Fraunhofer

RESEARCH NEWS

09 | 2014 ||

1 On the way to a safe and secure Smart Home

A growing number of household operations can be managed via the Internet. Today's "Smart Home" promises efficient building management. But often the systems are not secure and can only be retrofitted at great expense. Scientists are working on a software product that defends against hacker attacks before they reach the building.

2 Ethanol fireplaces: the underestimated risk

Ethanol fireplaces are becoming more and more popular. However, they are not only highly combustible – in the past, severe accents have occurred repeatedly with decorative fireplaces. The devices also pollute the air in the rooms. This has been proven by a recent Fraunhofer study. Wood-burning ovens are also on the testing block.

3 Central biobank for drug research

In developing new drugs it is crucial to work with stem cells, as these allow scientists to study the effects of new active pharmaceutical ingredients. But it has always been difficult to source enough stem cells of the right quality and in the right timeframe. A central biobank is about to remedy the situation.

4 Greater safety and security at Europe's train stations

When a suspicious individual fleas on a bus or by train, then things usually get tough for the police. This is because the security systems of the various transportation companies and security services are typically incompatible. The EU project, Secur-ED, aims at creating remedies and establishing better collaboration within the same city.

5 Simulations for better transparent oxide layers

Touchscreens and solar cells rely on special oxide layers. However, errors in the layers' atomic structure impair not only their transparency, but also their conductivity. Using atomic models, Fraunhofer researchers have found ways of identifying and removing these errors.

6 Fingerprints for freight items

Security is a top priority in air freight logistics but screening procedures can be very time consuming and costly. Fraunhofer researchers intend to boost efficiency with a new approach to digital logistics, without sacrificing the security of air freight operations.

The Fraunhofer-Gesellschaft is the leading organization for applied research in Europe. Its research activities are conducted by 67 Fraunhofer Institutes and research units at over 40 different locations throughout Germany. The Fraunhofer-Gesellschaft employs a staff of around 23,000, who work with an annual research budget totaling 2 billion euros. About 70 percent of this sum is generated through contract research on behalf of industry and publicly funded research projects. Branches in the Americas and Asia serve to promote international cooperation.

Editorial Notes:

RESEARCH NEWS | Frequency: monthly | ISSN 09 48 - 83 83 | Published by Fraunhofer-Gesellschaft | Communications | Hansastraße 27 | 80686 München | Phone +49 89 1205-1333 | presse@zv.fraunhofer.de | Editorial Staff: Beate Koch, Britta Widmann, Tobias Steinhäußer, Janine van Ackeren | Reprints free of charge.We encourage you to favor the online version and newsletter via www.fraunhofer.de/fhg/EN/press This bulletin is also available in German as FORSCHUNG KOMPAKT.

Fraunhofer

On the way to a safe and secure Smart Home

Botnet. A term from the world of computers is gradually tiptoeing its way into the world of building automation. You have to anticipate this kind of attack scenario, according to Dr. Steffen Wendzel of the Fraunhofer Institute for Communications, Information Processing and Ergonomics FKIE in Bonn. The researcher from the "Cyber Defense" department is the expert in hacker methods and, working jointly with Viviane Zwanger and Dr. Michael Meier, meticulously examines them. Attackers infiltrate multiple computers – "bots" (from the word "robots") – without their owners' knowledge, weave the computers together into nets, and misuse them for computer attacks. The researchers studied something that does not yet exist at all today: attacks by Botnets on "Smart Homes" using Internet-linked buildings or building operations. The finding: The threat is absolutely real: Internet-controlled electric roller shutters, HVAC and locking systems could all be used for these kinds of attacks."Our experiments in the laboratory revealed that the typical IT building is not adequately protected against Internet-based attacks. Their network components could be highjacked for use in botnets," Wendzel continues. In the process, the hackers do not have to seek out the PCs as in the past; instead, they look for the components in building automation that link the buildings with the Internet. These are small boxes installed in the buildings that look and work like routers for home computers."However, they are configured quite simply, can only be upgraded with some difficulty, and are loaded with security gaps. The communications protocol that they use is obsolete," explains Wendzel.

