Fraunhofer
SIT

FRAUNHOFER INSTITUTE FOR SECURE INFORMATION TECHNOLOGY SIT

A PROFILE OF FRAUNHOFER SIT

PREFACE

The market often does not offer what companies and their staff need. The reason is the rapid pace of IT development in recent years, which has brought on many challenges for the companies – especially when it comes to IT security. The reasons are numerous: The triumph of smartphones brought companies new flexibility, but also the associated IT security risks. At the same time, cloud computing caused a revolution of enterprise IT without answering any questions about compliance and privacy. However, attackers do not need to pay heed to such aspects. They are equipped better and better and execute more and more targeted attacks on companies to steal their ideas or harm them otherwise.

The leaders of many companies are looking for ways to take advantage of the technology, to limit associated risks and to comply with the legal framework. At the same time, IT managers are looking for solutions to meet the economic demands as well as their own safety regulations. Our experience has shown that the earlier all involved parties deal with the challenges in IT security and privacy, the more successful they can respond to trends.

Fraunhofer SIT offers its partners an important know-how advantage, which is immediately available. We concern ourselves today with the future standards that are driven by cloud computing. We consider smart devices today as a mobile interface to the cloud. At the same time we offer professional project management and fast response times as a part of contract research. For our partners, this means time and cost savings and at the same time results of highest quality. This booklet provides an overview of our competences, developments and activities. If you cannot find your IT security solution in here, please send us an email – maybe we are already working on it.

Sincerely Michael W (Prof. Michael Waidner)

CONTENTS

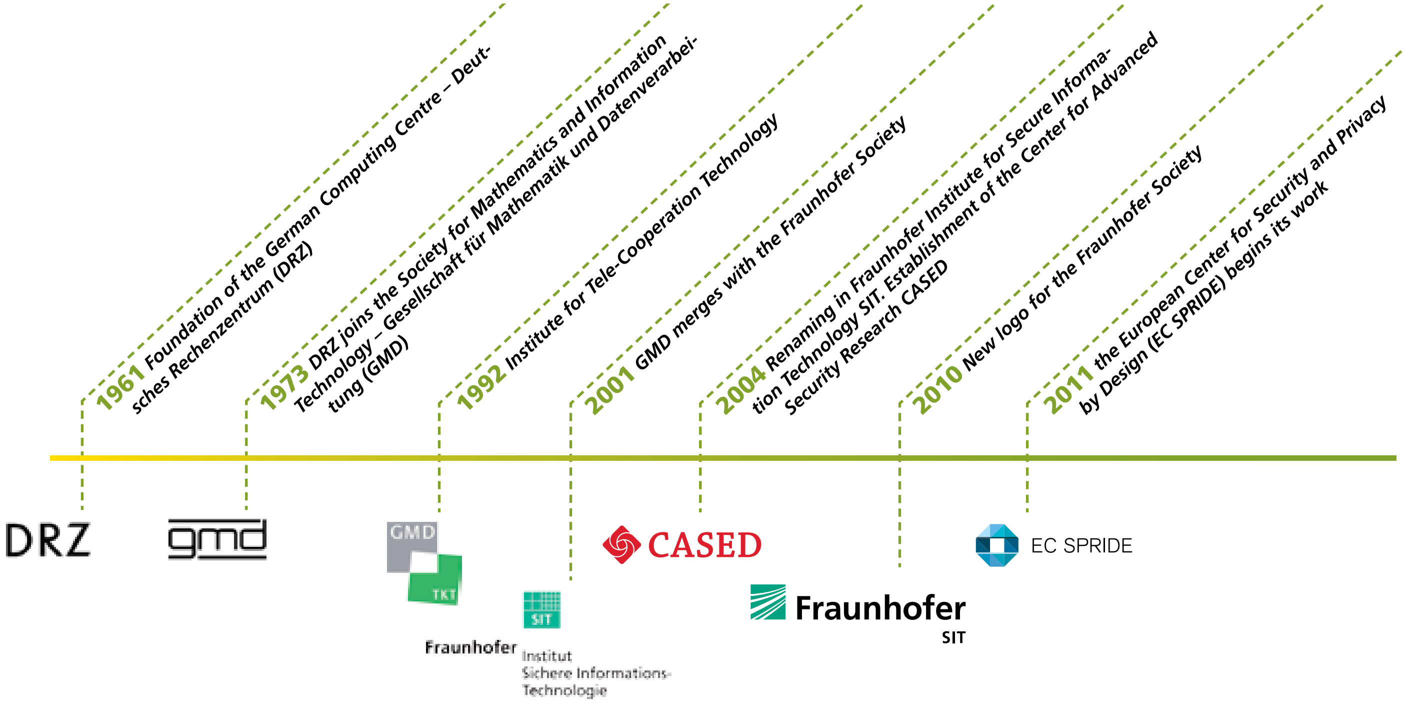
PROFIL

FIELDS OF EXPERTISE

A PROFILE OF FRAUNHOFER SIT

The Fraunhofer Institute for Secure Information Technology is one of the oldest and most respected research institutions for IT security in the world. More than165 employees support business and government in securing data, services, infrastructure and terminals. Fraunhofer SIT conducts applied research with the aim of bringing new technology to the market so that its potential can be used safely and completely. Together with its partners, the institute works on new methods and procedures, creates prototypes, developes customized IT solutions and tests existing products and systems.

A SHORT HISTORY OF FRAUNHOFER SIT



1961 Foundation of the German Computing Centre – Deutsches Rechenzentrum (DRZ)

1973 DRZ joins the Society for Mathematics and Information Technology – Gesellschaft für Mathematik und Datenverarbeitung (GMD)

1992 Institute for Tele-Cooperation Technology

2001 GMD merges with the Fraunhofer Society

2004 Renaming in Fraunhofer Institute for Secure Information Technology SIT. Establishment of the Center for Advanced Security Research CASED

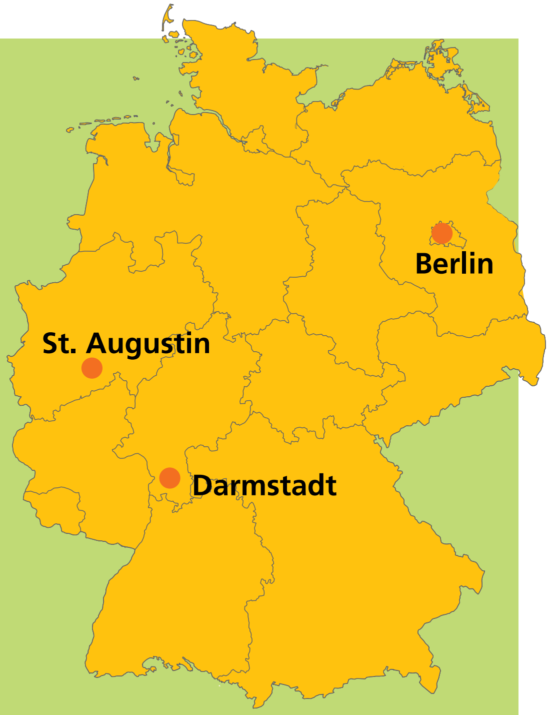
2010 New logo for the Fraunhofer Society

2011 the European Center for Security and Privacy by Design (EC SPRIDE) begins its work

KEY FACTS

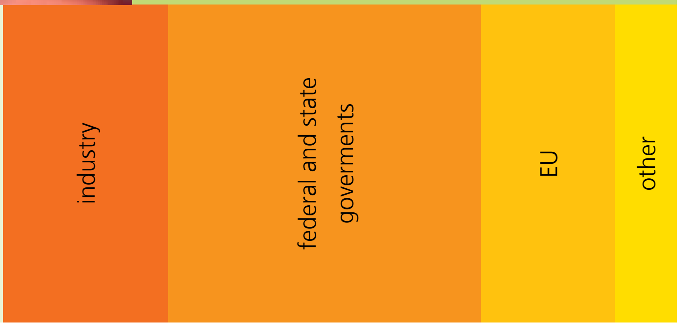
2 chairs at the Technical University Darmstadt

167 employees



3 locations: Darmstadt, Birlinghoven, Berlin

total revenue 2012: **6.7** million euro
industrial: 1.5 million euro
federal and state governments: 3.4 million euro
EU: 1.3 million euro
other: 0.5 million euro



IT SECURITY MADE IN DARMSTADT

CASED

CENTER FOR ADVANCED SECURITY RESEARCH DARMSTADT

Within the past ten years, Darmstadt developed a versatile research ecosystem with IT security focuses at Technical University Darmstadt, Fraunhofer Institute for Secure Information Technology (SIT) and Darmstadt University of Applied Sciences. Since July 2008, the three organizations bundle their competencies in the Center for Advanced Security Research Darmstadt (CASED). Today, more than 200 scientists are doing research on IT security. 16 professors specialize in different topics of IT security; altogether 28 professors of natural sciences, engineering sciences, economics and humanities are involved in CASED projects. This variety is unique in Europe.

