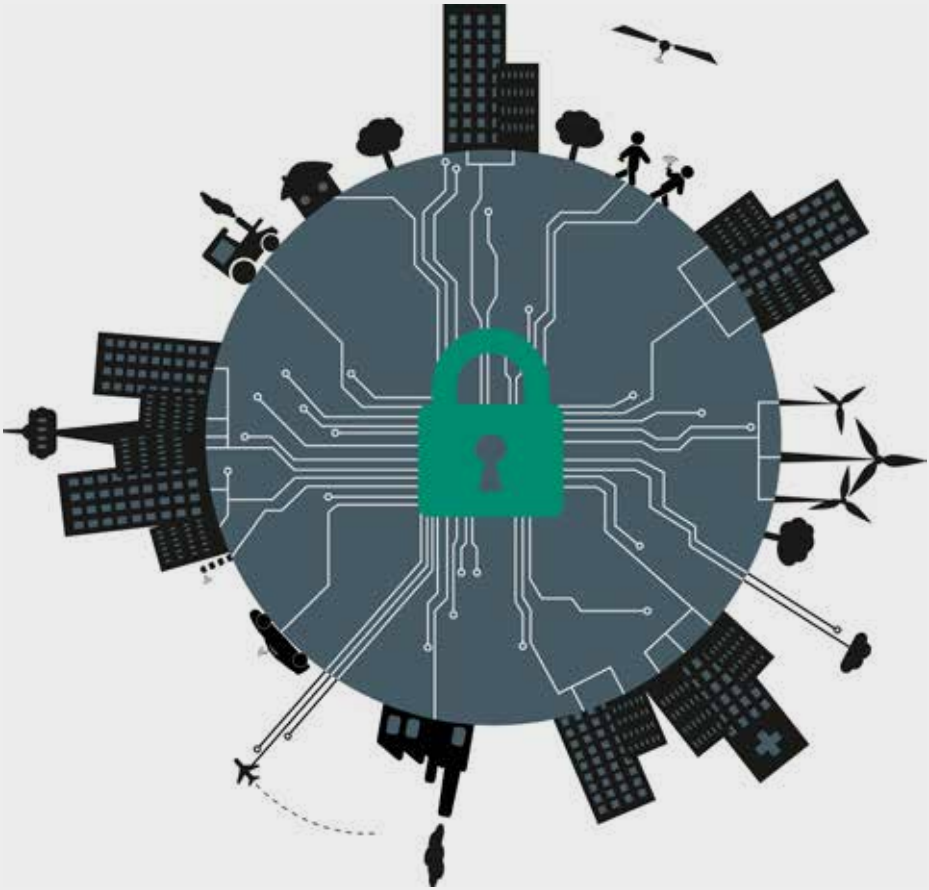
TOWARD A SECURE DIGITAL FUTURE

Cyber security is one of the cornerstones of digitalization. If people don't trust in the security of new technologies, the digital transformation will not succeed. In 2015, 45,000 cases of cybercrime causing total losses of 40.5 million euros were reported to the German Federal Office of Criminal Investigation. The number of unreported cases undoubtedly runs much higher. Meanwhile, the potential economic benefit of digitalization is increasing. Experts estimate that businesses in western Europe alone could earn an additional 420 billion euros between now and 2035 thanks to higher profit margins and less tied-up capital.

Risks and opportunities go hand in hand in the digital world. Being online means being open to attack. The more complex the structure, the greater its vulnerability. The purpose of cyber security research is to minimize risks in order to tap opportunities without compromising security. The Fraunhofer Institutes conduct research in many security-relevant fields, including critical infrastructures, industry 4.0, automotive security and Internet security in general. The examples featured in this brochure represent only part of this wide range of activities.

Education and training is a topic of great importance, because as digitalization advances we will have need of many more security specialists in the years to come. But there is already a perceptible shortage of specialists in this domain. To keep pace with the rising number of malevolent attacks by cyber pirates and develop new, more secure technologies, we need well trained experts familiar with the latest technological developments who are capable of devising creative solutions and novel countermeasures. For this reason, the Fraunhofer Academy has launched a cyber security training program in collaboration with a number of Fraunhofer Institutes and universities.