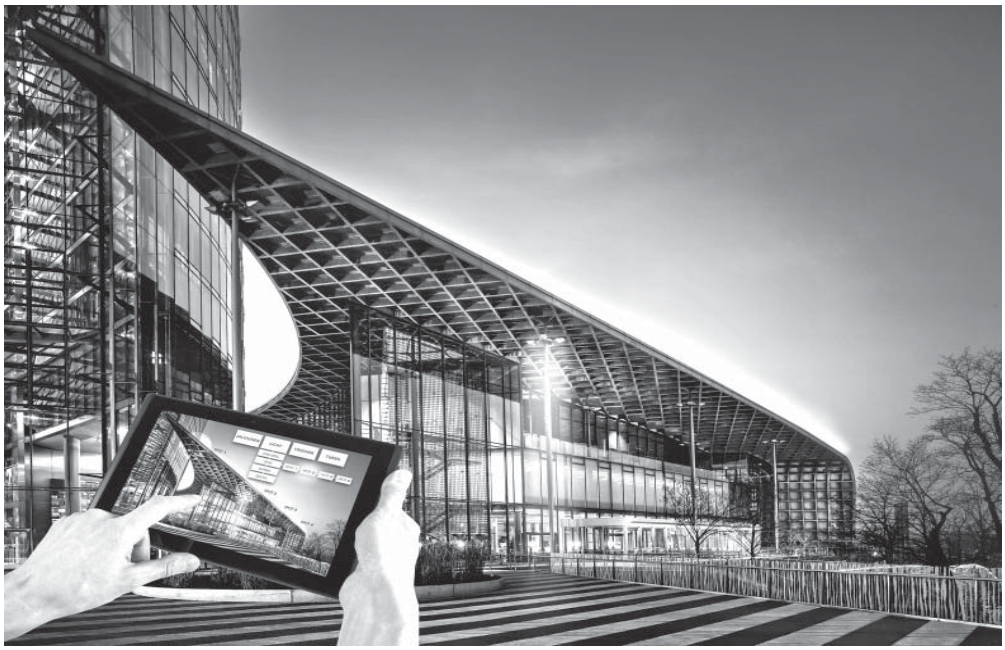
Sentinel software switches between Internet and building IT

To ensure that the heating, lighting, and ventilation of buildings can be controlled via the Internet, it is necessary to install special equipment: This involves mini-computers that measure temperature, light or humidity and are incorporated into networks. "Keeping them up to the latest standards is expensive," Wendzel says. At FKIE, the team has developed security software that can easily switch between Internet and building IT. The technology filters out potential attacks from communications protocols even before they reach the four walls of the actual brick-and-mortar home or office building. No matter what technologies are being used within the building: With this approach, they do not have to be replaced.

The researchers additionally examined the conventional communications standards of building automation, and building upon these, they have developed rules for data traffic. If arriving data do not adhere to these rules, then the communications flow is modified. "The software operates like a firewall with normalization components," explains Wendzel. All the results that are sent on their way to the systems are tested for plausibility by an "analyzer". If the alarm goes off, then the incident is immediately dispatched to the "normalizer." This either blocks the incident in its entirety or modifies it accordingly. The basic research has been concluded successfully. "In the next stage,

we want to make the technology production-ready with an industrial firm. In no later than two years, there should be a product on the market," states Wendzel.

In their analysis of Botnet attacks, the researchers sketched out definitive threat scenarios for smart homes. "From my perspective, the most compelling issue is 'monitoring,'" the cyber defense researcher says. When the attacker hacks into the building operations IT, he or she will learn where the residents or tenants are located and what they are doing, in a worst case scenario. That includes everything, right down to going to the toilet. Intruders, for example, could use this data in order to prepare for a burglary or raid. In this case, the hacker is acting in a passive capacity, simply tapping data. However, he or she could be equally capable of actively invading the systems. Take a contractor from the energy industry, for example. He could profit from more oil or gas sold if the consumption of multiple heating systems is artificially elevated. A recent example demonstrates how real this scenario is: Last year, there was a gap in the security system of a heating system connected to the Internet. Attackers had the ability to shut down or damage heaters. Therefore, security expert Wendzel is currently advising against carelessly linking all building functions in private homes to the Internet.