Competence Center For
Applied Security Technology
CAST

COMPETENCE CENTER FOR APPLIED SECURITY TECHNOLOGY

CAST e. V. offers a variety of services in the field of secure modern information technology and is a contact for all questions regarding IT security. Its network of competencies imparts knowledge of IT security technology on all educational levels – from supporting specialization in IT security at the TU Darmstadt to career-accompanying education. Through informational seminars, consultation, workshops and tutorials, CAST supports users when choosing the right security technology. The goal of CAST e. V. is to provide and develop the necessary competencies for the growing importance of IT security in all branches of business and public administration. Members of CAST e. V. are institutions like the Federal Office for Information Security (BSI) or the Bundeskriminalamt (Federal Criminal Police Office) as well as several Fraunhofer Institutes and companies like SAP or Software AG.

EC SPRIDE

THINKING ABOUT SECURITY AS EARLY AS THE DESIGN PHASE

The »European Center for Security and Privacy by Design« (EC SPRIDE) researches how IT developers can optimally secure software and IT systems from the very beginning – i. e. »by Design« – and throughout the entire lifecycle. The results are of relevance for pretty much every growth market: from the software industry, to the automobile and industrial engineering sectors, to utility and healthcare companies.

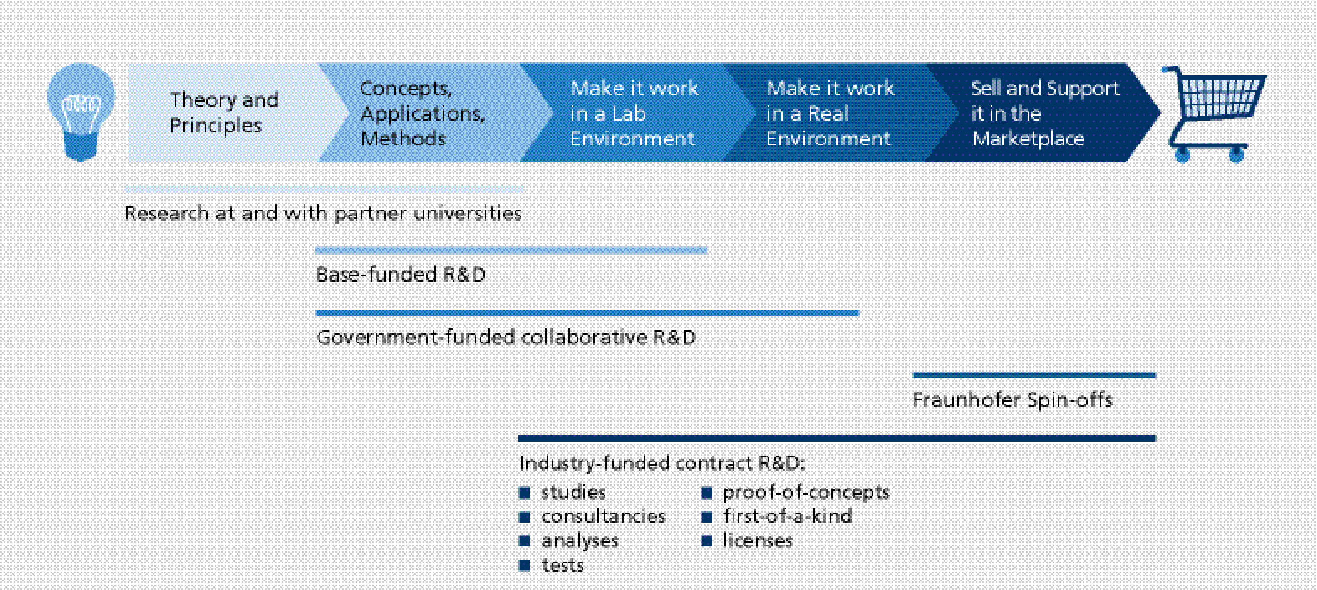
However, there are very few standards, processes and methods, which IT developers can use in order to be able to take the IT security requirements of their software into consideration from a very early stage. As a result of this, IT systems are generally not checked and made safe until after the design stage has been completed, which, in turn, results in unnecessary costs for both the manufacturers and the users. EC SPRIDE wants to close this »gap« with the assistance of new findings, tools and flexible procedures.

Software-Cluster

NEW SERVICES AND APPLICATIONS WITH EMERGENT SOFTWARE

The Software-Cluster covers a wide area in the southwest of Germany, and includes the key software development centers in Darmstadt, Kaiserslautern, Karlsruhe, Saarbrücken and Walldorf. The cluster region comprises four different states (Hesse, Baden-Württemberg, Rhineland-Palatinate and Saarland) – for corporate networks do not stop at political borders. In each of the four sub-regions in itself already exist significant clusters in IT and software with changing topics. The unifying element of the overlapping cluster region is the expertise in software, specifically enterprise software. With good reason, the cluster region is known as the cradle of enterprise software. In the area of the cluster, innovative companies and leading computer science faculties as well as research institutions are concentrated and make the region the »Silicon Valley of Europe«.

FOCUS ON APPLIED R&D



Theory and Principles

Concepts, Applications, Methods

Make it work in a Lab Environment

Make it work in a Real Environment

Sell and Support it in the Marketplace

Research at and with partner universities

Base-funded R&D

Government-funded collaborative R&D

Fraunhofer Spin-offs

Industry-funded contract R&D:

- studies
- consultancies
- analyses
- tests
- proof-of-concepts
- first-of-a-kind
- licenses

Fraunhofer covers all ranges in applied research and development: From research cooperations with universities over partnerships and projects with government and industry to the foundation of spin-off enterprises.

FORMS OF COOPERATION

WHAT WE OFFER:

Consulting: Risk analyses, evaluation of technologies and safety concepts, feasibility studies

Software and hardware security tests: Vulnerability analyses of prototypes, products and applications, technical pre-auditing, penetration tests, and system and application analyses

Development of prototypical solutions: Design and implementation of applications, development studies, integration and adaptation of systems and technologies

Development and optimization of secure electronic business processes and services: Drafting of IT architectures and creation of operating and IT security concepts

Licensing of solutions and security tools: Digital watermarking for video, audio, photos and ebooks, iMobileSitter – mobile password management, BizzTrust – solution for secure use of smartphones in enterprises, Key2Share – access management with NFC, OmniCloud – secure data backup in the cloud

Training/knowledge transfer: Concepts and teaching media for introducing IT security to companies and agencies. The institute conducts training courses and certification testing for the TeleTrusT Information Security Professional (TISP).

WAYS TO COOPERATE WITH US:

One-off contracts: We support you in pursuing your goal. A discussion with Fraunhofer identifies possible solutions and clarifies the form the partnership could take. We provide professional project management and quality results.

Framework contracts: Together with you we will develop strategies and project outlines in an answer to different problems and questions, or if a project position needs to be repeated.

Large-scale projects with multiple partners: Some challenges are so complex that they require multiple partners to develop a solution. Clients in this situation have access to the full range of Fraunhofer Institutes as well as external partners.

Strategic partnerships: Fraunhofer is determined to foster promising new technologies. Pre-competitive research which starts off without any ties to specific development contracts often results in long-term partnerships with companies.

Innovation clusters: The goal of a cluster is to bring together competent partners from within a region to solve challenging tasks. Clusters incorporate industry and universities, as well as other locally-based non-academic research institutions.

REFERENCES

PARTNER

Alcatel·Lucent

BAköV

BlackBerry

BMW GROUP

Bundesamt
für Sicherheit in der
Informationstechnik

BUNDESÄRZTEKAMMER

Bundesministerium
für Wirtschaft
und Technologie

Deutsche Post

DFS Deutsche Flugsicherung

Freudenberg

FUJITSU

hp

IHK Darmstadt
Rhein Main Neckar

infineon

Lufthansa

real,-

SIEMENS

software AG

T · ·

vodafone

COMPILATION OF IT SECURITY ASPECTS FOR MOBILE DEVICES

Lufthansa

Lufthansa AG plans to optimize the currently paper-based processes in the aircraft cabin. For this Lufthansa intends to provide the cabin crews with iPads as new working equipment. These multi-purpose devices should also be allowed for private use. Since in the official use of the devices, personal data of employees and customers are being processed, Lufthansa AG specified extensive requirements to protect the data. The most important requirement is the confidential treatment by strictly separating business and private use, and enforcing a safe configuration. For this application, Fraunhofer SIT has compiled a catalog of IT security aspects for iOS devices to be taken care of. It has developed specific measures for the implementation and configuration as well as organizational processes by which the security requirements can be met.