Prof. Dr. Reimund Neugebauer



"It is certain that nothing is certain, and even that is not certain."

Joachim Ringelnatz, German writer

"Arguing that you don't care about the right to privacy because you have nothing to hide is no different than saying you don't care about free speech because you have nothing to say."

Edward Snowdon, Whistleblower

"Passwords are like underwear – you don't let people see it, you should change it very often, and you shouldn't share it with strangers."

Chris Pirillo, Blogger

"The computer was born to solve problems that didn't exist before."

Bill Gates, Co-Founder of Microsoft

"Those who would give up essential Liberty to purchase a little temporary Safety deserve neither Liberty nor Safety."

Benjamin Franklin

"SOMETIMES PEOPLE JUST AREN'T AWARE OF THE PROBLEM"

Interview with Prof. Claudia Eckert of the Fraunhofer Institute for Applied and Integrated Security AISEC and Prof. Michael Waidner of the Fraunhofer Institute for Secure Information Technology SIT about the challenges, opportunities and initiatives relating to cyber security.

Not long ago, the idea of cloud computing was met with skepticism. Now nobody seems to give it a second thought. Does this mean users have become careless about data security?

Eckert: Many cloud users – especially small to medium-sized enterprises – still have apprehensions, mainly because they are afraid of losing control of their data. Statutory IT regulations are all very well, but what concerns them most is protecting confidential business information and customer data. Hence their heightened awareness of security issues. Providers of cloud services are increasing their efforts to gain more trust by guaranteeing transparency and joining certification programs. The aim of security research is to offer unbiased support to these providers in the form of suitable technological and organizational measures. And, as a rule, a professionally managed cloud infrastructure offers significantly more security for SMEs than a self-managed local solution.

Waidner: We too have noticed that companies are paying close attention to the type of data they store in the cloud, the cloud services they utilize, and the level of security offered by these services. But whatever solution they choose, cloud computing inevitably forms part of any successful company's operations these days. That is why Fraunhofer is developing backup solutions such as OmniCloud, which enable companies to store their data in the cloud safely and at low

Prof. Claudia Eckert

Prof. Michael Waidner

cost. Another of our projects involves developing automated analysis methods for evaluating the security of cloud services. These allow providers to demonstrate that their services comply with legal requirements or the customer's specific demands.

Professor Eckert, your institute specializes in integrated security. What kind of questions do companies ask you to solve?

Eckert: At the moment, the biggest security challenges are in the automotive sector, where the rapid development of autonomous vehicles poses numerous questions. Other key areas of concern are industrial security and networked health services such as personalized medicine and connected medical devices. In these areas of technology, the digital transformation has increased the demand for customized, embedded security solutions. Conventional solutions are rarely suitable for such applications because they aren't scalable, don't permit real-time processing, and are arduous to implement. Companies also have an increasing need for tools and methods with which to develop secure system solutions for applications such as risk assessment, which need to be standardized and deliver reproducible results to allow comparison beyond enterprise boundaries.

Professor Waidner, your institute frequently analyzes threat scenarios and tests security systems. What are the most common security weaknesses?

Waidner: The biggest threat is that of massive automated attacks in which hackers exploit known weak points in order to bring down servers or web applications. The majority of these attacks could be easily prevented if companies protected themselves with firewalls based on industry-standard processes and technologies. But sometimes they are not even aware of the problem, or lack training in the implementation of the necessary solu-

tions, or can't afford the costs involved, especially in the case of SMEs. Targeted attacks by organized criminals specializing in commercial and industrial espionage are another growing danger. To detect and ward off such advanced persistent threats, companies have little option other than to implement the latest generation of security solutions: tools for automated configuration testing and optimization, and management and monitoring tools for detecting even advanced attacks in their corporate IT networks.

Professor Eckert, the High Performance Center for Secure Networked Systems was set up in Munich this year. What are its research priorities?

Eckert: Research at the center will focus mainly on smart sensors, the tactile Internet, data analysis and processing, and integrated security. These will be major topics in the future. Specifically, we want to develop immediately viable solutions for applications such as connected mobility, healthcare, and industry 4.0. This will be our input to the roadmap to a connected world based on the Internet of Things. Through our research, we also want to help create key standards for secure system networking and establish design concepts for secure cyber-physical systems.