Building management with a tablet computer: In several modern office buildings, lights, louvers (blinds) and doors can be centrally controlled via the Internet. That brings gains in efficiency – but it holds risks, as well. (© Fraunhofer FKIE) | Picture in color and printing quality: www.fraunhofer.de/press

Fraunhofer Institute for Communication, Information Processing and Ergonomics FKIE | Fraunhoferstraße 20 | 53343 Wachtberg | www.fkie.fraunhofer.de
Contact: Dr. Steffen Wendzel | Phone +49 228 7360-555 | steffen.wendzel@fkie.fraunhofer.de
Press: Herrad Schmidt | Phone +49 228 9435-103 | herrad.schmidt@fkie.fraunhofer.de

Fraunhofer

Ethanol fireplaces: the underestimated risk

Go to the DIY-market in the morning, buy the fireplace, and that evening, enjoy the cozy warmth and homey atmosphere of your new ornamental hearth. The suppliers of ethanol fireplaces are doing a brisk business with the lightweight, easy-to-install ornamental stoves with no chimney. However, caution is warranted when operating these fireplaces, because ethanol is a fuel that, together with the air, forms a highly combustible atmospheric mixture. If ethanol runs out when filling the combustion chambers and it ignites, then the entire room could go up in flames.

On top of this, these decorative items conceal another potential risk: If the manufacturers are to be believed, the devices do not discharge any harmful combustible residues into the ambient atmosphere. A study by the Fraunhofer Institute for Wood Research WKI in Braunschweig indicates the opposite. "These stoves do not feature any guided exhaust system whatsoever, so all combustible products are released directly into the environment. Those are, for example, very fine combustion particles and gaseous compounds like formaldehyde and benzene. Hardly any data exists yet about the effect of ethanol stoves on air quality of interior spaces," explains Dr. Michael Wensing, chemist at WKI. The researcher and his colleagues have examined the level and nature of the released emissions. Likewise, the scientists have also put wood-burning stoves on the same test block.

Tests in the test chamber

The ethanol fireplaces were tested inside a stainless steel, 48 m^3 test chamber. In the process, the engineers took the DIN 4734-1 standard into account, defined the technical minimum standard for ethanol fireplaces, and ventilated the test chamber according to manufacturer instructions. Dr. Wensing's team examined four stoves and a total of eight liquid and gelatinous fuels. "In purely theoretical terms, ethanol and bioethanol completely burns up into carbon dioxide (CO_2) and water. But under real conditions, things turn out differently. On a case-by-case basis, precisely how the course of that incineration runs really depends on the quality of the fuel and other factors – like the type of fuel, or the incineration temperature. As a rule, ethanol does not burn out completely. Rather, the incineration process results in CO_2 – along with poisonous gases (like carbon monoxide, a respiratory toxin), organic compounds (like benzene, a carcinogen), and irritant gases (like nitrogen dioxide and formaldehyde), as well as ultrafine combustion particles," explains Wensing. In the majority of cases, the scientists were able to measure high concentrations of pollutants, and the guideline values were frequently exceeded. For example, all devices exceeded the guideline value for indoor air quality of 0.35 mg/m^3 for nitrogen dioxide; in one case, the result was considerable: 2.7 mg/m^3. With respect to formaldehyde, the stoves likewise failed to stay within the recommended quantity of 0.1 ppm (parts per million). Here, the highest value measured equaled 0.45 ppm. One stove reached a peak concentration of released carbon

dioxide equal to 6,000 ppm – placing it far above the hygienically acceptable threshold value of 1,000 ppm. The decisive factor here is also the fuel consumption rate. This means that the more ethanol which is burned within a certain period, the greater will be the volume of pollutants released. At the same time, ultrafine combustion particles were released. These have a diameter measuring 10,000 less than the thickness of a human hair – and they can penetrate deep into the human lung. "Ornamental stoves with ethanol-based firing are a source for pollutants in indoor air that are hazardous to one's health. In order to guarantee an air quality level that does not pose a risk to human health, we advise avoiding the use of these devices in the interior of apartments. The units should only be operated in large, very well-ventilated spaces, " states Wensing in summary.