SECURITY ANALYSIS FOR IOS MOBILE DEVICE MANAGEMENT

DATEV

Datev eG offers its members and their clients a connection of their local network to a common centralized security infrastructure under the product DATEVnet. Within this security concept, the secure connection of tele-workstations to the court office, as well as the interlinking of commercial units, and the connection of smart phones and tablets with iOS play an important role. Together with Datev, Fraunhofer SIT has realised several projects in which the security of mobile devices against external and internal attacks was tested. To simulate these attacks, Fraunhofer SIT used reverse engineering techniques. The aim was to reveal possible weaknesses and threats of the iOS operating system and the mobile device management strategy.

AWARENESS FOR EMPLOYEES

Realizing that the personal factor is one of the severest vulnerabilities for IT security, real,– -group implemented an IT security initiative with the employees in the focus.
real,– -group intends to revise their security policies to adjust the presentation to the needs of the personnel and encourage the employees to a security positive behavior. The most important part of the IT security initiative is an awareness campaign addressing the employees in all countries and in all positions and job roles. Fraunhofer SIT supports the ambitious tasks of this security initiative. The institute's scientists evaluate the security policies by reviewing the comprehensibility of the texts as well as the scope of the topics and devise concepts for the international awareness campaign. They accompany real,– in implementing, monitoring and evaluating the measures.

COLLABORATION IN SECURE SOFTWARE ENGINEERING

Software AG collaborates with Fraunhofer SIT to optimize its secure software engineering for enterprise middleware products. Consistently delivering secure software requires tools, techniques, processes, and metrics that a vendor can apply without disrupting agile development processes. Together, Fraunhofer SIT and Software AG develop practical approaches to risk assessment, threat modeling, security design, and other aspects of secure software engineering. The result is a toolbox for secure software that fits the specific needs of Software AG and its webMethods product line.

SYSTEM AUDITING AND SUPPORT

DFS Deutsche Flugsicherung

On behalf of DFS (Deutsche Flugsicherung), Fraunhofer SIT has conducted a system audit of the multi-site building automation management level. Due to the enormous number of properties to be monitored, DFS was forced early on to increase the efficiency in the field of classical facility management. The large number of cross-sectional issues made system support a challenge: wide-area networks, server virtualization, distributed intelligence, centralized monitoring, redundancy at all levels. Fraunhofer SIT conducted a vulnerability assessment and made recommendations for improvements. Data was obtained and analyzed both in stress and in control mode.

DEVELOPMENT OF THE WEBINAR: »IT-GRUNDSCHUTZ«

Bundesamt
für Sicherheit in der
Informationstechnik

The German Federal Office for Information Security (BSI) provides with its »IT-Grundschutz« a method for planning and reviewing information security in private and public institutions. The introductory webinar »IT-Grundschutz« that BSI is offering free of charge on its website has been developed by Fraunhofer SIT on BSI's behalf. The course teaches how businesses and administrative bodies can protect their information technology. The webinar is complemented by other online courses, also developed by Fraunhofer SIT: The webinar GSTOOL introduces the application of GSTOOLs, BSI's tool for implementing IT-Grundschutz; the webinar emergency management explains the application of the BSI standards 100-4: emergency management.

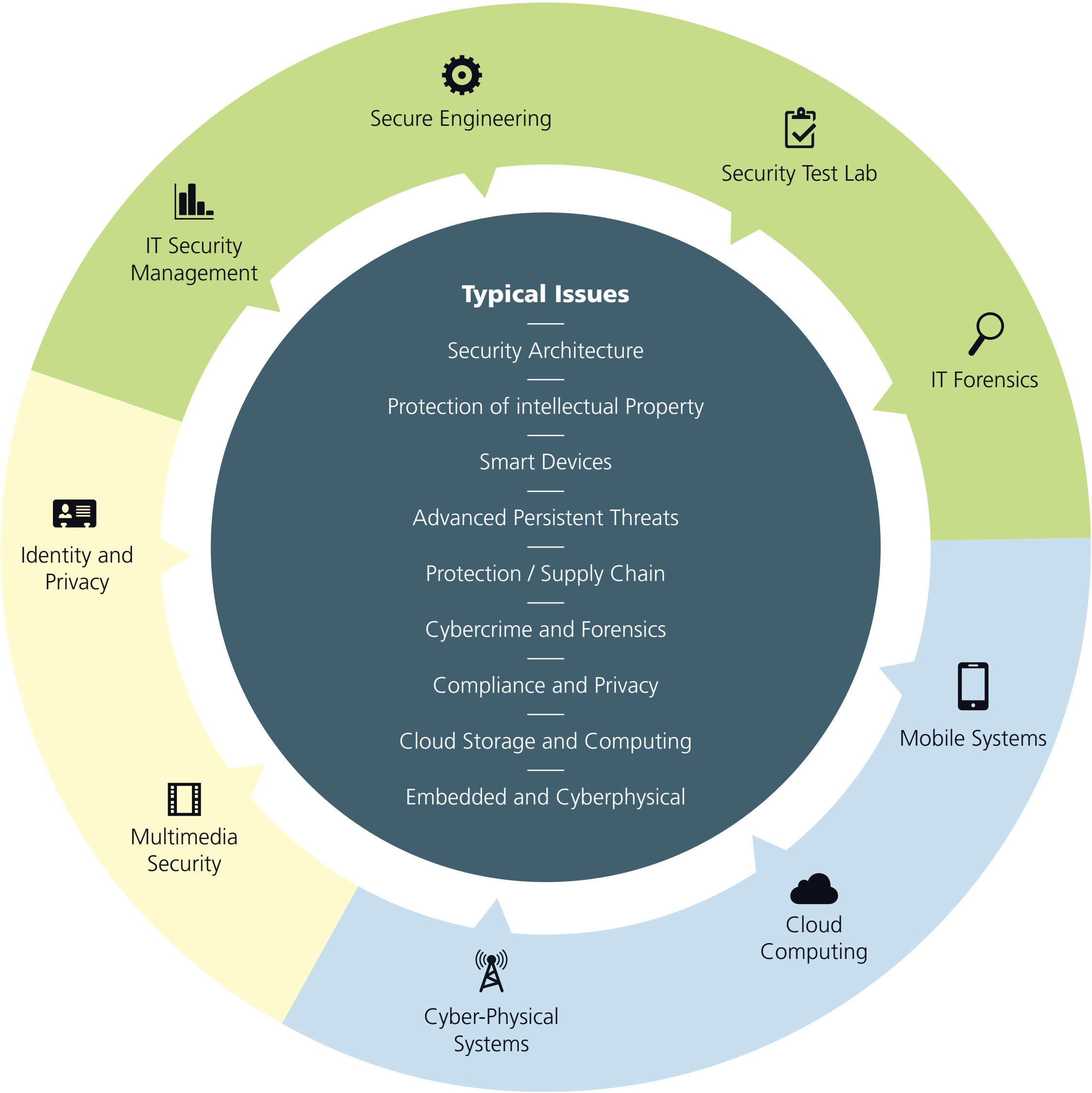
SECURITY ANALYSIS OF BLACKBERRY ENTERPRISE SOLUTION

RIM has a longstanding reputation in developing wireless solutions with best-in-class security and working with world-class organizations. In support of RIM‹s commitment to innovation and continuous improvement, RIM commissioned Fraunhofer Institute SIT to conduct a rigorous security analysis of the BlackBerry Enterprise Solution. The technical expertise and professionalism of the SIT project team was impressive and evident in the quality of their work and the constructiveness of their cooperation.

TRAINING FOR IT SECURITY OFFICERS

To support the safety management of the German government, the Federal Academy of Public Administration (BAköV) and the Federal Office for Information Security (BSI) have been offering for several years a course to train IT security officers in the federal government. The course is composed of a basic training, which includes a wide range of topics related to information security and is completed with a certificate, and a follow-up course to deepen selected topics. The design and development of this modular designed training and the related materials (manual, tests) have been and will also in the future be supported by Fraunhofer SIT.

COMPETENCES



Typical Issues

Security Architecture

Protection of intellectual Property

Smart Devices

Advanced Persistent Threats

Protection / Supply Chain

Cybercrime and Forensics

Compliance and Privacy

Cloud Storage and Computing

Embedded and Cyberphysical

CYBERSECURITY ANALYTICS AND DEFENCES

Modern societies continually face emerging threats in the cyber space. Despite tremendous efforts to secure the cyber space, most defences are not widely deployed, and the existing countermeasures are often circumvented. In contrast, the extent and sophistication of the attacks are on a constant rise. The attacks target critical infrastructure, cyber physical systems, financial organisations, email and web services, cloud platforms and data centers, users and the Internet infrastructure. The attacks deplete resources via denial of service, disrupt the functionality and operation of systems and enable the perpetrators to intercept the communication, e.g., for surveillance, censorship, malware distribution, credentials theft.

