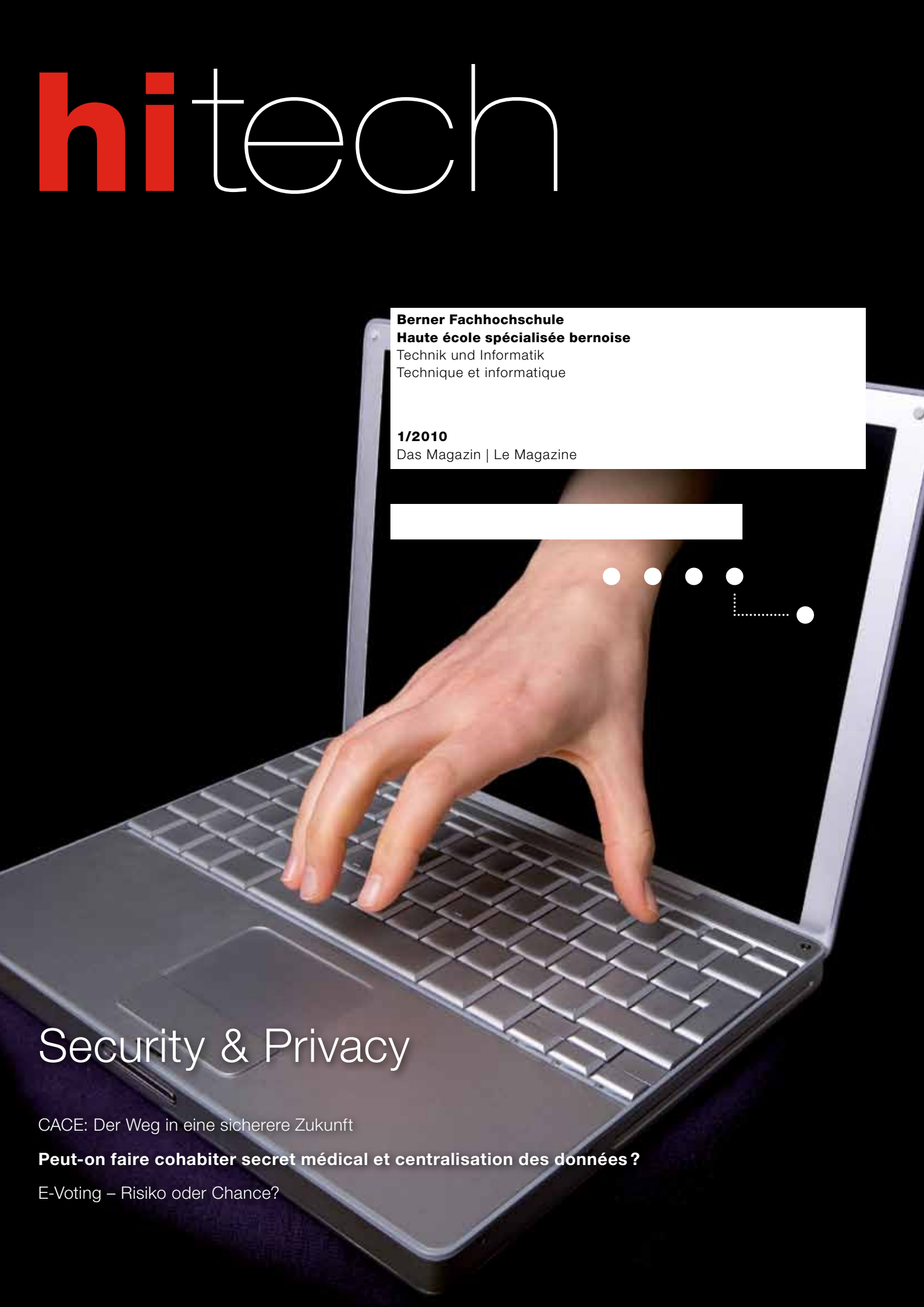
hitech

Berner Fachhochschule
Haute école spécialisée bernoise
Technik und Informatik
Technique et informatique

1/2010
Das Magazin | Le Magazine



Security & Privacy

CACE: Der Weg in eine sicherere Zukunft

Peut-on faire cohabiter secret médical et centralisation des données ?

E-Voting – Risiko oder Chance?

Focus 3
Security & Privacy

Titelseite: Hacker am Werk
Couverture: Hacker au travail
Photo: ©Tyler Olson, fotolia

IMPRESSUM

Redaktion Gabriella Scorrano, Diego Jannuzzo
Adresse BFH-TI, hitech-Redaktion, Postfach, 2501 Biel,
E-Mail Redaktion hitech@bfh.ch
Homepage hitech.bfh.ch
Adressänderungen und Inserate communication.ti@bfh.ch, 032 321 62 33, Inseratenschluss für die Ausgabe 2/2010: 31.03.10
Auflage 6800 Exemplare, erscheint 3x jährlich
Grafik, Layout Ingrid Zengaffinen
Druck Stämpfli Publikationen AG, Wölflistrasse 1, Postfach CH-3001 Bern – hitech 1/2010: Februar 2010

Sie finden das ganze Magazin in Deutsch und Französisch auf: www.hitech.bfh.ch

IMPRESSUM

Rédaction Gabriella Scorrano, Diego Jannuzzo
Adresse HESB-TI, hitech-Rédaction, Case postale, 2501 Biel/Bienne
E-Mail Rédaction hitech@bfh.ch
Homepage hitech.bfh.ch
Changement d'adresses et acquisition d'annonces communication.ti@bfh.ch, 032 321 62 33, Date butoir pour les annonces du prochain hiTech: 31.03.10
Tirage 6800 exemplaires, paraît 3x par année
Graphisme, mise en page Ingrid Zengaffinen
Imprimerie Stämpfli Publikationen AG, Wölflistrasse 1, Postfach CH-3001 Bern – hitech 1/2010: Février 2010

Ce magazine existe en version française et allemande à l'adresse: www.hitech.bfh.ch