The testing of wood-burning stoves – which have always been popular as an additional heat source – resulted in a quite different picture, based on the testing. In Germany, emissions from this heat source into the outside air are subject to strict regulatory mandates. The stresses placed on inhabited interior spaces – for example, from stove doors with faulty seals – had been neglected until now. For that reason, researchers from WKI studied seven stoves in situ in homes under real-life conditions. Here, the focus was placed on volatile organic compounds, fine and ultrafine particles, and combustion particles like carbon dioxide, carbon monoxide, formaldehyde and nitrogen dioxide. The finding: As long as the stove door is closed, the influence on the air quality within the interior space is negligible. Emissions enter the air of the room only when the fire wood is replenished and ignited. At that point, the researchers were able to measure a brief spike in concentrations. "During closed-door operation, no substances of any noteworthy level were released. For instance, the formaldehyde values were harmless," Wensing explains. There were a few exceptions, though: With one of the ovens, the researchers identified very high concentrations of benzene at 72 micrograms/m^3. However, they attribute this rise to the consumption of the paraffinic ignition device. By comparison: When lighting up this oven with paper, the value was only 8 micrograms/m^3." As long as the stove door and the ash pan are well-sealed, there is no need to fear any compromise to human health. The ventilation damper should be positioned in such a manner that the stove draws air well, and any paraffinic ignitors should be dispensed with," says Wensing.

Ethanol fireplaces create an inviting atmosphere. However, they emit a substantial amount of pollutants. (© Fraunhofer WKI/Manuela Lingnau) | Picture in color and printing quality: www.fraunhofer.de/press

Fraunhofer Institute for Wood Research WKI, Wilhelm-Klauditz-Institut | Bienroder Weg 54E | 38108 Braunschweig | www.wki.fraunhofer.de
Contact: Dr. Michael Wensing | Phone +49 531 2155-331 | michael.wensing@wki.fraunhofer.de
Press: Simone Peist | Phone +49 531 2155-208 | simone.peist@wki.fraunhofer.de

Fraunhofer

Central biobank for drug research

Human stem cells help scientists assess how patients are likely to respond to new drugs and to examine how illnesses come about. For a few years now, it has been possible to take tissue samples from adults and use reverse programming to artificially produce stem cells, which have the potential to create any kind of cell found in the human body. Before this discovery, pharmaceutical researchers had to use adult stem cells or primary cells, which have a more limited potential. Another option is to use stem cells harvested from human embryos, but – quite apart from the moral considerations – these cells are available only in limited diversity. The new technique makes it possible for instance to reprogram adult skin or blood cells so that they behave in a similar way to embryonic stem cells and can become any type of cell. "These are known as induced pluripotent stem cells, or iPS cells for short," says Dr. Julia Neubauer from the Fraunhofer Institute for Biomedical Engineering IBMT in St. Ingbert, Germany. "Although an increasing number of regional biobanks have emerged in recent years, none of them fulfills the requirements of the pharmaceutical industry and research institutions. What is needed is a supply of 'ready-to-use' stem cells, which means large numbers of consistently characterized, systematically catalogued cells of suitable quality."

At the beginning of 2014, the IBMT teamed up with 26 industry and research partners to launch a project aimed at establishing a central biobank – the European Bank for induced pluripotent Stem Cells (EBiSC) – to collect iPS cells taken from people suffering from certain specific conditions (http://ebisc.org/). Six months into the project and the first cells are available for use in the development of new drugs. By its three-year mark, it is hoped the project will be in a position to offer over 1000 defined and characterized cell lines comprising a hundred million cells. Such quantities are needed because a single drug screening involves testing several million cells. The main biobank facility is being built in the English city of Cambridge and an identical "twin" will be set up at the IBMT's Sulzbach location in Germany.