Fraunhofer SIT is focused on fortifying the foundations of the Internet, and on developing easy to deploy defences, ensuring security and availability of the Internet. To that end, we study vulnerabilities in the standards and in the design of the deployed systems and services in the Internet, we research challenges and obstacles towards adoption of cryptographic schemes for defences of systems and networks and study incorrect deployments of cryptography. In particular:

- Defences against Denial of Service (DoS) attacks: DoS attacks pose a critical threat to Internet stability, and are used as a tool for censorship, for eliminating competition, or for cyberwarfare between nationstates or groups. We design and develop easy to deploy and effective defences preventing DoS attacks.
- Detection of malware and advance persistent threats (APTs): a large fraction of the Internet computers is infected with malware (malicious software). Attackers can then exfiltrate sensitive users' data (such as credentials, passwords or credit card numbers), perform eavesdropping on the communication, or can exploit compromised computers in DoS campaigns. We develop network based malware detection techniques.
- Design and adoption of cryptographic schemes: integration of cryptography into Internet systems introduces multiple challenges and obstacles. In particular, design and adoption of defences requires understanding of the architecture of the Internet infrastructure. Furthermore, adoption of cryptography may also result in reduced security, when deployed incorrectly. We use Internet measurements for inferring the topology and configuration of the Internet networks and services, and adjust the cryptographic schemes to match and interoperate with the existing systems.
- Privacy and anonymity: privacy of the data and communication is essential for economy, autonomy of the Internet and safety. Unfortunately, recent revelations pertaining to surveillance by the nation-states and publicised attacks show that privacy is a far dream. We design privacy preserving communication protocols, ensuring efficiency and quality of service.

Dr. Haya Shulman
haya.shulman@sit.fraunhofer.de

RESEARCH TOPICS

Internet infrastructure: security of the fundamental building blocks, such as routing and naming systems, comprising the foundations of the Internet, is critical to the security and stability of the Internet clients and services. Unfortunately, the Internet infrastructure, as well as the services that it provides, is subject to numerous attacks. We research vulnerabilities in the Internet infrastructure, such as those allowing to intercept the communication, and design countermeasures preventing the attacks.

Cloud platforms: cloud offers a convenient platform providing hosting and management of services for customers. However, coresidence and sharing of the platform between multiple customers (often with conflicting interests), introduces new security challenges. We research security aspects, such as isolation on a network layer, as well as infrastructure guarantees provided by the cloud platform.

Web: a majority of the attacks against end users exploit vulnerabilities in the web as well as in incorrect or vulnerable deployment of cryptographic mechanisms. Securing the web is critical to enabling clients to perform online transactions and communications, and important for guaranteeing profit of the service providers. We evaluate security of browsers, and communication channel.

Voice over IP and mobile communication: telephony is increasingly operated over IP networks. Intercepting phone communication is detrimental to privacy and security of individuals, organisations and governments. We investigate vulnerabilities exposing to attacks and design countermeasures preventing them.

Industrie 4.0 and cyber physical systems: elements involved in production of Industrie 4.0 are interconnected between themselves and the Internet. Cyber physical system monitor physical processes, sensors and devices. Within this context we also study industrial control systems, in particular, SCADA. Securing the communication is substantial to preventing catastrophic events and incidents. We research fault tolerance and evaluate vulnerabilities pertaining to communication between the devices on the grid.

SECURE ENGINEERING

Software development is the outcome of complex processes involving a large number of people. Bridging the gap from architecture and specifications to the final implementation is only one of the challenging tasks that developers have to face. In addition, the interaction and communication between the diverse players has to be mastered throughout the engineering process. Languages, methods, and tools in the engineering process need to support the variety of perspectives of the players involved.

Fraunhofer SIT develops and optimizes standardized engineering methods that can guarantee a defined level of IT security. The focus is on support for stakeholders who are not experts in IT security, yet need to be equipped to take the right IT-security design decisions.

Together with partners in industry, Fraunhofer SIT develops new engineering approaches and optimizes software development processes in regard to IT security. The Institute can draw on rich experience when it comes to analyzing and evaluating software. It supports software manufacturers over the complete software life cycle and offers:

- Security design decisions/application-specific threat models
- Definition of protection goals
- Test methods for different software products
- Training programs for developers
- Evaluation and productive use of test tools
- Development of tools for specific applications

Fraunhofer SIT and EC SPRIDE Competence Center
In the field Security and Privacy by Design, Fraunhofer SIT is working together with the Technical University Darmstadt in the largest center of expertise in security, EC SPRIDE. The center is funded by the Federal Ministry of Research.

The Technical University Darmstadt and Fraunhofer SIT explore how IT developers can protect software and IT systems from the first design and over the entire life cycle. The results are relevant for all the growth markets, for the software industry, automotive and mechanical engineering as well as energy and healthcare industries.

Prof. Dr. Eric Bodden
secure-engineering@sit.fraunhofer.de

SECURE ENGINEERING LAB

THINK TANK FOR SECURE SOFTWARE ENGINEERING

Software AG and the Center for Advanced Security Research Darmstadt (CASED), represented by Fraunhofer SIT, have agreed to form a strategic partnership. Software AG can thus use the expertise of an institution with a background in excellent research for their software development process. Furthermore, the partnership strengthens the region as well as the cooperation of two partners in the software cluster. The joint activities focus on building a new laboratory for CASED for Secure Engineering.

The partnership focuses on the theme »IT security« and should serve in the long term as a transferable example of cooperation between industry and research. Another objective is to strengthen the software cluster in southwest Germany and the Darmstadt House of IT. In the first step, the partnership aims at a duration of three years.

The focus includes topics such as the safety of products and services as well as compliance. Software AG and CASED will also cooperate closely in the context of research and consultancy contracts and in publicly funded projects. The Secure Engineering Lab is the organizational framework for the joint activities of the Technical University of Darmstadt, Fraunhofer SIT and Software AG with its security team. The lab is directed and represented to the outside by Prof. Mira Mezini, Chair of Software Engineering at the Technical University of Darmstadt and Prof. Michael Waidner, Fraunhofer SIT.

CLOUD COMPUTING

Cloud computing will mark the next revolution for users of IT resources. Outsourcing hardware and software to the cloud represents a major step on the road to a new IT paradigm. Many potential cloud computing users are aware of the opportunities, yet hesitate to give the new technology a try.

By definition, outsourcing to the cloud means relinquishing control. Will it still be possible to comply with all relevant statutory requirements in the cloud, especially those linked to data protection? Will the data still be protected against unauthorized access? Will it be kept sufficiently separate from that of other customers? Can a third-party administrator be trusted in the first place? Does switching to the cloud entail a long-term commitment to one provider?

Increased security = increased efficiency

Fraunhofer SIT helps businesses leverage the benefits of the cloud: we develop and implement security concepts for cloud services, evaluate the security mechanisms of cloud vendors, formulate service level agreements, and help ensure conformity with legal regulations. The Institute also undertakes feasibility studies on behalf of customers planning to outsource data and services to the cloud.

Customers benefit

- Rapid development of know-how
- Best-practice security and technical excellence
- Risk minimization with user-friendly security
- Professional project management
- Sustainability through orientation and on standards
- State-of-the-art technology
- Neutrality of provider and producer
- Sustainability through orientation and on standards

Dipl.-Inform. Michael Herfert
cloud-computing@sit.fraunhofer.de

OMNICLOUD

SECURE AND FLEXIBLE CLOUD-BACKUP

Cloud Computing allows enterprises to reduce their costs immensely, at the same time they increase the flexibility of their own IT. Many companies, however, still hesitate to take a step towards Cloud due to a fear of losing control over their data, and problems with data privacy and protection. With OmniCloud, Fraunhofer SIT has developed a solution that allows users to access cloud storage services easily and securely, and supports the move to other providers. Losing data can entail major consequences for companies, both economically and legally. That is why every company operates its own backup solution.

Data leakage and dependencies

Surveys show that specifically security concerns keep companies from using cloud computing. Another obstacle is the commitment to one cloud provider, because adapting processes often comes with considerable costs, the provider's interfaces are proprietary, and functionalities differ. This fosters a dependency, a provider lock-in, even if the conditions of use permit termination of contract on short notice.

Investments into your future

HESSEN

The investments for this development were co-financed by the EC's European Regional Development Fund and the State of Hesse.