Von der IT-Sicherheit zur Informationssicherung

Marc Henauer
Sektionschef
Eidg. Departement für Verteidigung, Bevölkerungsschutz und Sport, Dienst für Analyse und Prävention. Abteilung Informationsmanagement Cyberprevention MELANI. www.melani.admin.ch

Seit Jahren gehört es zum guten Ton in der IT-Branche, klassische technische Schutzmassnahmen wie Antivirensoftware, regelmässige Updates von Programmen und Betriebssystemen, den Einsatz von Firewalls und die Notwendigkeit von Backups zu propagieren. Dieses ABC der wichtigsten Schutzmassnahmen für Computer, sei es in einem privaten Haushalt oder in einem geschäftlichen Umfeld, sind noch immer gültig und unter allen Umständen weiterhin einzuhalten. Allerdings genügen sie heutzutage nicht mehr.
Beim Auto gelten Sitzgurte, eine angepasste Geschwindigkeit und das Befolgen von Verkehrsregeln als Voraussetzungen für ein sicheres Fahren, und dennoch können diese Sicherheitsvorkehrungen einen Unfall nicht immer verhindern. Genauso verhält es sich in der heutigen Welt der Bits und Bytes. Zwar liessen sich noch immer die überwiegende Mehrheit der Angriffe auf Computer und Netzwerke mit technischen Sicherheitsvorkehrungen verhindern, doch wie im Verkehr muss auch in der Welt der Informations- und Kommunikationstechnologien endgültig vom «absoluten Sicherheitsgedanken» Abschied genommen werden.
Diese Entwicklung erfordert ein Umdenken: Neu muss der Fokus auf den Schutz der Information gelegt und vom ausschliesslichen Schutz der Computer und Netzwerke, auf denen die Informationen lagern, abgesehen werden. Dies wird ein verstärktes Informations- und Datenmanagement, Informationsklassifizierung und dergleichen nach sich ziehen. Zudem wird eine klare Risikoabwägung vorausgesetzt, die dazu führen muss, dass die Sicherheit von Verteilkanälen, Zugriffsrechten und Speicherorten dem tatsächlichen Wert einer Information angepasst werden. Nicht jeder Kanal oder Speicherort ist gleich sicher und nicht alle Dokumente sind in einem Betrieb gleich sensibel. Damit muss die Informationssicherung in den geschäftlichen und strategischen Risikomanagement-Prozess eingebunden und Teil eines umfassenden Sicherungskonzeptes, welches sich von der physischen, über die personelle, bis zur IT-Sicherheit erstreckt. Denn die Zeiten, in denen die IT-Sicherheit als – von der Geschäftsleitung kaum wahrgenommene – Supporteinheit im Dunkelfeld agierte, sind definitiv vorbei.

Marc Henauer
Master of Arts NSST
Sektionschef

De la sécurité informatique à la sûreté de l'information

Dans la branche IT, depuis des années, il est de bon ton de programmer des mesures de protection technique traditionnelles telles que les antivirus, les mises à jour régulières des programmes et des systèmes d'exploitation, l'utilisation de pare-feu et les sauvegardes périodiques. Ce b. a.-ba des mesures essentielles qui servent à protéger les ordinateurs, dans un ménage privé ou dans un cadre professionnel, demeure certes valable et doit être respecté dans tous les cas. Actuellement, il n'est toutefois plus du tout suffisant.
En voiture, il faut attacher sa ceinture, adapter sa vitesse et respecter la signalisation pour circuler en sécurité. Et encore, ces prescriptions ne suffisent pas toujours pour éviter un accident. Il en va de même dans le monde actuel des bits et des bytes. Comme dans la circulation, même si les mesures techniques de sécurité et le bon sens permettent de déjouer la plupart des attaques visant les ordinateurs et les réseaux, il faut se faire à l'idée qu'«il n'y pas de sécurité absolue» dans le monde des technologies de l'information et de la communication.
Cette évolution exige de revoir notre façon de penser: il faudra désormais mettre l'accent sur la protection de l'information et ne plus se contenter de protéger les ordinateurs et les réseaux, où sont stockées les informations. Autrement dit, la gestion de l'information et des données, la classification de l'information, etc., joueront un rôle de plus en plus important. En outre, une véritable analyse des risques s'impose pour adapter à la valeur réelle de l'information la sécurité tant des canaux de distribution que des droits d'accès et des lieux de stockage. Tout canal ou lieu de stockage n'offre pas la même sécurité, de même que certains documents sont plus sensibles que d'autres. La sécurité de l'information a donc sa place dans le processus commercial et stratégique de la gestion des risques et doit faire partie intégrante du concept global de sécurité qui s'étend de la protection des bâtiments et des personnes à la sécurité IT.
L'époque où la sécurité IT agissait dans l'ombre, comme unité de support à peine perçue par la direction d'une entreprise, est bel et bien révolue.

Marc Henauer
Master of Arts NSST
Chef de section

Security and Privacy in the Information Society

Security, Privacy, Identity – Schlüsselwörter, die in unserem täglichen Umfeld wichtig sind und gerade im Bereich von elektronischem Informationsaustausch zentral für den Erfolg sind. Was sind die Probleme? Wo gibt es Lösungsansätze?

Prof. Dr. Bernhard Anrig
Studienleiter Informatik
RISIS, E-Voting Group
Foto: www.arteplus.ch

Dans les années à venir, les problèmes ayant trait à Sécurité, Confidentialité, Identité nous accompagneront sûrement dans la société de l'information, et ce tout particulièrement en combinaison ou, à tort bien souvent, comme des buts opposés:

«We've been told we have to trade off security and privacy so often – in debates on security versus privacy, writing contests, polls, reasoned essays and political rhetoric – that most of us don't even question the fundamental dichotomy. But it's a false one. Security and privacy are not opposite ends of a seesaw; you don't have to accept less of one to get more of the other.»
Quelle: Bruce Schneier Security vs. Privacy http://www.schneier.com/blog/archives/2008/01/security_vs_pri.html

Le futur de la société de l'information est donc basé sur la combinaison de Sécurité et Confidentialité dans les différents domaines de la vie de tous les jours, qu'elle soit réelle ou virtuelle. Malheureusement, ces buts ne peuvent pas être atteints à l'aide d'un ensemble de simples petites mesures ad-hoc qu'on ajouterait aux applications déjà existantes dans le domaine de l'informatique. Pour qu'elles soient vraiment fiables, il faut les inclure de manière globale lors de la conception et du développement des processus et des applications (cf. article de D.-O. Jaquet-Chiffelle, p. 24).