Gently freezing cells

The IBMT was brought on board for EBiSC by virtue of the comprehensive expertise it gained through participation in the EU's "Hyperlab" and "CRYSTAL" projects. For EBiSC, IBMT scientists are responsible for freezing the cells and for automating cell cultivation and the biobank itself. In order for stem cells to have a long shelf life, they have to be chilled to temperatures of below 130 degrees Celsius. The scientists have to prepare the cells so they can survive the cold shock of nitrogen gas. The IBMT has, for instance, developed technologies that allow cells to be frozen in an extremely gentle way. "Cells don't respond well to being removed from the surface they are grown on, but that's what people used to have to do in order to freeze them. Our method allows the cells to stay put," explains Neubauer.

Just as with foodstuffs, stem cells depend on an unbroken cold chain to preserve their functionality and shelf life. The scientists store the cells in special containers – or cryotanks – each measuring one by two meters. To remove a particular sample, the scientists have to open the cryotank. The problem is that this exposes all the other samples to warmer ambient air, causing them to begin to thaw out. "It's just like when you go to your refrigerator at home – it's not a good idea to leave the door open too long," says Neubauer. She and her colleagues at the IBMT and industry partner Askion GmbH have together developed a stem cell biobank complete with protective hoods that protect the other samples whenever the cryotank is opened. In addition to maintaining the temperature, the hoods help keep another key shelf-life criterion, humidity, at a constant level.

Flawless freezing is important, but it is just as important to automate the whole process. "That not only guarantees consistency, it's what makes it possible to provide large quantities of cells of the required quality in the first place," says Neubauer. And the scientists' cooling process already boasts a finished technology. In their automated biobank, each cell sample is labelled with barcodes to allow them to be traced. The samples travel along a conveyor belt to the individual cold containers, and a computer monitors the entire freezing and storage process.

Now the scientists are working on automating cell cultivation – or the multiplying of the cells. There are essentially two possible approaches. One is to use robots that translate each manual maneuver into a mechanical one. The other is to use stirred bioreactors that provide free-moving cells with the ideal diet of nutrients and oxygen. Both technologies feature in the IBMT's portfolio. "By the time the project is completed, we'll know which is the better method for what we're trying to do," says Neubauer.

The biobank comprises three cryotanks, equipped with cooled protective hoods, and a transfer station from which the sample containers are transported via a rail system. There is enough space for approximately 60,000 samples. (© Fraunhofer IBMT) | Picture in color and printing quality: www.fraunhofer.de/press

Fraunhofer Institute for Biomedical Engineering IBMT | Ensheimer Straße 48 | 66386 St. Ingbert | www.ibmt.fraunhofer.de
Contact: Dr. Julia Neubauer | Phone +49 6894 980-258 | julia.neubauer@ibmt.fraunhofer.de
Press: Dipl.-Phys. Annette Maurer | Phone +49 6894 980-102 | annette.maurer@ibmt.fraunhofer.de

Fraunhofer

Greater safety and security at Europe's train stations

The train is leaving in a few minutes. But the teeming crowd at the train station finds it anything but easy to get to the right platform quickly. It is confusing and the overcrowded train platforms make travelers aggravated. Even security experts, train employees, police and firefighters work up a sweat. For example: when they are pursuing a wanted person, or if a suspect leaves a suitcase behind unmonitored. The train stations use IT systems that are intended to protect their customers from hazards. Admittedly, there are problems, though: frequently, only one train station or an individual mass transit operator is in danger. Since the use of this IT is not coordinated on a centralized basis, the systems within a city are frequently incompatible with each other. That makes it difficult to exchange information in critical situations and to respond in tandem.