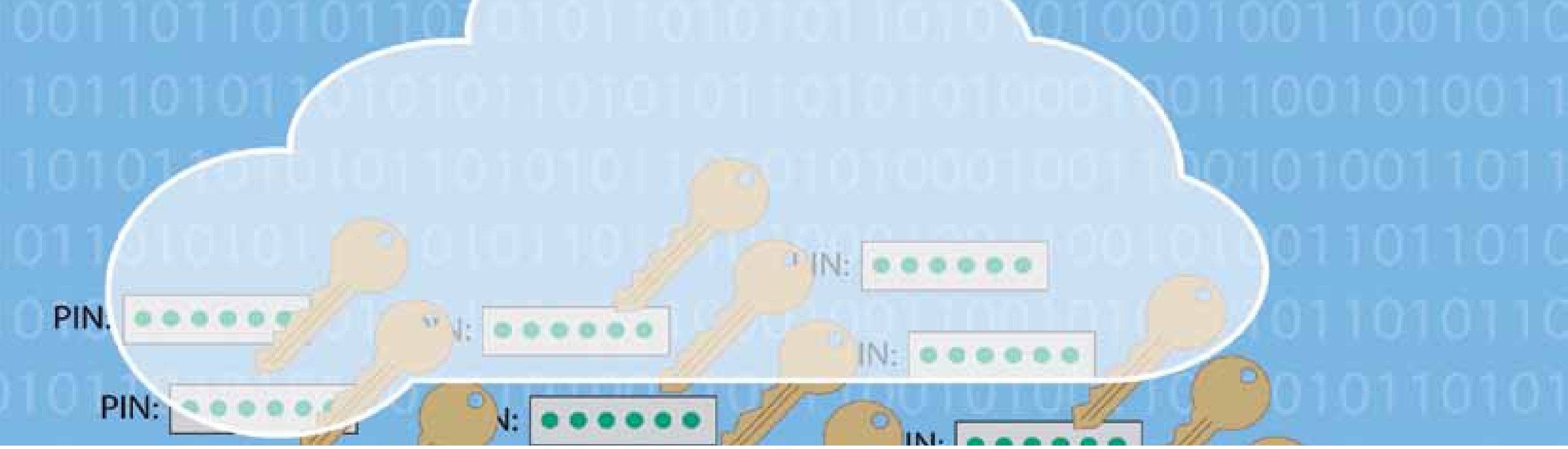
Adapter with integrated encryption

With OmniCloud, Fraunhofer SIT has developed a solution to prevent provider lock-ins and unwanted data leakage. OmniCloud is a software component running at the customer's site, building up a connection to the cloud provider. It encrypts data before they reach the cloud. OmniCloud manages the encryption. Beyond that, OmniCloud also acts as a translator between different cloud APIs. This means that companies can access OmniCloud over an API of the major providers. OmniCloud then transmits the data to another provider and his API. This basically eliminates provider lock-ins.

Avoid doublings

OminiCloud also offers a deduplication functionality, even if provider APIs do not support such a functionality. Files present as multiple copies at an enterprise will be filed in the cloud only once. This reduces storage costs and the volume of the data. Deduplication and data encryption are carried out completely on the customer's side. The security issues normally associated with deduplication thus do not occur. Fact: OmniCloud combines the security of a conventional backup with the cost benefits of a cloud backup, offering customers an economical advantage while providing utmost security.

Dipl.-Inform. Ruben Wolf
ruben.wolf@sit.fraunhofer.de



SCANNER FOR MACHINE IMAGES

CASED SCIENTISTS DEVELOP INSTRUMENT FOR TEST

Scientists from the Darmstadt Research Center for Advanced Security (CASED) have discovered major security vulnerabilities in numerous virtual machines published by customers of Amazon's cloud. From 1100 public Amazon Machine Images (AMIs) used to provide cloud services about 30 percent are vulnerable, allowing attackers to manipulate or compromise web services or virtual infrastructures. The main reason lies in the careless and error-prone manner in which Amazon's customers handle and deploy AMIs. CASED scientists have developed a vulnerability scanner for customer virtual machines created to run on Amazon's infrastructure. It can be freely downloaded at http://trust.cased.de/AMID.

Cloud computing is becoming increasingly popular. More and more companies and private users are offering services in the cloud. While security experts have been mainly focusing on security aspects of the underlying cloud infrastructure and provider, it seems that in practice the threats caused by the cloud customers when constructing services are still underestimated or ignored.

The scientists at Fraunhofer SIT in Darmstadt and the System Security Lab at the Technical University Darmstadt examined services published by customers of Amazon Web Services (AWS). Even though AWS provide their customers with very detailed security recommendations on their web pages, the scientists found that at least one third of the machines under consideration have flawed configurations. The research team could extract security critical data such as passwords, cryptographic keys and certificates from the analyzed virtual machines. Attackers can use such information to operate criminal virtual infrastructures, manipulate web services or circumvent security mechanisms such as Secure Shell (SSH).

Prof. Dr. Michael Waidner
michael.waidner@sit.fraunhofer.de

HOW SECURE IS CLOUD STORAGE?

STUDY WITH CRITERIA CATALOGUE FOR USERS

The security of cloud storage services is often inadequate. This is the result of a Fraunhofer SIT study »On the Security of Cloud Storage Services«, which involved the testing of various providers. Their conclusion: none of the providers that were tested were able to fulfill all of the security requirements, and some of them were even lacking proper encryption. In addition to technical shortcomings, the testers also found errors in relation to user guidance. The latter could result in confidential data being found with the help of search engines. In addition to the market leader Dropbox, Fraunhofer SIT also checked the security of six other cloud storage service providers, including CloudMe, CrashPlan, Mozy, TeamDrive, Ubuntu One and the Swiss provider Wuala. Besides specific points of critique with regard to different services and improvement recommendations, the study provides a catalogue of criteria for the evaluation of cloud storage services. With the help of this catalogue, other providers can be evaluated as well.

The testers focused in particular on data encryption and the securing of communication. Every provider displayed security deficits, and what's more, none of the services were able to fulfill all of the basic security requirements. For example, some of the providers do not use any of the 'standard' secure protocols for securing data transmissions within the cloud. Negative points were also assigned if, for example, data was moved to the cloud without being encrypted.

With some of the service providers, the users mistakenly believed that their sensitive information could only be accessed by a small group of people, whereas in reality it could be viewed by anyone, without anybody even noticing this. Such file sharing is critical, even when the data is encrypted. Fraunhofer SIT informed the providers about the results prior to the publication of the study.

A free download of the study is available at
www.sit.fraunhofer.de/cloudstudy

Dipl.-Inform. Michael Herfert
cloud-computing@sit.fraunhofer.de

MOBILE SYSTEMS

IT trends emanate from mass markets nowadays. This is particularly clear in relation to smartphones and tablet PCs. Although these devices were not originally designed for commercial use, they are now being utilized increasingly in companies. Employees often use such smart devices for both private and work-related activities. And because of this, companies are looking for solutions that will protect business-critical data and services while enabling the efficient management of mobile devices.

What happens if a device is lost or confidential company data is unknowingly taken outside of the company? What if an attacker has gained access to a mobile device containing critical company services? How can these devices be managed in a simple and flexible manner (Mobile Device Management), and in doing so, are companies actually allowed to back up private data?

At the moment, there are no tried and tested methods available for realizing concepts such as »dual use« or »bring-your-own-device« in a responsible and simple manner. The key challenges here relate to the security awareness of users and the management of mobile devices (including the data on them) throughout the entire lifecycle. Fraunhofer SIT has a wealth of experience with iOS, Android and other common operating systems. The employees of the institute harden mobile systems, develop innovative applications and security modules, evaluate already products available, and support companies and public authorities with their extensive know-how and manufacturer neutrality.

Offerings

- Technical advice in relation to iOS, Android and OS's
- Evaluation of existing solutions
- Integration of protected mobile end devices
- Concepts for secure mobile device management
- Secure configuration of smart device solutions
- Adjustment to existing systems
- Awareness workshops for employees and management

Test lab for mobile security

Security analyses for mobile platforms and infrastructures, practical tests for smartphone solutions apps, etc. – with/ without public test report

Dr.-Ing. Kpatcha Mazabalo Bayarou
kpatcha.bayarou@sit.fraunhofer.de

Dr. Jens Heider
mobile-systems@sit.fraunhofer.de

APPICAPTOR

FRAMEWORK FOR APP SECURITY TESTS

Which apps are safe to install on the company tablet or smartphone? Allowing the staff to use apps indiscriminately may endanger the company's own security. Many app developers do not have sufficient IT security knowledge, which frequently leads to inadvertent vulnerabilities. App stores may check for malware, but specific app security features and correct implementation are not the subject to verification. Fraunhofer SIT has developed the »Appicaptor« test framework exactly with this scenario in mind, giving enterprises an opportunity to automatically check if apps are compliant with their IT security policy.

iOS, Android, Windows Phone, BlackBerry

»Appicaptor« generates an individual test report for each app and each operating system, with the analysis being carried out automatically. These management reports can be understood by people without comprehensive IT security knowledge. The system issues a warning when vulnerabilities or the insecure use of sensitive data are detected. Since apps are often revised and new insights emerge concerning weaknesses and implementation errors, »Appicaptor« repeats the tests regularly as well, thus constantly evaluating the security features based on the latest technological knowledge.

»Appicaptor« is a framework composed of different analytical methods and tools, which can be expanded by almost any new tool and test procedures. Even though the internal makeup of the iOS platform is not very well known, the institute was able to develop and integrate methods into »Appicaptor«, with which iOS app risks could be identified precisely and quickly.