«The term ‹information security› means protecting information and information systems from unauthorized access, use, disclosure, disruption, modification, or destruction in order to provide integrity [...], confidentiality [...], and availability [...].»
US Code Collection 44 §3542

«Article 8 – Right to respect for private and family life
1. Everyone has the right to respect for his private and family life, his home and his correspondence.»
Council of Europe, Convention for the Protection of Human Rights and Fundamental Freedoms, 1950

Research Institute for Security in the Information Society RISIS

In diesem Spannungsfeld Security, Privacy, Identity wird in der BFH-TI von verschiedenen Gruppen im Rahmen des Forschungsschwerpunkts Mobile Informationsgesellschaft intensiv geforscht. Neu sind diese Tätigkeiten im Research Institute for Security in the Information Society RISIS unter Leitung von Dr. D.-O. Jaquet-Chiffelle konzentriert. Im vorliegenden hitech präsentieren wir einige aktuelle Projekte und Arbeiten, die in diesem Themenbereich angesiedelt sind.

Security & Privacy ist insbesondere auch das grundlegende Element für erfolgreiche Unternehmen in den Wachstumsbereichen E-Business, E-Commerce, E-Government etc.; ohne den Enabler Security & Privacy kann hier kein Erfolgsmodell gebaut werden. Während wir in der Schweiz zum Beispiel beim Thema Datenschutz schon auf gutem Weg sind, ist dies in anderen Staaten nicht immer so ausgeprägt der Fall. In einer mehr und mehr international vernetzten (Geschäfts-)Welt sind wir aber je länger, je mehr darauf angewiesen, dass auch auf transnationaler Ebene gewisse Grundsätze in diesem Bereich garantiert werden können.

Security & Privacy dans le «Cloud»

En informatique, le mot-clé «Cloud Computing» est le résultat d'un vrai battage publicitaire. Le Cloud Computing décrit typiquement la situation où l'on n'exploite plus localement les logiciels ni l'équipement informatique; ceux-ci sont mis à disposition dans le «Cloud» par un prestataire de service, et sont donc liés par réseaux, typiquement par internet. Les avantages d'un tel système sont évidents: payement du service par utilisation, moins de ressources locales, utilisation durable et efficace de l'infrastructure, etc. Toutefois, les inconvénients sont eux aussi très nombreux, spécialement dans le domaine de Sécurité et Confidentialité. En voici quelques-uns: quand les données se trouvent à quel endroit dans le «Cloud», c'est-à-dire sur quel serveur situé dans quel pays ? Quelle protection des données est assurée ? Qu'en est-il des aspects juridiques dans tout cela ? Selon le contexte de l'application, de multiples questions variées attendent une réponse satisfaisante (cf. article d'E. Benoist, p. 16), spécialement aussi dans le domaine du Profiling et du Data Mining.
Dans la recherche cryptologique, des progrès intéressants ont été faits dans le contexte de la cryptographie homomorphe sous addition et multiplication qui permet des calculs chiffrés sûrs malgré une infrastructure peu sûre. Cependant, dans la pratique, ces résultats sont loin d'être applicables.
Dans le même contexte, les dangers et donc les attaques potentielles qui résultent de la mobilité informatique croissante des clients, comme laptops, téléphones mobiles, etc., sont encore loin d'être pris en compte de manière suffisamment sérieuse (cf. article d'U. Fiedler, p. 14).

Implantierbare medizinische Bauteile

Bezogen auf den Menschen und seinen Körper wird uns das Thema Security & Privacy wohl im Bereich der implantierbaren medizinischen Bauteile und der dazugehörigen Herausforderungen «hautnah» beschäftigen. Beispielsweise können aus gewissen implantierten Herzschrittmachern bereits heute via kontaktloser Kommunikation statistische Daten ausgelesen werden. Einerseits können Angriffe auf solche Bauteile lebensbedrohend sein oder einen grösseren Eingriff in die Privatsphäre darstellen, andererseits ist die Möglichkeit des Datenaustauschs natürlich für verschiedenste Anwendungen unabdingbar und insbesondere auch im Interesse und zum Wohle des Patienten.

«Protecting implantable medical devices against attack without compromising patient health requires balancing security and privacy goals with traditional goals such as safety and utility.»
D. Hailperin et al., «Security and Privacy for Implantable Medical Devices», in IEEE Pervasive Computing, vol. 7(1) 2008.

Im Rahmen des EU-Projekts FIDIS Future of Identity in the Information Society (FP6) wurden unter Mitarbeit der BFH-TI neben den rein technisch-informatischen Problemen auch die rechtlichen, ethischen und sozialen Aspekte dieser Probleme diskutiert und in «A Study on ICT Implants» publiziert (siehe www.vip.ch > Publications). ■

Kontakt:
> bernhard.anrig@bfh.ch
> Infos: www.vip.ch

«Can't say. It's private.»

Gregor Nyffeler : L'informatique est un service qui doit s'adapter à son environnement.

Gregor Nyffeler est le responsable des services informatiques de la HESB. Il s'est diplômé en biologie à l'Université de Berne, tout en se spécialisant et en travaillant en informatique. Après avoir suivi une formation en System Engineering, il a travaillé dans l'économie privée, dans deux branches complètement différentes, parce qu'il aime découvrir de nouveaux milieux. Le vaste environnement de la HESB est son domaine d'investigation depuis trois ans.