Professor Waidner, in Darmstadt you have not one but two competence or high performance centers. What research topics are they working on?

Waidner: At the Center for Research in Security and Privacy (CRISP), created in 2015, more than 450 researchers are looking into ways of systematically evaluating and demonstrably improving the security of complex and heterogeneous IT-based systems. To support their efforts, Fraunhofer has created a new high performance center dedicated to security and data protection in the digital world, giving companies quicker access to the latest research findings in this field. This will enable businesses to integrate security and data protection aspects into their products and applications at an early

stage in the development process. The Fraunhofer center maintains close collaborative ties with local universities and industry. This concentration of facilities makes Darmstadt one of the world's largest research hubs for cyber security.

US companies seem to hold the lead with regard to IT security solutions. In what areas can Germany beat them?

Eckert: I'm sorry, I don't agree. The Americans might offer better consumer solutions and software, but when it comes to embedded software, and more particularly embedded, hardware-based security, Germany holds the lead. "Security made in Germany" is a trusted brand. Many research centers here are top-notch international players. In the future, too, German solutions will play a very significant role in solving the security issues surrounding industry 4.0 and in automotive security. Because in addition to our expertise in application development, we also have the technological and engineering know-how needed to build sustainable and secure solutions. Moreover, national research organizations like Fraunhofer provide German scientists with the ideal instruments for transforming their research into innovative concepts and bringing them to commercial maturity in close collaboration with industry and in accordance with industry's needs.

Waidner: Generally speaking, the U.S. is probably a more fertile ground for security solutions, but German researchers are equally capable of developing competitive solutions. We have excellent universities, and our non-university research institutions are the envy of the world. Take Israel, for example, where last year Fraunhofer SIT started building up a joint project center for cyber security with the Hebrew University of Jerusalem. No research organization that combines leading-edge fundamental research with application-oriented research, as exemplified by Fraunhofer, currently exists in Israel. So even advanced digital societies like Israel have need of German expertise in cyber security.

CYBER SECURITY IN PRODUCTION: SECURE CONNECTIONS

Industry 4.0 involves connecting machines and data – both within one company and beyond company boundaries. Fraunhofer experts are seeking effective ways of protecting manufacturers' proprietary data against hackers.

Up to now, very few production plants were linked to the Internet and thus exposed to cyber attacks. Industry 4.0 changes all this. On the positive side, this open networking approach enables machines to communicate with one another or with the manufacturer via a remote data link. On the negative side, annual losses of more than 22 billion euros were suffered by industry alone due to data theft, espionage and sabotage, according to the 2016 Bitkom survey.

Researchers are busy working on effective solutions to protect connected industrial plants against cyber attacks and espionage. IT security in industry 4.0 (IUNO), a German national reference project, counts 21 partners including three Fraunhofer Institutes, Bosch, Siemens and Volkswagen, all working toward a common goal. "We are developing a toolbox of IT technologies that will enable SMEs to get ready for industry 4.0," says research scientist Dr. Thorsten Henkel from Fraunhofer SIT. It defends against risks including the theft of intellectual property and counterfeiting. If, for example, a company sells the CAD data for a brake disk, the buyer is only allowed to produce a fixed number of brake disks, based on the relevant price agreement. Another challenge is that of ascribing an identity to the machine generating these data – with rights to data protection similar to those granted to humans. But what hap-

pens if the machine is altered through the addition or replacement of component parts? Under what conditions does the machine's identity remain the same, and when not?

Simulating cyber attacks

Attacks on production networks can have drastic consequences, possibly even bringing them down completely. Researchers at Fraunhofer Institute of Optronics, System Technologies and Image Exploitation IOSB have the possibility of using the institute's IT security lab for industrial control systems to simulate potential cyber attacks and, by analyzing the results, develop new defense strategies and appropriate countermeasures. Using the lab's facilities, the researchers can simulate the complex IT infrastructure of an entire factory, including the office network and the networks for planning, monitoring and controlling production.