Range of Services

- Concepts for the secure use of mobile devices (integrated mobile device management)
- Technical consultation; IT security guidelines
- Providing app recommendation lists (whitelist/blacklist)
- Support in secure app development
- Automatic basic tests and compliance checks
- In-depth manual app vulnerability analyses
- Expert tests of app binaries and app source code audits
- Development of concepts, procedures and tools for IT security testing of mobile services and devices

Investments into your future

HESSEN

The investments for this development were co-financed by the EC's European Regional Development Fund and the State of Hesse.

Dr. Jens Heider
jens.heider@sit.fraunhofer.de

IS YOUR SMARTPHONE CHEATING ON YOU?

FREE AWARENESS-POSTER

Download the poster:
sit4.me/posterdownload

BIZZTRUST

PROTECTION OF SENSITIVE DATA AND SERVICES

In many enterprises smart devices such as smartphones and tablets have become part of the corporate culture. But very often, current commodity smart devices do not fulfil the underlying corporate security requirements. With BizzTrust for Android, Fraunhofer SIT has developed a security framework that protects sensitive enterprise data, apps, and services both on the device and when connecting to an enterprise's network without restricting functionality and user.

In dual-use scenarios, the employer needs to take care of the security and management of the smartphone and at the same time protect corporate assets and services on the device and in the corporate IT infrastructure against various malware attacks. This particularly concerns any application that is installed for private use, since these applications are considered to be untrusted and should not affect the corporate data and services. Moreover, the employer should not have the full control over the employees' private data on the device.

BizzTrust resolves these problems and creates a security framework that combines domain isolation and modern communication protocols. BizzTrust separates applications and data into security domains, executing personal applications in parallel while isolated from business applications. This is also done for all services including SMS, phone functionality, etc. The isolation is context-based, i.e., security policy enforcement can depend on the context the device is in, allowing very flexible treatment of sensitive and uncritical data and apps. Furthermore, the flexible remote maintenance protocols make it possible to analyze the software status of a remote device by attesting the state of the corporate domain and to enforce update or remediation procedures based on an enterprise's security policy. With the extended remote management, the business compartment of the employee's phone can be integrated into the enterprise event management infrastructure.

Features:

- Protection of business data
- No restrictions for private use
- Secure enterprise communication (encryption)
- Remote management and update
- Supports bring-your-own-device strategy
- Automatic policy enforcement

Investments into your future

The investments for this development were co-financed by the EC's European Regional Development Fund and the State of Hesse.

oliver.kuech@sit.fraunhofer.de
www.bizztrust.de

IDENTITY AND PRIVACY

Data protection scandals regularly attract massive attention. The harm caused to the image of the companies concerned is often immense. Customer defection, collapsed sales, and lost confidence among business associates are just a few of the potential consequences. If compliance requirements have been violated, there is also a risk of penalties, legal disputes, and claims for compensation by the victims.

Fraunhofer SIT helps businesses and public authorities to handle sensitive data in an efficient and legally secure way by testing, customizing, and developing made-to-measure solutions. The proliferation of identities and roles is one of the principal challenges here. At the same time, maximum data quality needs to be reconciled with user self-determination. This is only possible if identity management and data protection are acknowledged as an integral part of the overall system from the outset. For this reason, Fraunhofer SIT focuses on solutions that are secure »by design«.

eGovernment, eHealth, and automotive
Fraunhofer SIT supports businesses and public authorities wishing to protect information and identities. In particular, our services include:

- Analysis and customizing of existing solutions for identity and access management (IAM)
- Design and implementation of data protection concepts
- Implementation of internal / external public key infrastructures – either with or without integrated Smart card technology
- Data protection audits
- Consulting and development activities linked to electronic patient files
- Secure integration of Germany's new identity card in online and corporate applications (training, consulting, development)
- Testing and development of secure ICT applications for motor vehicles
- Web 2.0 identities

Prof. Dr. Michael Waidner
identity-and-privacy@sit.fraunhofer.de

iMOBILESITTER

CLEVER PASSWORD MANAGEMENT FOR iPHONES

Passwords or PINs are needed for numerous things nowadays, such as EC cards, mailboxes and connections to networks or resources, which are used for private and/or business purposes. But the more we have, the more difficult it becomes for us to remember them without the assistance of tools such as password managers. These must fulfil the highest possible security standards. Fraunhofer SIT has developed the software iMobileSitter, which manages access data on iPhones and protects it against hacker attacks using a particularly clever method. The iMobileSitter is available in the App Store.

The software is extremely easy to use: the user simply needs to remember a master password; iMobileSitter takes care of the rest. The software protects all access data on the iPhone with an innovative method, which will really exasperate hackers: it accepts any master password that is entered, thereby opening the storage area and displaying the supposed secrets. Each result that is displayed really looks like it could be the right one. For example, if a four digit PIN has been saved, a combination between 0000 and 9999 will always be displayed, which means a hacker will be unable to tell whether the attempt was successful. What's more, it doesn't matter whether the hacker performs the attack directly or uses software to automate the attack. The fact that the attack was unsuccessful will not become apparent until the hacker tries to use an ATM and the EC card is withheld after three incorrect attempts. The legitimate user, on the other hand, will recognise a typo immediately: a small symbol on the screen serves as a kind of feedback for the legitimate user. The user recognizes that he has entered the correct master password if the expected symbol is displayed. The attacker does not know the user's symbol; for the attacker the symbol has no semantic value with respect to the correctness or incorrectness of the master password that has been entered.

Who would benefit from iMobileSitter?

- Companies that place a great deal of importance on secure password management for their employees
- Private individuals who want to protect their passwords
- For all those who want to do a good deed: gift vouchers can be purchased in the App Store, which can then be used to purchase the software

ruben.wolf@sit.fraunhofer.de
www.imobilesitter.de

SECURITY MANAGEMENT

Not only technical failures or human errors, but targeted attacks can cause irreparable damage in both the private and public sectors as well. It is clearer today than ever that it is not sufficient for each user simply to protect their own information with high-tech solutions such as firewalls or virus scanners.

The basic principle underlying the BSI Standard on Information Security reads: »Practical experience has shown that optimizing information security management frequently improves information security more effectively and lastingly than investing in security technology«. In order to guarantee an adequate level of security, an organisation's resources and processes must be considered in a holistic approach and taken into account in its security concepts. This approach ensures that the information security management is properly aligned to the business processes and supports the achievement of the information security targets.

Risk evaluation and management

- Guidance for planning and designing appropriate information security management concepts that meet an established set of standards
- Support for policy development and evaluation, the evaluation of assets, and the implementation of measures
- Conceptual design and implementation of an incident and business continuity management system
- Audits for evaluating safety levels
- Implementation of indicator systems to control information management system performance
- Planning and realization of training programs and awareness campaigns tailored to specific target groups

Mechthild Stöwer
security-management@sit.fraunhofer.de

COMPETENCE CENTER PKI

PUBLIC KEY INFRASTRUCTURES AND SMARTCARDS

In cooperation with other Fraunhofer Institutes, Fraunhofer SIT maintains the Fraunhofer Competence Center for Public Key Infrastructures (CC-PKI – www.pki.fraunhofer.de). Under the leadership of the CC-PKI, a Public Key Infrastructure (PKI) was planned and established for the Fraunhofer-Gesellschaft. This Fraunhofer-PKI has been in use since 2008 and has proven its worth in a very heterogeneous and complex environment.

In the highly secure Trust Center at Fraunhofer SIT's Birlinghoven location, smartcards are produced for the Fraunhofer-Gesellschaft to serve as a medium for keys, certificates and employee IDs as well as PIN letters. About 22,000 employees use these smartcards for encryption, electronic signatures and authentication. The cards are optically personalized (photo), and can also serve as an employee ID. Optionally, they can be equipped with RFID and magnetic stripes, for example to facilitate working time recording or payment system use. Other types of hardware token and soft token (software keys) complete the broad range of services and allow for the covering of a wide range of use cases and applications – including mobile applications.

The valuable experience we have gained through conceptualization, development, deployment and operation of the Fraunhofer PKI is a solid basis for further PKI projects. Our experience also extends to such aspects as user friendliness (service desk), redundancy, revision security, and the development of various interfaces including web interfaces, online forms, etc. We offer comprehensive know-how and support for the definition of complex security concepts and processes, and for their implementation in a production environment. We have experience with personalizing smartcards in highly secured rooms and networks, and can provide broad competence with regard to key escrow, registration authorities, setting up operation service desks and the development of customized software components.

We can provide you with

- Design and setup of a PKI
- Adjustment of an existing PKI
- Professional consultation and coaching on all PKI related issues: Does your business need a PKI? Which Trust Center architecture is best suited?
- Operational model development taking into consideration of characteristics of digital certificates, use cases, policies, auditing acceptability, key escrow, service desks and support
- Selection of products and their technical and organizational integration
- Development of additional components such as forms and web interfaces

claudia.hirsch@sit.fraunhofer.de
pki.sit.fraunhofer.de

SECURITY TEST LAB

How secure IT actually is in practice only becomes apparent when it is targeted by an attacker. Remediating vulnerabilities after the damage has been done is both difficult and expensive, especially if the root of the problem is located deep down in the system architecture. A security analysis in the Fraunhofer SIT Test Lab delivers valuable information about whether a product or service really is secure before it is too late. If security holes exist, our tests do more than simply buy you time; our experts also suggest ways to close the critical gaps. And if your products are fully compliant with the relevant security requirements, you can provide proof of this to your customers with a Fraunhofer SIT certificate.