Monsieur Nyffeler, la situation actuelle des services informatiques de la HESB peut-elle être optimisée ?
Je pense que l'hétérogénéité, qui est une force de la HESB, peut devenir une faiblesse dans le domaine des prestations de services. Actuellement, à la centrale, mon équipe est composée de 15 personnes ; mais chaque département de la HESB a aussi son service informatique. Tous ont déjà entendu parler du grand projet de réorganisation, Zeno, qui est en phase d'élaboration : il s'agit d'unir et de centraliser les prestations de services, le controlling des finances, l'administration des étudiant-e-s, les ressources humaines et les services IT. Zeno est un projet ambitieux, qui exige beaucoup de changements. Cependant il ne s'agit pas d'affirmer que tout ce qui existait était mauvais, mais plutôt qu'il y avait un déficit et un potentiel. La technologie et les interconnections existantes étaient et sont d'un très bon niveau et il faut les maintenir, tout en accroissant leur vitesse et leur flexibilité.

Informatique implique circulation de données. Circulation de données implique problèmes de sécurité. Qu'est-ce que cela signifie pour une HES ?
La sécurité IT est un sujet important qui n'a pas seulement à faire avec la technologie, c'est un problème de conscience et de processus. En effet, bien qu'on puisse se sécuriser et protéger par la technologie, aucun système n'est aussi efficace que la conscience de chacun-e. Ici, il reste beaucoup à faire. Je pense que les écoles supérieures en général ont des défis à relever dans le domaine ICT pour garder l'équilibre entre ouverture, flexibilité, liberté de recherche et une certaine protection et sécurité IT. Il ne faut pas en faire trop, ni trop peu. Nous ne sommes pas une banque, mais une école. Nous, nous voulons maintenir une certaine liberté, mais nous avons, dans notre environnement, des résultats passionnants de recherches et d'autres données sensibles que nous nous devons de protéger en conséquence. Pour nous, le défi réside surtout dans le fait que l'environnement bouge et change. Par ex., les étudiant-e-s utilisent toujours plus d'appareils tiers. Comme c'est leur laptop, nous n'avons pas ou peu la possibilité d'intervenir sur cette machine. Cela signifie que nous devons protéger nos prestations de services tout en permettant à d'autres appareils de communiquer avec notre environnement sans nous porter préjudice.

Gregor Nyffeler
Responsable des services informatiques à la Haute école spécialisée bernoise (HESB-ITS)
Photo : Tobias Gerber

Estimez-vous que vos interventions contre la criminalité cybernétique sont suffisantes ?
Pas encore, même si nous avons aujourd'hui déjà beaucoup de possibilités internes à ce niveau et qu'il y a aussi de très bons mécanismes entre les Hautes écoles.
L'année prochaine, nous développerons un projet pilote concernant les systèmes de network access control. Dans le département TI, des travaux de diplôme s'y réfèrent déjà. Sur la base de ces travaux de diplômes, nous essayerons de construire un système prototype à même de surveiller notre environnement de manière proactive. Dans cette première phase, nous allons rassembler des expériences et il y aura probablement des choses qui ne fonctionneront pas comme nous le souhaitons et peut-être des blocages. Cependant, nous devrons y parvenir sans que notre institution, nos prestations de services, le travail des collaborateur-trice-s, des professeur-e-s et des étudiant-e-s n'en soient entravés.

Est-ce que notre école a subi des attaques cybernétiques criminelles importantes, par exemple d'espionnage de projets ?
Ce serait bien si nous pouvions le dire, parce qu'ainsi il serait vraiment urgent d'agir! Non, je ne connais pas de cas d'espionnage de données de recherche enregistrées à la HESB. Mais cela ne veut pas dire qu'il n'y en ait jamais eus. Aujourd'hui, l'intention d'un bon espion est d'entrer dans un système informatique et d'emporter les informations sans que personne ne le remarque. C'est pour cette raison que je pense que nous devrons investir plus d'énergie, de personnel, de ressources dans ce domaine pour être sûrs qu'il n'arrive rien.

Les étudiant-e-s ne devraient-ils pas être sensibilisé-e-s aux problèmes de la sécurité avant d'entrer dans notre école ?
Je pense que c'est différent d'une section à l'autre et que beaucoup de personnes, même si elles manient avec soin les appareils et l'ICT security, ne sont pas toujours conscientes de tout ce qui se passe dans l'Internet. Quand on réalise comment la criminalité cybernétique se professionnalise, il est toujours plus difficile en tant qu'utilisateur conscient de ne pas tomber dans l'excès de précautions. Maintenant, les pirates n'envoient plus seulement des spams dont le texte est illisible, ils pratiquent en arrière fond le social engineering pour nous connaître et nous extirper de l'argent ou des connaissances ou d'autres informations qu'ils vendront ou exploiteront ensuite. Par chance, en tant que Haute école, nous ne sommes pas au centre de l'attention de ces criminels. ■

Interview et texte: Gabriella Scorrano

Berner Fachhochschule setzt auf Sicherheit im Internet

Das Internet ist immer mehr ein Tummelplatz für kriminelle Elemente. Hacker sabotieren Steuersysteme von Industrieanlagen und Verkehrsleitsystemen, täuschen falsche Webseiten vor und schleusen Würmer und Trojanische Pferde in unsere Rechner. Damit solch verbrecherische Attacken nicht unsere Wirtschaft lahmlegen, entwickeln Experten innovative Sicherheitssysteme.

Prof. Dr. Endre Bangerter
RISIS, Security Engineering Lab
Foto: www.arteplus.ch

Schutz im Web dank raffinierter Hightech

Ein Beispiel dafür ist das Labor für Sicherheitstechnik (Security Engineering Lab SEL) an der BFH-TI in Biel unter der Leitung von Dr. Endre Bangerter. Seine Forschungsschwerpunkte liegen auf der Kryptographie und der Malwareanalyse. Unter Kryptographie versteht man die Wissenschaft von der Ver- und Entschlüsselung von Daten mit mathematischen Verfahren zur Datensicherung. Mit theoretischen und praktischen Forschungsarbeiten will das SEL-Team Krypto-Protokolle sicher in Rechner implementieren. Im internationalen CACE-Projekt (Computer Aided Cryptographic Engineering), mitfinanziert von der EU, tüfteln er und sein Team zusammen mit 12 Partnern aus 9 Ländern an der Automatisierung von Design und Implementierung kryptographischer Protokolle und Systeme für Computernetze (siehe Beitrag S.12).