In addition to the challenges posed by cyber attacks, a recurring question when developing new security solutions is who owns the data. How can companies share information without revealing commercial secrets or losing control over proprietary data? It was for this reason that Fraunhofer launched its initiative to create the Industrial Data Space, a network of trusted data that allows companies to connect their data while retaining sovereignty over it.

IT security for industry 4.0

In a study commissioned by the German Federal Ministry for Economic Affairs and Energy (BMWi), researchers at several Fraunhofer Institutes and various partners investigated the legal, organizational and technical aspects of IT security for industry 4.0. Their proposed recommendations included the introduction of minimum standards of IT security and corresponding legal regulations, the use of digital identities and certified products in digital supply chain networks, and the creation of concepts for an integrated view of safety and security aspects.

http://s.fhg.de/cyber-security

AUTOMOTIVE SECURITY: ON THE MOVE

Autonomous cars, electric mobility, and car2X communication illustrate how digitalization is bringing a new dimension to mobility. It opens up huge opportunities but also unimaginable risks for vehicles and road users. For this reason, these future scenarios will be impossible to implement without adequate cyber security and data protection.

Nowadays, the volume of data circulating in a modern car is higher than in an airplane. Not all of it relates to technical functions: some data is also unwittingly provided by the driver. For as well as recording speed and motion profiles, onboard sensors also record personal data such as seat adjustment settings or gear-changing habits. Manufacturers and service providers can use this type of information to implement a host of new, useful applications. But data protection activists take a more skeptical view because the driver doesn't know what data are being recorded, and has no choice in the matter. Researchers at Fraunhofer SIT, together with partners from science, government and industry, have set out to change this in the SeDaFa project (self-determined data protection in connected vehicles). "What we're aiming for is transparency about what data are actually recorded and giving the driver sovereignty over those data. Everyone should have the right to decide for themselves what data they reveal and to whom," explains Professor Christoph Krauß, Fraunhofer SIT department head and project coordinator. It's not a question of denying all access to data but of respecting certain data protection rules. One of the solutions proposed by the researchers is to aggregate data from a group of vehicles and forward it under a pseudonym or anonymously, so as to mask the identity of the vehicle from which specific data were obtained. "The main focus lies on assessing the risk incurred by the user. This is effec-

tively unmapped territory for which no basic precepts exist. The question we need to ask is how to format the data in order to allow the user to evaluate the risk of communicating it to a third party," says Krauß. This isn't always as easy as it sounds, because a seemingly anodyne speed profile can be overlaid with geographical and topological data, including the location of stop lights, to produce a route profile. The next step is to carry out field studies to find out the best way of making drivers aware of such data protection risks. After that, the researchers intend to develop a demonstrator, which will be similarly tested in field studies.

Making tomorrow's car hack proof

As connectivity grows between vehicle IT systems and the Internet, so too does the risk of hacking attacks. People will not accept autonomous cars, for example, unless the maps they use to navigate are protected against manipulation. Fraunhofer researchers are therefore participating in several EU projects to develop end-to-end, standardized IT security concepts for car2X communication, to ensure authenticity, integrity and confidentiality when sensitive data are exchanged.

Secure e-vehicle charging

Electric cars present another set of security risks. What safeguards can be provided to make sure no-one recharges their battery using someone else's account? Or to prevent route profiles from being compiled on the basis of EV charging behavior? These and other questions concerning secure charging and billing systems are being investigated in the DELTA project by Fraunhofer SIT researchers and partners, including RWE subsidiary innogy. They are developing prototypes for an in-car charging controller and an EV charging point with integrated smart meter. This includes implementing built-in safeguards to protect the charging station itself and the data transmitted between vehicle, charging station and backend systems. In this way, the data remains secure throughout the charging process.

http://s.fhg.de/automotive

SECURITY FOR CRITICAL INFRASTRUCTURES

A cyber attack that paralyzes infrastructures such as energy, water or hospitals would have catastrophic consequences. But it is often particularly difficult for smaller providers to protect their own systems and hence the entire infrastructure adequately. Fraunhofer researchers are developing simplified protection and risk assessment models primarily for this target group.