The Test Lab's services at a glance:

- Product evaluations based on typical installations
- Service security analyses
- Certificates and published test reports as proof of product security (including recommendations for installation and configuring)
- Product comparisons and product selection guidance
- Evaluation of the security risks linked to integration projects
- Recommendations for remediating vulnerabilities

Attack is the best form of defense

The Fraunhofer SIT Test Lab tests the IT security of IT products on behalf of manufacturers and business users. Each security analysis is based on requirement and threat analyses, architecture evaluations, and real attacks, all of which are taken into account in the overall assessment for a specific application.

Prof. Dr. Eric Bodden
security-testlab@sit.fraunhofer.de

HARDWARE SECURITY LAB

SECURITY AND PRIVACY FOR A CYBER-PHYSICAL WORLD

IT components are a central component of many devices and products that are part of our everyday lives. Whether car, production facility or medical technology, these embedded systems often take on control functions and play an important role for new products. At the same time they are more and more networked with the internet, physical systems and sensors – they become cyber-physical systems. These IT components are an attractive target for attackers and counterfeiters.

Conventional protective measures have been proven in practice to be unusable. Therefore, Fraunhofer SIT works in the hardware lab security on new procedures to protect cyberphysical systems and their communication channels.

In this context we examine hardware fingerprints (Physical Unclonable Functions – PUFs) and corresponding function patterns that allow devices to be identified unambiguously. Fraunhofer SIT uses this for cryptographic applications and security protocols.

The hardware security lab's range of offers aims at manufacturers of embedded systems, equipment manufacturers and other hardware developers.

We offer:

- Cyber-threat monitoring and threat mitigation
- Security and privacy for smart infrastructures
- Cryptographic engineering
- Hardware security analysis and physical crypto-analysis
- Implementation attacks and fault analysis
- Constructive side channel analysis
- Hardware assurance and trojan analysis

Michael Kasper
michael.kasper@sit.fraunhofer.de

IT FORENSICS

Many criminals use computers and the Internet nowadays to achieve their goals, But they often leave digital traces behind, which can help to discover, solve or prove criminal or illegal activities. It is the job of IT forensics to identify, secure and analyze such digital footprints.

However, ongoing technical developments mean the investigators are confronted with significant challenges: the volume of data has increased to such an extent, that the information can only be searched through, analyzed and evaluated efficiently with the help of IT-based forensic tools. These tools must be updated on an ongoing basis, however, in order to ensure they can keep up with the rapid technical developments. What's more, perpetrators also use computer technology to hide their tracks and prevent the utilization of IT-based forensic procedures and tools through the targeted use of specific technologies.

Field of activity and services

Fraunhofer SIT is active in many areas of IT forensics and offers, among other things, the following services and products:

- Procedures and software for identifying illegal multimedia data
- IT-based forensic analyses: identification of traces on different data storage media and systems
- Analysis and improvement of IT-based forensic tools: tests, development, ongoing development
- Forensic hacking: exploitation of security weaknesses to obtain data that can be used for IT forensics
- Procedures and software for the swift identification of similar files
- Mobile forensics: IT-based forensic analysis of smartphones, tablets and other mobile devices
- Forensic analysis of financial data: statistical methods for identifying fraud
- File carving: procedures and software for identifying and restoring files and file fragments

Dr. Markus Schneider
it-forensics@sit.fraunhofer.de

FORBILD

FORENSIC IMAGE RECOGNITION

Police investigators and prosecutors often have to browse large amounts of data in search of illegal images. To automatically scour the masses of pictures as quickly and efficiently as possible, they use methods and tools of computer forensics.

Fraunhofer SIT extends and specifies these methods with the project »ForBild« – forensic image recognition: With robust hashes images can be identified quickly and reliably. Fraunhofer SIT has been testing and optimizing this complementary method. The technique does not use the file properties for image recognition, but is tied to human perception: If an image appears identical to a human eye, the comparison value is the same. With that, the process ignores possible changes in the image file size, the noise factor, or the file format and focuses on visual similarities to identify the images. This mechanism is called robust hash, following the cryptographic functions.

Within the project »ForBild«, Fraunhofer SIT, LSK Data Systems GmbH and the Technical University of Darmstadt have tested robust hashing and optimized simple robust hash functions, so that they can be used as a supplement to the usual cryptographic hash functions. The robust hash for the images to be examined must be calculated very quickly, so that large quantities can be analyzed as quickly as possible. The robust hashes should also identify images very safely to achieve a low error rate; for each false alarm must be checked manually, creating pressure on the investigators. At the same time, the recognition rate must not be so low that the tool is useless for image search. »ForBild« project partner LSK Data Systems has integrated the robust hash process into a compact disk reader. This allows investigators to put a stack of CDs with pictures they want to check into the disk reader and check the data automatically. Thus, the investigators are relieved of time and mental effort while looking for relevant material. Fraunhofer SIT recommends to consider this process as a complement to traditional hash procedures in the prosecution of child pornography.

Fraunhofer SIT is planning an extension of the robust hashing, to involve other media and other technical strategies. They will also include videos that should be examined forensically on illegal shots.

2. Platz 2012
Deutscher
IT-Sicherheitspreis

Dr.-Ing. Martin Steinebach
martin.steinebach@sit.fraunhofer.de

CYBER-PHYSICAL SYSTEMS

Cyber-physical systems cover a variety of mobile and embedded devices that combine computational and physical aspects, such as RFIDs, sensor nodes and smartphones. These systems have become an integral part of our everyday lives. Moreover, embedded computing platforms such as smartphones undergo a rapid development becoming progressively more sophisticated with regard to their computational, storage, and interface capabilities.

Cyber-physical systems hold enormous potential for a wide range of applications, and they act as enablers for many future technologies. At the same time, the growing popularity and widespread use of cyber-physical systems, along with the fact that they are increasingly employed to process and store privacy-sensitive and security-critical data, makes them attractive targets for all kinds of software (e.g. viruses and Trojans) and hardware (e.g. side channel) attacks.

Fraunhofer SIT has carried out extensive work on the security and data protection aspects of cyber-physical systems and their communication channels.

Key aspects:

- Research and development of cryptographic techniques and security technologies specifically for cyber-physical systems
- Analysis and extension of existing security architectures for cyber-physical systems and development of novel security solutions, particularly for smartphones
- Development of hardware fingerprints such as Physically Unclonable Functions (PUFs)
- Design and development of hardware based attestation techniques for checking the integrity of devices
- Development of novel identity and facility management solutions based on cyber-physical systems, which combine physical and logical security concepts

Prof. Dr. Michael Waidner
cyber-physical-systems@sit.fraunhofer.de

KEY2SHARE

ACCESS CONTROL IN ENTERPRISES

Key2Share is a new app for NFC-enabled Android smartphones that allows enterprise employees to access offices and other enterprise premises using digital access control tokens stored on their mobile phones.

The Key2Share app utilizes Near Field Communication (NFC) technology, which enables the phone to emulate a contactless smartcard that can be used with standard contactless smartcard readers. The Key2Share app allows an enterprise to distribute and manage the digital access control tokens of its employees in an efficient and controlled way. Tokens can be issued and revoked remotely, delegated to other employers or visiting guests, and support context-aware and time-limited access control policies. For example, these policies may deny access to office rooms during weekends and holidays, or specify whether tokens can be delegated to other users. Electronic door locks can provide access logs for auditing, or unlock all exits in case of an emergency (such as fire or earthquake).

Storing and handling digital access control tokens on a mobile phone raises risks of being targeted by attacks. Particularly, in the context of enterprise usage scenarios attackers may be motivated to perform sophisticated attacks. These risks are addressed by the underlying platform security architecture, which protects digital access control tokens on the smartphone. It provides a secure storage and a secure execution environment, where digital tokens can be securely stored and processed in strict isolation from untrusted and possibly malicious code.

Alexandra Dmitrienko
alexandra.dmitrienko@sit.fraunhofer.de

MEDIA SECURITY

Digitization leads to more a efficient production and distribution of media. At the same time, it creates a whole series of risks and challenges for producers and distributors. Media that are digitally produced and distributed are more susceptible to unauthorized external access and more easily passed on illegally – and unnoticed – by internal offenders.
To protect digital media, Fraunhofer SIT marks the originals with digital watermarks. Each medium can be individually marked and traced back to its source.