Im Fokus Malware geht es um so genannte Schadprogramme wie Viren, Würmer und Trojaner, die ein wachsendes Sicherheitsproblem sind. «Entwickelten früher Freaks Malware, um ihre technischen Fähigkeiten zu beweisen, stellen wir seit etwa dem Jahr 2004 eine zunehmende Kriminalisierung fest», kommentiert Endre Bangerter. «Mit Malware lässt sich Geld verdienen, beispielweise mit Angriffen auf E-Banking, mit dem Diebstahl und Missbrauch von Kreditkartendaten». Heutige Cybercrime-Gangs weisen Strukturen und «Wertschöpfungsketten» auf, die durchaus mit dem Banditentum im Drogenhandel vergleichbar sind. Zwar bieten Antiviren-Programme einen gewissen Schutz, doch sind sie nicht unfehlbar, und so wird Malware oft gar nicht oder zu spät erkannt. Grund dafür ist einerseits die immens grosse Anzahl von Malware, die täglich neu freigesetzt wird, anderseits lässt sich Malware nicht so leicht erkennen. Eine Lösung des Problems ist laut dem Professor für IT Security nicht in Sicht.

Schadprogramme unter der Lupe

Will man Malware erfolgreich bekämpfen, muss man sie zuerst analysieren. Das heisst, es gilt zu verstehen, wie sie funktioniert, also beispielsweise zu wissen, welche Daten gestohlen und an wen weitergeleitet werden, wie sie sich verbreitet, auf welche Art sie sich in ein System einnistet. Verschiedene Firmen befassen sich mit der Analyse, besonders Antiviren-Experten, aber auch CERTs (Computer Emergency Response Teams) von Regierungen, Banken und Grossunternehmen.

Malwareanalyse ist eine aufwändige und komplexe Aufgabe, denn Malware beinhaltet zunehmend Funktionalität, um sich einer Analyse zu entziehen oder sie zumindest zu erschweren. Viele Malware ist verschlüsselt, der Schadcode lässt sich selbst von Fachleuten nicht ohne weiteres einsehen und analysieren: Sie entschlüsselt sich erst bei der Ausführung. Doch führt kein Weg an der Analyse vorbei, um die Auswirkungen und den Schaden einer Malware abschätzen sowie Abwehrmassnahmen ergreifen zu können.

Das Malware-Team am Security Engineering Lab entwickelt dafür verschiedene Tools und Techniken zur effizienten Malwareanalyse. So realisierten die SEL-Forscher im Lugh-Projekt ein Werkzeug, das Malware vollautomatisch entschlüsselt und sie somit wieder der Analyse zugänglich macht. Wie erste Experimente zeigen, kann das entwickelte Werkzeug eine grosse Zahl verschlüsselter Malware erfolgreich knacken. Da die Software sehr effizient arbeitet und Malware in kurzer Zeit entschlüsselt, eignet sie sich für die Massenanalyse von Schadprogrammen. Inzwischen ist die SEL-Entwicklung bei Schweizer Sicherheitsexperten auf Interesse gestossen. Die Berner Dreamlab Technologies AG, ein auf IT Security spezialisierter und international ausgerichteter Solution-Provider, will mit der Berner Fachhochschule – vermutlich in einem Projekt der Förderagentur für Innovation KTI – das Tool weiter entwickeln und kommerzialisieren (siehe Beitrag S.11).

Schnittstelle zwischen Forschung und Beratung

Für die auf Grundlagenforschung basierenden SEL-Aktivitäten bringt Endre Bangerter den geeigneten Rucksack an Erfahrungen mit. Seine Dissertation verfasste er in der Gruppe für Sicherheitsforschung beim IBM Zurich Research Lab gemeinsam mit den Forschern für Systemsicherheit der Ruhr Universität in Bochum. Dann nahm er Einblick in die industrielle Praxis als technischer Berater für Accenture, dem weltweit tätigen Managementberatungs-, Technologie- und Outsourcing-Dienstleister, sowie bei IBM Global Services. «Die Schnittstelle zwischen Grundlagenforschung und angewandter Forschung und Entwicklung bietet eine interessante Herausforderung», urteilt der international aktive Fachmann für Computerwissenschaft, welcher mit der Gründung des Instituts für Sicherheitstechnik RISIS dieser Kompetenz an der Berner Fachhochschule mehr Visibilität verleihen will. «Wir beraten industrielle Partner in IT-Sicherheit, ohne dabei bestehende Consulting-Firmen zu konkurrieren, können dank unserem Background aus der Grundlagenforschung hoch spezialisiertes Know-how anbieten.»

Die IT Security hat auch in der Ausbildung am Departement für Technik und Informatik an der BFH ein besonderes Gewicht. «Im Bachelor of Science für Informatik ist IT-Sicherheit einer der vier Schwerpunkte», betont der Forscher. «So verlassen doch pro Semester an die 20 – 30 Sicherheitsspezialisten die BFH-TI.» IT Security spielt ebenso im Rahmen des Master of Science in Engineering eine wichtige Rolle. Hierbei sind die Masterstudenten in verschiedene Security R&D Projekte eingebunden. ■

Kontakt:
> endre.bangerter@bfh.ch
> Infos: security.ti.bfh.ch

Text: Elsbeth Heinzelmann.
Journalistin Technik und Wissenschaft

Dr. Endre Bangerter: Kryptographie und Malwareanalyse im Security Engineering Lab SEL
Foto: Elsbeth Heinzelmann

Integrale Informationssicherheit

Die Sicherheitsspezialisten der Dreamlab Technologies AG bieten an der Berner Fachhochschule IT-Security-Zertifikatskurse an und arbeiten in gemeinsamen Forschungsprojekten mit. Kursteilnehmerinnen und -teilnehmer profitieren von der praktischen Erfahrung der Sicherheitsprofis, Forschende von der Industriepartnerschaft.