Without thinking, a user opens an e-mail attachment and now the computer has stopped working – it's infected with a virus. Frustrating enough for the ordinary citizen but devastating if the attack affects critical infrastructures. In the worst case, a country's entire water supply could be cut off, or vital power and telecommunication networks brought down. In view of these potential threats to national security, the German government has given top priority to defending critical infrastructures against cyber attacks. This is totally justified, given that such infrastructures have long since become the target of terrorists of all persuasions.

Even more complicated is that, in the new energy economy, generating plants are not only directly interlinked but also increasingly connected to the Internet. This makes perfect sense in terms of energy policy, but is very risky from the point of view of cyber security and thus demands powerful security solutions. Plant operators are faced with the challenge of regularly updating their IT security systems and preserving network integrity within an infrastructure that is no longer centralized but instead consists of numerous, heterogeneous, regional utility companies -- it is precisely these who have the most difficulty assuring security.

Evaluating security levels

The first step involves identifying security

weaknesses. Which gateways do hackers use? What loopholes need to be closed? The German Federal Office for Information Security (BSI) has designed a self-assessment questionnaire to serve as a checklist for identifying risks. But it is too complex for smaller companies. As part of the MOSAIK project, researchers at the Fraunhofer Institute for Applied and Integrated Security AISEC are therefore attempting to produce a slimmed-down version. "The BSI's version is designed for risk-assessment experts, whereas our simplified version can be used by plant operators," says Dr. Jörn Eichler, head of the Secure Software Engineering department at Fraunhofer AISEC. "We have reformulated the checklist so that expert knowledge of security is no longer required, thus reducing the number of questions. For instance, an employee merely has to enter the information that a telephone system allows data access, and our method automatically assigns a threat level on the basis of previously identified, similar threats. We have also developed a tool that makes the process easy to use."

The scientists are developing a model-based, modular system for this purpose. It provides templates for specific industrial sectors and technologies, which users can adapt to the requirements within their own company.

Possible data protection concepts

Data protection presents the same difficulties as risk assessment. The options are so numerous that it is almost impossible for small companies to choose the one that will be most effective. What concept offers the best protection against the identified threats? Here too, researchers are working on a solution. "Our method supports the use of templates to choose suitable countermeasures," explains Eichler. In the long term, they aim to provide a simulation tool enabling different options to be tried out to determine their effectiveness in the identified threat scenarios without disrupting ongoing operations.

http://s.fhg.de/cyber-security

DIGITAL SERVICES: HOW TO ASSURE SECURITY AND DATA SOVEREIGNTY

Nearly everyone uses search engines and shops online: Round-the-clock digital services simplify our everyday lives, but can we be sure that our data are safe when using these services, and are not being used to steal our assets or identity?

It's all very well being able to look something up on the Internet or browse in online stores, but digital services collect data on the individuals and companies that use them, rarely tell you how these data are analyzed, and often sell the resulting detailed user profiles for a profit. "Data has become the fourth production factor," says Michael Ochs, business area manager at Fraunhofer Institute for Experimental Software Engineering IESE. "Privacy, identity theft, intellectual property rights, and trusted services are major issues that need to be considered by users of digital services."

Be white? Be black?

In many cases, to access certain services, you have to check a box accepting the general terms and conditions of the site. It's an all-or-nothing situation because if you check "yes" to be whitelisted, you have no choice over the way in which your personal data are used, and by whom. On the other hand, if you don't want to reveal your personal data, your only option is to check "no" and be blacklisted (i.e. excluded from this service). While on the one hand legal instruments such as the EU General Data Protection Regulation (GDPR) codify users' rights and increase transparency, companies still need access to data that will enable them to develop innovative business

models and arm themselves against cyberspace pirates.
Technology-based methods such as data-use monitoring and biometric identification could help to bridge the gap between these two universes and create a balance between user benefits and the risks of misuse.