Protection for content, protection for users
Fraunhofer SIT's digital watermarking technology is already used in numerous archives, online portals, and equipment. It is optimized in an ongoing process. Its solutions boast high performance values with regard to:

- Protection of digital media without compromising usability
- Individual marking of audio, video, images, PDF documents
- Highly efficient processes for downloadable solutions
- Individual alignment to requirement profiles

Protection for online shops
Online shops are characterized by direct contact between the vendor and the customer, and it is this contact that forms the basis for transaction watermarks. Each customer receives an individually marked copy of the purchased media. Fraunhofer SIT solutions have been successfully implemented for many years, and today enjoy a reputation for excellent performance, above-average robustness, and high transparency. Particularly in the audio sector – not only music but also audio books – the Institute has made a name for itself as a reliable solution provider. MP3, AC3, and PCM-WAV are all supported as data formats, and it makes no difference whether or not the material is compressed.

Protection for samples
The damage caused by the illegal distribution of material is enormous. The vulnerability to unauthorized copying is especially great if the media are distributed upfront of their official release on the open market (press samples, advance copies etc.). On the one hand, right holders must be in a position to protect their works, while on the other, the addressees must be able to access the media without any problems. Fraunhofer SIT offers integrated solutions based on Rimage systems for this purpose, in which recipient lists are automatically processed, customer watermarks embedded in the data, and the recipient‹s ID printed on the storage medium – with no possibility of confusion.

Dr.-Ing. Martin Steinebach
media-security@sit.fraunhofer.de

MARK'N'SEARCH

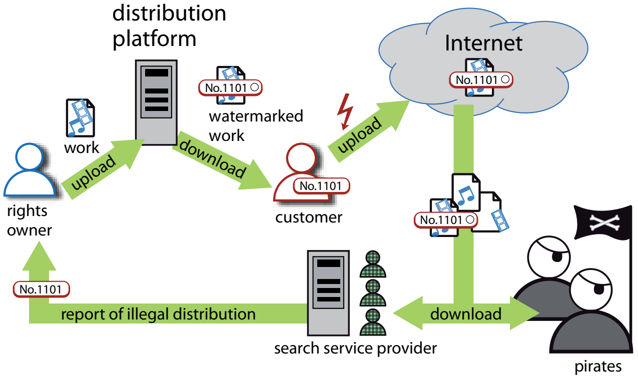
SOLUTION FOR CUSTOMER-FRIENDLY COPYRIGHT PROTECTION

It never was easier to copy and distribute all kinds of works without quality loss. As a consequence, practically all current works are available on the Internet – regardless of their copyright status. This is true for music, audio books and movies, but also for eBooks or software. The digital watermarking technology developed at Fraunhofer SIT enriches works with additional information. For example transactional watermarking allows to link a work individually to its buyer. Should such a work appear on the internet, the embedded watermark message allows direct identification of the original buyer. No protection is complete without some means of control. Digital watermarks literally become one with the protected work and are therefore extremely hard to remove – surviving even analog-digital conversion. But before a work can be checked for watermarks, the work needs to be found first.

Many rights owners still only search sporadically and manually for watermarked works. In addition, such searches are most often limited to filesharing networks. To improve this situation the MediaSearch Framework has been developed by Fraunhofer SIT. It mimics behavior of normal users and in doing so finds watermarked works everywhere on the Internet –fully automated.

»Mark 'n' Search« thus protects works independently of their actual distribution channel. Besides several filesharing networks, sharehoster, UGC sites (like YouTube and other web 2.0 sites) as well as specialized blogs are already searchable.

Fraunhofer SIT offers the complete »Mark'n'Search« package: The Fraunhofer SIT watermarking container, a highly efficient and fast transactional watermarking technology designed with the special needs of online shops in mind, plus a targeted, fully automated search service for watermarked works.



martin.steinebach@sit.fraunhofer.de
http://watermarking.sit.fraunhofer.de

BOARD OF TRUSTEES

Edgar Aschenbrenner
E.ON IT GmbH | Chairman of the Management Board

Prof. Dr. Johannes Buchmann
Technische Universität Darmstadt

Guus Dekkers
Airbus S.A.S. | CIO

Dr. Thomas Endres
Voice-Verband der IT-Anwender e.V. | President

Dr. Johann Fichtner
Siemens AG | Director IT-Security Siemens Corporate Technology

Michael Hange
Bundesamt für Sicherheit in der Informationstechnik | President

Dr. Wolfram Jost
Software AG | CTO R&D and Product Management

Dr. Matthias Kaiserswerth
IBM | Director of the Zurich Research Laboratory

Volkmar Lotz
SAP | Technical Director

Dr. Ulrike Mattig
Hessisches Ministerium für Wissenschaft und Kunst

Dr. Hans-Joachim Popp
Deutsches Zentrum für Luft- und Raumfahrt e. V. | CIO

Hinrich Völcker
Deutsche Bank AG | Managing Director, CTO Global IT Security

CONTACT

Vice President; IT-Forensics
Dr. Markus Schneider
markus.schneider@sit.fraunhofer.de
Phone +49 6151 869-337
Fax +49 6151 869-224

Cybersecurity Analytics and Defences
Dr. Haya Shulman
haya.shulman@sit.fraunhofer.de
Phone +49 6151 869-505
Fax +49 6151 869-224

Cloud Computing, Identity & Privacy
Dipl.-Inform. Michael Herfert
michael.herfert@sit.fraunhofer.de
Phone +49 6151 869-329
Fax +49 6151 869-224

Media Security, IT Forensics
Dr.-Ing. Martin Steinebach
martin.steinebach@sit.fraunhofer.de
Phone +49 6151 869-349
Fax +49 6151 869-224

Secure Engineering, Security Test Lab
Prof. Dr. Eric Bodden
eric.bodden@sit.fraunhofer.de
Phone +49 6151 16-75422
Fax +49 6151 869-224

Marketing and PR
M.A. Oliver Küch
oliver.kuech@sit.fraunhofer.de
Phone +49 6151 869-213
Fax +49 6151 869-224

Director
Cyber-Physical Systems and Mobile Systems
Prof. Dr. Michael Waidner
michael.waidner@sit.fraunhofer.de
Phone +49 6151 869-250, Fax +49 6151 869-127

Mobile Systems
Dr.-Ing. Kpatcha Mazabalo Bayarou
kpatcha.bayarou@sit.fraunhofer.de
Phone +49 6151 869-274
Fax +49 6151 869-224

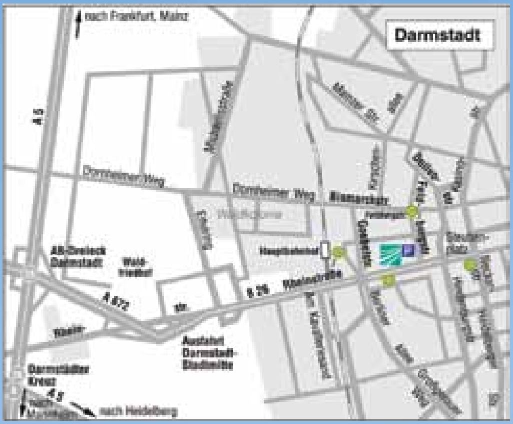
Cyber-Physical Systems
Dr. Christoph Krauß
christoph.krauss@sit.fraunhofer.de
Phone +49 6151 869-116
Fax +49 6151 869-224

Security Management
Mechthild Stöwer
mechthild.stoewer@sit.fraunhofer.de
Phone +49 2241 14-3123
Fax +49 2241 14-3007

Industrial Security
Dr.-Ing. Thorsten Henkel
thorsten.henkel@sit.fraunhofer.de
Phone +49 6151 869-4271
Fax +49 6151 869-224

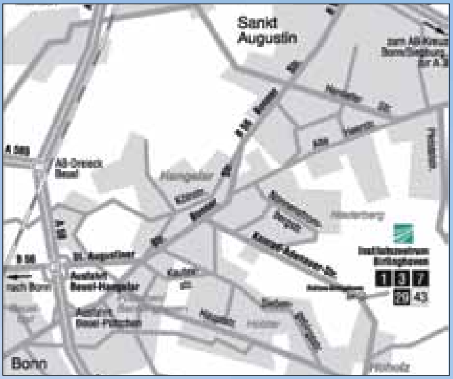
Test Lab Mobile Security
Dr. Jens Heider
jens.heider@sit.fraunhofer.de
Phone +49 6151 869-233
Fax +49 6151 869-224

Administration
Dipl. oec. Elvira Schepel
elvira.schepel@sit.fraunhofer.de
Phone +49 6151 869-210
Fax +49 6151 869-224



Headquarter Darmstadt
Rheinstrasse 75
64295 Darmstadt
Germany

Phone +49 6151 869-399
Fax +49 6151 869-224
info@sit.fraunhofer.de



Location St. Augustin
Schloss Birlinghoven
53757 Sankt Augustin
Germany

Phone +49 2241 143-272
Fax +49 2241 143-007
info-bi@sit.fraunhofer.de