Nicolas Mayencourt
Inhaber & CEO Dreamlab Technologies AG
Foto: Dreamlab Technologies AG

Die Erfahrung von Dreamlab Technologies nutzen

«Ein integraler Ansatz, wie er von Dreamlab verfolgt wird», erklärt Nicolas Mayencourt, CEO von Dreamlab, «umfasst Informationssicherheit, Prozesssicherheit, Netzwerksicherheit, Kommunikationssicherheit, physische Sicherheit und auch menschliche Faktoren. Sicherheit spielt von der Vision bis zur Implementierung eine Rolle. Dreamlab Technologies hat für jeden einzelnen Schritt ein entsprechendes Angebot: Vom Audit über Consulting, Operations und Solutions bis hin zu Schulungen. An der Fachhochschule bringen wir unser Industriewissen und mehr als zehn Jahre Erfahrung mit ins Klassenzimmer.»

Wissen auf dem neusten Stand

«Wir sind überzeugt», so Mayencourt, «dass nur ein ganzheitlicher Ansatz zum Erfolg führen kann. Alles andere ist Symptombekämpfung. Um zukünftige Technologien bereits heute nutzbar zu machen, arbeiten wir deshalb in wichtigen internationalen Vereinigungen (W3C, OWASP, ISECOM) mit und kooperieren mit verschiedenen Bildungseinrichtungen. Diese Zusammenarbeit macht es möglich, dass wir stets auf dem neusten Stand des Wissens sind. Wir können Forschung, Praxis und offene Standards aufeinander abstimmen und damit auch die Zukunft mitgestalten.»

Forschen mit Industrieanschluss

Die IT-Security-Spezialisten von Dreamlab engagieren sich neben ihrer praktischen Tätigkeit in der Firma auch als Dozenten an der Fachhochschule und in gemeinsamen Forschungsprojekten. Mayencourt erklärt: «Dank dieser Partnerschaft können neueste Erkenntnisse rasch in die Praxis umgesetzt werden. Gegenwärtig entwickeln wir beispielsweise eine Malware-Analyse-Suite, die mit einem neuen Ansatz kryptographische Verfahren umgeht.»

Lernen von den Profis

Seit mehreren Jahren bieten die Experten von Dreamlab an der Berner Fachhochschule Zertifikatskurse für Security-Analyse und Security-Testing an. Ausserdem sind Zertifikatskurse für sichere Webentwicklung im Angebot und der Bereich «Offensive Security» wird neu aufgebaut. «Wir sind», erklärt Mayencourt, «davon überzeugt, dass Wissen allen zugänglich gemacht werden sollte. Das ist auch der Grundsatz von offenen Standards, wie wir sie verwenden und mitprägen. Nur eine aufgeklärte, wissende Gesellschaft ist auch frei und unabhängig. Dafür setzen wir uns ein.» ■

Kontakt:
> contact@dreamlab.net
> Infos: www.dreamlab.net und www.ti.bfh.ch

DREAMLAB
TECHNOLOGIES
Nicht glauben. Wissen.

CACE: Der Weg in eine sicherere Zukunft

Fehlerhafte Implementierungen sicherheitsrelevanter Software sorgen immer wieder für negative Schlagzeilen. Im Rahmen des CACE-Projekts versuchen Mitarbeitende der BFH-TI im Security Engineering Lab solche Probleme zu lösen, indem sie Programmierer kryptographischer Anwendungen durch entsprechende Zusatzsoftware unterstützen.

Stephan Krenn
Dipl.-Ing., Assistent RISIS, Security Engineering Lab und Doktorand an der Universität Fribourg
Foto: www.arteplus.ch

In den vergangenen 30 Jahren haben sich computergesteuerte Geräte zu unverzichtbaren Hilfsmitteln unserer Gesellschaft etabliert: Computer, Handys und Digitalkameras sind aus Haushalten nicht mehr wegzudenken. Gemeinsam mit ihrer steigenden Verbreitung und der Bereitschaft, auch persönliche Daten mit diesen Geräten zu verwalten, steigt auch die Notwendigkeit, diese Daten vor fremden Zugriffen zu schützen.
Oft ohne sich dessen bewusst zu sein, verwendet fast jeder Benutzer elektronischer Geräte täglich krytographische Techniken, um den Schutz seiner Privatsphäre zu garantieren: Die Kryptographie (oder auch Wissenschaft der Verschlüsselung) erlaubt es, verschlüsselte E-Mails zu senden und zu empfangen, bargeldlos im Supermarkt zu bezahlen, Bankgeschäfte über das Internet zu erledigen oder elektronische Ausweise wie den E-Pass sicher zu verwenden.

«Software is hard» (D. Knuth)

Das Programmieren hochwertiger Software ist für sich genommen bereits eine Herausforderung. Selbst weit verbreitete und teure Software enthält Fehler, welche zu inkorrektem Verhalten von Anwendungen führen können. Das kryptographisch sichere und zugleich effiziente Realisieren von Anwendungen verlangt Entwicklern jedoch neben Programmierkenntnissen zusätzlich umfangreiches Wissen aus der Mathematik und Elektrotechnik ab. Diese erlauben es, sowohl die theoretische als auch die praktische Sicherheit kryptographischer Implementierungen sicherzustellen. Man könnte obiges Zitat des renommierten Computerwissenschaftlers Donald Knuth also durch «Crypto software is even harder» ergänzen.

Teure Fehler

Durch mangelndes Verständnis komplexer Zusammenhänge in Protokollen und durch Programmierfehler entstehen immer wieder Sicherheitsprobleme mit weitreichenden Konsequenzen.
So entstanden zum Beispiel laut Medienberichten im Frühjahr 2008 dem Westschweizer Unternehmen Kudelski Kosten in Millionenhöhe, als die von ihm entwickelte Verschlüsselungstechnik für Bezahlsender geknackt wurde.
Ein Fehler in der Implementierung des GPG E-Mail-Verschlüsselungssystems ermöglichte 2004 Angriffe auf die Privatsphäre von Anwendern. Grund dieses Problems war eine inkorrekte Optimierung des Systems: Um die Geschwindigkeit zu erhöhen, wurden sensible Sicherheitsparameter verändert.
In der für sichere Internetverbindungen (https) häufig verwendeten OpenSSL-Implementierung wurden in den letzten Jahren immer wieder Schwachstellen entdeckt. Manche dieser Schwachstellen waren die Folge fehlerhafter Implementierungen und vermeintlicher Optimierungen. Eine andere Schwachstelle erlaubte, durch eine sogenannte Side-Channel-Attacke Rückschlüsse auf sensible Daten zu ziehen. Bei solchen Attacken werden physikalische Eigenschaften ausgenützt. Zum Beispiel variiert der Stromverbrauch des Prozessors für verschiedene Befehle leicht, oder das Durchführen bestimmter Rechenoperationen dauert länger als das anderer. Diese Unregelmässigkeiten können von Angreifern genutzt werden, um verwendete Schlüssel zu rekonstruieren.
All diese Beispiele zeigen, dass die Sicherheit von händisch implementierter Kryptosoftware oft auf Grund subtiler Fehler verletzt wird.