Be gray – and be secure!
Fraunhofer researchers offer a third alternative: Be gray and be secure. Using IND2UCE technology developed by Fraunhofer IESE, users are given the final decision as to whether they wish to share their data, and if so in what form. If access to data is additionally controlled by means of biometric techniques, such as those offered by Fraunhofer Institute for Computer Graphics Research IGD, nothing more stands in the way of the secure use of digital services. The unique aspect of these techniques is that one or more physical characteristics are used to authenticate and identify the user. This is a much safer way of protecting sensitive personal data or a company's intellectual property than the use of passwords alone. Moreover, data-use monitoring provides service users with a simple and direct means of controlling the exploitation of their data by service providers and other third parties.

The first prototype applications of the new technology are already in use. In the financial services sector, for instance, they are being used to protect clients' personal data. And in cloud and hosting services they are being used to prevent data from being stored outside legally permitted geographical areas, and to prevent competitors' applications from being executed on the same virtual machine. Other services enabling users to keep control over their data thanks to the new technology will shortly be launched on the market. The IND2UCE technology received an EARTO (European Association of Research and Technology Organisations) innovation award.

http://s.fhg.de/usage-control

SECURITY FOR EVERYBODY

IT security solutions only work if they are human-centered. Most people don't have the time or patience to read through endless pages of incomprehensible jargon. They prefer to trust their intuition and hope that nothing will go wrong. Professor Matthew Smith at the Fraunhofer Institute for Communication, Information Processing and Ergonomics FKIE is working on solutions to make IT security easier to use.

Professor Smith, how do you intend to simplify IT security systems?
In everyday practice, security technologies are often used incorrectly or simply ignored. That's why security research tends to focus on the technological aspects; when people make mistakes when trying to use the technology it is assumed that the user is at fault. Our concept of "usable security" sees things from the opposite perspective: If the user makes a mistake, it's because the technology is badly designed.

What does this mean in concrete terms?
The first stage involves finding out where the problems lie. To do this, we invite people to join us in the lab, where we can observe how they work with security technologies. What problems do they have as users? At what points do they need help? By eliminating these stumbling blocks, we make the technology less complicated. We also implement users' specific requests. In the final stage, we test the developed solution.

How does this benefit users?
Take, for example, the apps on a smartphone. Some apps can access the user's address book and photos, or pinpoint the device's location, and so on. Users don't usually keep an eye on which types of data a particular app is allowed to access. And if they do try to look up this information, it is presented in such obscure lan-

Prof. Matthew Smith

guage that they soon abandon the attempt. We have developed a system for Android that provides users with examples, for instance we show an actual picture from the phone and say "This app can access your photos like this one and delete them." A study has shown that users of our solution are much more likely to install more privacy friendly apps than a control group without our technology. In other words, these users are able to see more clearly which apps access which types of data, and can act accordingly.

What topics are you researching at the moment?

Whereas research into usable security traditionally focuses on the end user, we turned our attention a while ago to the security experts. After all, they are human too – except that their errors have far more serious consequences than errors made by end users. This approach has been very fruitful. To cite an example: App developers use encrypted communication in their applications to provide protection against hackers. But this protection was found to be inadequate in nearly one out of every five apps that tried to use encryption, allowing hackers to fish for credit card numbers or bank account information. Together with the app developers, we conducted a study to find out where and why errors were being made, and elaborated a suitable solution. The result is a greatly simplified development process in which typical programming errors no longer occur.

When will your technology be available on the market?

Google has now integrated our approach in the Android N update. Even expert studies that focus on malware demonstrate that usability is an incredibly important issue – both for end users and for security specialists. Usable security is a powerful concept because it treats people and technology as equal partners.

CYBER SECURITY TRAINING LAB FOR TOMORROW'S SECURITY

Professionally trained IT security specialists are a rare commodity in Germany. So as not to fall behind in the arms race with cyber criminals, IT teams and managers must constantly hone their skills and improve their expertise in order to stay at least one step ahead. Several Fraunhofer Institutes and universities of applied sciences are now offering a modular, part-time study program to alleviate the unmet demand for training opportunities.

Training and development in the field of IT security is an issue of national interest, given that cyber attacks on critical infrastructures or industrial complexes can result in significant financial losses, the disruption of vital supply networks, or the breakdown of public order. The growing trend toward connectivity and digitalization only accentuates the threat.