Technologies that "understand" each other

The Secur-ED Project aims to reveal how organizational and information technology-based collaboration within major European cities can be improved – even doing so when facing a variety of threats and differing parameters. The abbreviation stands for Secure Urban Mass Transportation – European Demonstrator. With 39 partners and a budget of EUR 40.2 million, it is one of the largest demonstration projects in European security research. "Since most major cities already have numerous sensors – like video cameras – and control centers for security in local transit, we initially analyzed where the duties lay for those participating partners as well as for the existing IT systems, " says Dr. Wolf Engelbach, Project Director at IAO. "For this purpose, we have developed an interoperability concept: It describes the best possible ways for participants to share their information during crisis situations. Building on that foundation, concrete formats that regulate the exchange can be developed and implemented." To enable security agencies to more effectively share their information and discuss their approaches, the researchers also built a multi-touch table: After extraordinary events, the participants can select data, provide it to the partners and jointly assess the situation.

Test runs in Berlin, Madrid, Milan and Paris

Together with their partners, the researchers connected the new solutions from Secur-ED to integrated solutions – coordinating for the train stations and railroad networks in Berlin, Madrid, Milan and Paris – and tried them out there in test runs. For instance, an "unauthorized party" slipped into a railroad storage depot in Milan, which the staff at the "control center" was able to detect with the aid of a heat-sensitive camera and a camera with a zoom-lens. In another scenario, a bus driver felt one passenger was "suspicious" and reported this to Central. Although the passenger got out at the train station, the employee at the control center kept an eye on him – thanks to a new software product. All they had to do was mark the suspicious individual on the camera image. The software then automatically calculated where the suspect might have

moved and of the total 300 cameras, recommended to the employee those cameras that last tracked that individual.

When conducting a manhunt for specific individuals, the police will soon be able to count on the project's findings, as well: For example, the researchers in Madrid transmitted an image of the individual being sought via LTE – the cellular network – to the city's busses. Cameras in the busses compared the faces of boarding passengers with that of the target individual. If the face was a match, the system dispatched an automatic message to the bus driver and the control center.

Despite the sheer number of these exercises, the project partners were unable to run through all the developments in all their variations. Therefore, the researchers at IAO also developed recommendations as to how various scenarios could subsequently be adapted. These include agent-based simulations and calculations for gas dispersion in order to plan evacuations as well as to place cameras and sensors.

The closing conference of Secur-ED (www.secur-ed.eu) takes place on September 17 in Brussels. In addition, the project will be presented at Future Security 2014, the security research conference in Berlin, from September 16 to 18 (www.future-security2014.de).

The EU research project, Secur-ED, aims to achieve greater security at Europe's train stations. Here, fire department staff can be seen on a test run in Madrid. (© Secur-ED) | Picture in color and printing quality: www.fraunhofer.de/press

Fraunhofer Institute for Industrial Engineering IAO | Nobelstr. 12 | 70569 Stuttgart | www.iao.fraunhofer.de
Contact: Dr. Wolf Engelbach | Phone +49 711 970-2128 | wolf.engelbach@iao.fraunhofer.de
Press: Juliane Segedi | Phone +49 711 970-2124 | juliane.segedi@iao.fraunhofer.de

Fraunhofer

Simulations for better transparent oxide layers

Smartphones, tablet computers, and ticket machines are just some of the many devices nowadays that are touchscreen-operated. These screens are based on special oxide layers that are transparent and conduct electricity. The technical term is TCO (transparent conducting oxide) layers. TCOs are also used on solar cells and in heated windows. So that the technology keeps pace with new products and applications, manufacturers are constantly improving the layers, making them better conductors of electricity and increasing their transparency – after all, when used in tablet computer or smartphone displays, users need to be able to see the content on the screen clearly through the layers. Any additional sheen caused by the oxide would be a problem. The same principle applies for solar cells: rather than impeding sunlight, the oxide layers must allow it to pass unobstructed into the cell. Accordingly, transparency and conductivity are the key elements that the developers of new oxide layers must consider – but the manufacturing temperature and the plasticity of the layers are also important.