Lösung durch Automatisierung?

Das von der Europäischen Union geförderte Forschungsprojekt CACE (Computer Aided Cryptography Engineering) hat sich zum Ziel gesetzt, die Anforderungen an Entwickler sicherheitsrelevanter Software zu senken, und dadurch die Anzahl von Fehlern in kryptographischen Anwendungen zu verringern. Gemeinsam mit 11 namhaften Universitäten und Firmen wie Nokia entwickelt das Security Engineering Lab SEL an der Berner Fachhochschule in Biel Theorie und Software, um das Entwickeln und Überprüfen sicherheitsrelevanter Anwendungen zumindest teilweise zu automatisieren.
Dafür arbeiten fünf Arbeitsgruppen in verschiedenen kritischen Bereichen. Zwei dieser Arbeitsgruppen arbeiten auf einem maschinennahen Level und entwickeln Programme, welche es erlauben, hocheffiziente und gegen bestimmte Arten von Side-Channel-Attacken resistente Implementierungen zu erhalten. Dadurch werden insbesondere die notwendigen elektrotechnischen Anforderungen an Programmierer gesenkt.
Auf einem wesentlich abstrakteren Level arbeiten zwei weitere Arbeitsgruppen. Die von ihnen entwickelten Programme transformieren anwendungsnahe Problembeschreibungen automatisch in korrekte kryptographische Protokolle. Die betrachteten Anwendungen umfassen zum Beispiel elektronische Abstimmungsverfahren und anonyme Anmeldungsverfahren zu Online-Services.
Schliesslich entwickelt eine letzte Arbeitsgruppe Anwendungen, um die Korrektness der obigen Schritte auch formal sicherzustellen. Diverse Standards verlangen eine solche formale Verifikation zwingend, um Software für sicherheitskritische Bereiche freizugeben.

Das CACE-Projekt startete Anfang 2008 und endet mit Dezember 2010. Zum aktuellen Zeitpunkt sind die theoretischen Rahmenkonzepte weitgehend fertiggestellt, und Prototypen von den einzelnen Arbeitsgruppen entwickelten Programme stehen auf der Projekthomepage (siehe Infobox) zur Anwendung bereit. ■

Kontakt:
> stephan.krenn@bfh.ch
> Info: security.ti.bfh.ch/

Im Zuge des internationalen CACE-Projekts versuchen Forscher, das korrekte Realisieren kryptographischer Software zu automatisieren.

Der Weg in eine sicherere Zukunft
Foto: ©Sebastian Kaulitzki
©robinmac, fotolia

CACE-Projekt
(Computer Aided Cryptography Engineering)

Projektbeginn:	01.01.2008
Projektdauer:	3 Jahre
Teilnehmer:	12 Universitäten und Firmen aus 9 Ländern
Mehr Infos unter:	www.cace-project.eu

Sicherheit in Funknetzen

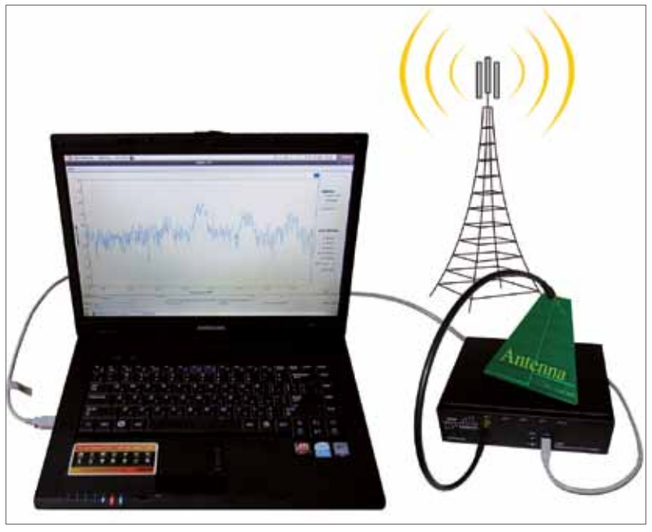
Täglich benutzen wir Laptops und Handys. Die Anbindung dieser Geräte über Funknetze und die damit verbundenen Bedrohungen nehmen wir aber kaum wahr.

Dr. Ulrich Fiedler
Professor für Informatik
Foto: www.arteplus.ch

Funknetze sind einfach zugänglich. Dies trägt nicht nur wesentlich zur breiten Nutzung dieser Netze bei, sondern öffnet verschiedensten Bedrohungen Tür und Tor. Abhören und unzulässiges Mitbenutzen ist vergleichsweise einfach.