There is a huge demand for training in this domain. Already in 2014, 61 percent of the companies that responded to a survey by the German Chambers of Industry and Commerce (IHK) cited expertise in IT security as one of their priorities when recruiting qualified staff. And yet in 2015 only five of the 64 major universities with computer science departments offered degree courses in IT and cyber security. Moreover, according to a study published by Frost & Sullivan, the shortage of trained specialists in the security industry will reach 1.5 million worldwide by 2020.

Collaboration with universities of applied sciences

In response to this problem, Fraunhofer and a select group of universities of applied sciences have developed a modular

concept for cyber security training. The cyber security training lab created for this purpose will receive six million euros per year in funding from the German Federal Ministry of Education and Research (BMBF) during its first years of operation.

This collaborative approach enables the latest theoretical or practical research findings to be immediately incorporated into the teaching program. Course participants will work in modern laboratories equipped with simulation tools allowing real threat scenarios to be tested. They can specialize in the following thematic areas:

- Industrial manufacturing/Industry 4.0
- Critical infrastructures/Use cases for energy and water infrastructures
- High-security and emergency-response facilities
- Internet security and IT forensics
- Software quality/Product certification
- Embedded systems, mobile security and the internet of things

The teaching components are condensed into a compact format requiring only part-time attendance, and the modules can be combined in different ways to match the IT security requirements of various professional functions. The Fraunhofer Academy intends to develop new modules based on demand and provides end-to-end quality management.

Industry supports this initiative, as confirmed by Thomas Tschersich, Senior Vice President Group Security Service at Deutsche Telekom AG: "We particularly appreciate the modular format that concentrates teaching content in short training units, enabling the transfer of knowledge in specific subject areas. This is ideal for part-time study and for specific training in the use of modern tools."

http://www.cybersicherheit.fraunhofer.de

SECURITY AT LARGE

Until now, cyber security researchers tended to focus their attention on island solutions of a manageable size. The Center for Research in Security and Privacy (CRISP) in Darmstadt, funded by the German federal government and the state of Hessen, represents a new departure in that its research focuses on ways of protecting large-scale, real systems such as the internet, industry 4.0 or smart power grids. True to its watchword of "Security at large", the center bundles the expertise of Darmstadt University of Applied Sciences, Darmstadt Technische Universität, the Fraunhofer Institute for Secure Information Technology SIT, and the Fraunhofer Institute for Computer Graphics Research IGD. Together, these researchers are investigating the way components interact, testing composite systems, and developing holistic security solutions.

http://s.fhg.de/CRISP-en

SECURE PAYMENT

The black market in stolen credit card data is flourishing, and fraudsters are constantly inventing new scams. From Trojan horses in card-reading devices to the hacking of online accounts, phishing techniques are rapidly evolving. MINTify rule software helps banks detect credit card fraud and blocks suspicious transactions according to a set of predefined rules. The software is based on algorithms developed by researchers at the Fraunhofer Institute for Intelligent Analysis and Information Systems IAIS in Sankt Augustin in partnership with Paymint AG. Banking systems have to process millions of datasets in a minimum of time. It used to take up to half an hour to validate a transaction. Now, thanks to self-learning algorithms, the software can detect fraudulent activities within minutes and block the suspicious transactions.

http://s.fhg.de/fraud-mining

More information:
http://s.fhg.de/cyber-security

Publisher's details

Fraunhofer-Gesellschaft e.V.
Communications
Hansastraße 27c
80686 Munich
http://s.fhg.de/contact-press

Concept: Mandy Kühn

Editorial content:
Janine van Ackeren, Mandy Kühn,
Tanja Schmutzer

Graphics and Layout:
Larissa Hummel

Photo acknowledgments

Cover, Page 15, 16, 22: Shutterstock
Page 3: Ines Escherich/Fraunhofer
Page 4: Fraunhofer AISEC
Page 7: left: Andreas Heddergott/
TU Muenchen
right: Fraunhofer SIT
Page 8: iStockphoto
Page 11: Sven Doering/Agentur Focus/
Fraunhofer
Page 13: PantherMedia/Cindy Fischer
Page 19: Fraunhofer FKIE
Page 20: Fraunhofer IOSB
Page 21: Matthias Heyde/
Fraunhofer FOKUS