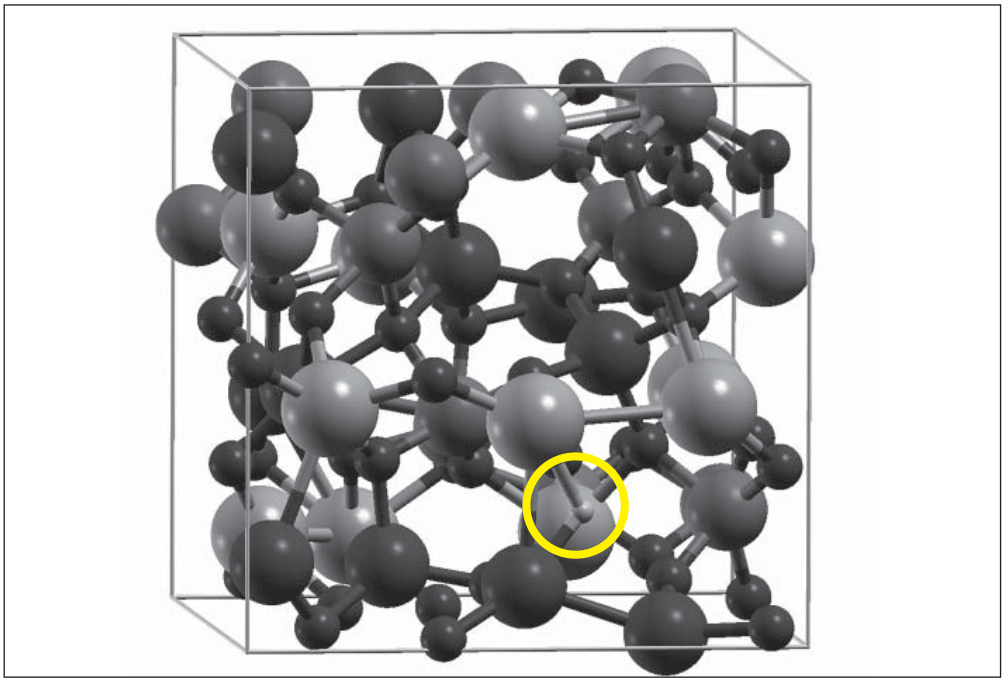
Realistic simulation of atomic structure

Researchers at the Fraunhofer Institute for Mechanics of Materials IWM in Freiburg help manufacturers to optimize oxide layers. "We've developed a practical and effective method for simulating the properties of TCO layers," says IWM scientist Dr. Wolfgang Körner. Most impressive of all is the fact that the scientists' simulations of the layers' atomic structure are highly realistic and take into account all possible atomic errors – irrespective of whether the layers are disordered, amorphous structures or crystalline, highly ordered ones. On the basis of these simulations, the scientists then investigate how well the electrons can move in the layer, in other words how well the oxide conducts electrical current. "We can specifically track how a layer's density of states changes when we change its atomic structure," explains Körner. The researchers can also establish whether light is absorbed or passes through the layer unobstructed, making it appear transparent. "Because we do the trial-and-error material tests on a computer, we can calculate the properties possessed by the respective material composition of the TCO being studied much faster and more cost-effectively than by traditional means," says Körner. Through his projects, Körner is deepening our understanding of how the different properties of the oxide layers arise. This understanding is helping his industrial partners to improve their production and to obtain specific oxide layer properties.

The researchers have already managed to find the principal defects that occur in these layers. It is simply not possible to manufacture the structures with absolutely zero errors. As much as manufacturers want them to consist only of certain defined atoms such as zinc, tin, and oxygen, other atoms – hydrogen is a common culprit – have a habit of crashing the party, changing the layer's conductivity and transparency. But what defects in atomic structure actually impair transparency? And how can we remove these defects to make the oxides more transparent? One of the researchers'

findings was that the transparency of certain oxides is improved by heating them once to a suitably high temperature or by heating them up in an oxygen-rich environment.

A second approach sees the scientists tackle the problem from the other end: they add various specifically defined atoms into the structure and simulate the effects this has on a layer's properties. The goal here is to further boost conductivity and transparency by means of suitable "impurities" and to be able to design a material by computer in this way.



Detail from a model of an amorphous oxide layer into which hydrogen atoms have been introduced in a targeted process. The tiny encircled sphere on the bottom right is hydrogen; oxygen is represented by the small spheres; the big spheres stand for indium, tin, and gallium.
(© Fraunhofer IWM) | Picture in color and printing quality: www.fraunhofer.de/press

Fraunhofer Institute for Mechanics of Materials IWM | Wöhlerstraße 11 | 79108 Freiburg | www.iwm.fraunhofer.de
Contact: Dr. Wolfgang Körner | Phone +49 761 5142-374 | wolfgang.koerner@iwm.fraunhofer.de
Press: Katharina Hien | Phone +49 761 5142-154 | katharina.hien@iwm.fraunhofer.de

Fraunhofer

Fingerprints for freight items

Thousands of freight items are shipped by plane every day, around seventy percent of them in airliners. Stringent controls are supposed to prevent hazardous substances such as explosives from being smuggled on board. Screening procedures, such as x-ray scanning of freight, are time consuming and costly and have to be repeated in the event of suspicious circumstances. Easily verifiable features that verify that a freight item is "secure" have been lacking until now.

Researchers at the Fraunhofer Institute for Factory Operation and Automation IFF in Magdeburg are working with development partners and users such as Panalpina and Lufthansa Cargo in the joint project ESecLog to resolve the dilemma between security and efficiency: Using simple screening procedures, they aggregate features such as 3D contours or RFID identifiers into one central shipment profile for every freight item. "The trick is that we document and aggregate these features into one complete digital image. Thus, every freight item has one digital fingerprint. This delivers accurate infor´-mation of freight's security status throughout the entire transport chain across operations and at any time," explains Olaf Poenicke, project manager at the Fraunhofer IFF.

Safety Wire Prevents Subsequent Tampering

The partners are working, for instance, on a marker that can be used to verify whether a freight item has already been x-rayed – something that has not been traceable. The researchers are additionally developing an RFID seal in order to detect subsequent tampering with a shipment. To do so, they affix a transponder on a package's seal with an ultrafine safety wire. If it is opened, the wire breaks. The shipment continues to be identifiable but the screener is additionally notified that the wire has been damaged. "This technology makes it possible to even inspect entire pallets. If one of the freight items has a broken wire, the shipment concerned can be identified precisely by its ID," according to Poenicke. A pallet's contour can additionally be captured by means of a 3D scan. The pallet's contour changes if a package is subsequently placed on it.

All of this information is aggregated into a kind of shipping record. Screeners can view this documentation in the central fingerprint information system as a timeline on a tablet. If necessary, they can retrieve additional information on individual stations and view all of the x-ray scans once again. This system will drastically reduce the work required for reinspections. Until now, every freight item has to be individually reinspected or even opened whenever there is suspicion of tampering. Poenicke explains what might happen in the worst case: "Deliveries are often made overland. When the cargo is already considered to be secure, the truck is sealed before shipment. If someone at the airport determines that the seal has been broken, then the entire contents have to be reinspected." ESecLog systems would make it possible in such a case to check quickly whether individual packages have been tampered with.

It will be a while, though, until the system is put to use: Now that the consortium has designed the individual systems, the technologies are in the development stage and should be operational by the end of the year. A test environment is supposed to be built in the coming year to optimize the interaction of the systems. The researchers from the Fraunhofer IFF will be presenting this project at the International Supply Chain Conference in Berlin from October 22 to 24. ESecLog is being funded by the Federal Ministry of Education and Research (BMBF).

Air freight being loaded. Researchers at the Fraunhofer IFF are working with other partners on a digital fingerprint for security-sensitive air freight in the project ESecLog. This is intended to make tampering with shipments easily detectable in the future. (© Fraunhofer Fraunhofer IFF/Anna Mahler) | Picture in color and printing quality: www.fraunhofer.de/press

Fraunhofer Institute for Factory Operation and Automation IFF | Sandtorstraße 32 | 39106 Magdeburg | www.iff.fraunhofer.de
Contact: Olaf Poenicke | Phone 49 391 4090-337| olaf.poenicke@iff.fraunhofer.de
Press: Anna-Kristina Mahler | Phone +49 391 4090-446 | anna-kristina.mahler@iff.fraunhofer.de