WirelessLAN (WLAN)

WirelessLAN (WLAN) ist weit verbreitet. Ausser in Haushalten gibt es auch an Flughäfen, in Cafés und Hotels viele Zugangspunkte. Insbesondere bei privaten Zugangspunkten ist der Netzwerkverkehr oft unverschlüsselt und kann sehr einfach mitgehört werden.
Bei älteren Zugangspunkten ist der Netzwerkverkehr WEP-verschlüsselt. Diese Verschlüsselung hat eine Sicherheitslücke im Design des Protokolls. Im Versuch konnten wir den Schlüssel solcher Zugangspunkte mit einem Laptop stets innerhalb von weniger als zwei Minuten ermitteln.
Neuere Zugangspunkte benutzen die 2003 standardisierte WPA/WPA2-Verschlüsselung. Auch diese Verschlüsselung kann mit einer Dictionary-Attacke geknackt werden. Im Versuch gelang es uns den Schlüssel zu ermitteln, nachdem wir einen Ausschnitt aus dem Netzwerkverkehr von wenigen Megabytes aufgezeichnet hatten.
Der Erfolg dieser Attacke hängt davon ab, ob der Schlüssel im verwendeten Wörterbuch (Dictionary) verzeichnet ist. Aus diesem Grund bieten gewisse Internetdienste gegen eine geringe Gebühr von ca. 30 CHF eine umfassende Analyse von aufgezeichnetem Netzwerkverkehr an. Diese Dienste benutzen dann riesige Wörterbücher und Hunderte von Rechnern, um den Schlüssel mittels Cloud-Computing innerhalb weniger Stunden zu ermitteln.
Wir empfehlen daher für die WPA/WPA2-Verschlüsselung ein komplett zufälliges Passwort mit mindestens 20 Zeichen zu verwenden. Dieses Passwort sollte neben Buchstaben auch Zahlen und Sonderzeichen enthalten. Für Firmen empfiehlt sich zusätzlich ein Radius-Server.



Eine relativ einfache Ausrüstung genügt, um damit Handys in der Umgebung zu identifizieren.
Quelle: U. Fiedler

Mobilfunk (GSM)

Die meisten von uns haben ein Handy. Soll der Sprachverkehr auf ein solches Handy abgehört werden, z.B. zu Zwecken der Strafverfolgung, setzen die Sicherheitskräfte dazu sogenannte IMSI-Catcher ein. Ein solcher IMSI-Catcher gibt sich als Basisstation mit sehr grosser Sendestärke aus. In der Folge verbindet sich unser Handy zu dieser Basisstation und kann somit abgehört werden. Dies ist allerdings aufwendig.
Um ein Handy in der Umgebung zu identifizieren, genügt es bereits, den Kontrollverkehr zwischen der nächsten Basisstation und allen Handys in der Zelle dieser Basisstation mitzuhören. Aktiv in das Geschehen einzugreifen und den Sprachverkehr zu entschlüsseln ist dazu nicht nötig. Mit solchem passivem Mithören können alle Besitzer von Handys, die zu einem gewissen Zeitpunkt in der Nähe von sensitiven Orten, wie z.B. einem Juweliergeschäft oder einer Bank waren, im Nachhinein ermittelt werden. Dies könnte im Falle eines Vorfalls, wie z.B. einem Juwelen- oder Bankraub, von grossem Interesse sein.
Unsere Versuche zeigen, dass passives Mithören des Verkehrs von Basisstation zu Handy mit einem sogenannten Software-Radio sehr einfach möglich ist. Sobald das Handy angerufen wird, kann die durch den Anruf ausgelöste Kontrollmessage mitgehört werden. Diese Message enthält die IMSI, über welche die SIM-Karte im Handy identifiziert werden kann. Dies wiederum ermöglicht den Rückschluss auf den angerufenen Besitzer.
Mit wenig mehr Aufwand können wir auch den Verkehr vom Handy zur Basisstation mithören. Sobald ein Handy über Bereichsgrenzen hinweg bewegt wird, meldet es sich mit einer Kontrollmessage bei der neuen Basisstation an. Diese Message, welche die IMSI enthält, kann mitgehört werden. Über die IMSI kann die SIM-Karte identifiziert und ein Rückschluss auf den Besitzer gemacht werden, der sich über die Bereichsgrenzen hinweg bewegt hat. Relativ einfach kann zusätzlich abgeschätzt werden, ob das Handy in der Nähe ist.
Werden nun die mitgehörten IMSIs zusammen mit einer Abschätzung über den Ort und einem Zeitstempel aufgezeichnet, können damit sensitive Orte wie Juweliergeschäfte oder Banken geschützt werden.

Fazit

Abhören von Funknetzen ist einfach möglich. Verschlüsselungen auf WirelessLANs können oft mit geringem Aufwand geknackt werden. Für die moderne WPA2-PSK-Verschlüsselung wird dies sogar als Service im Internet angeboten.
GSM-Verkehr abzuhören ist möglich, aber aufwendig. Im Versuch konnten wir mit moderatem Aufwand Handys in der Umgebung identifizieren. ■

Kontakt:
> ulrich.fiedler@bfh.ch
> Infos: labs.ti.bfh.ch/wireless

WiressLAN (WLAN) Eine sehr einfache Ausrüstung genügt, um Standort und Verschlüsselung von WLAN-Zugriffspunkten zu ermitteln.
Quelle: U. Fiedler

Peut-on faire cohabiter secret médical et centralisation de données ?

Une équipe de la HESB-TI développe, en collaboration avec l'Institut IEFM de l'Université de Berne, le système MEMdoc[1]. Ce système web collecte des données médicales sur une très large échelle pour établir l'efficacité de traitements, de médicaments ou d'implants. Toutefois, dans le but de protéger le secret médical, les données complètes ne sont disponibles que dans le browser du médecin[2].

Prof. Dr. Emmanuel Benoist
RISIS, Web-Security Group
Photo : www.arteplus.ch

Quelle méthode est la plus efficace pour lutter contre votre mal de dos ? Quel type d'implant sera le plus efficace pour vous ? Pour répondre à ces questions, les médecins ont besoin de données précises et en grande quantité. Les observations à l'échelle d'un hôpital ou d'un canton même sur une longue période ne sont pas suffisantes. Dans le cadre d'un projet commun avec l'Institut pour la recherche évaluative en médecine (IEFM, en allemand) de la faculté de Médecine de l'Université de Berne, l'équipe dirigée par Emmanuel Benoist essaie de mettre en place un système informatique permettant la collection de telles données.

La gestion de qualité est un domaine absolument vital en médecine. Elle requiert une grande quantité de données. Elle permettra, entre autres, de déterminer si un produit nouveau est plus efficace que le produit sur le marché, ou de déterminer quels sont les «meilleurs» médecins ou hôpitaux selon des critères exclusivement scientifiques.

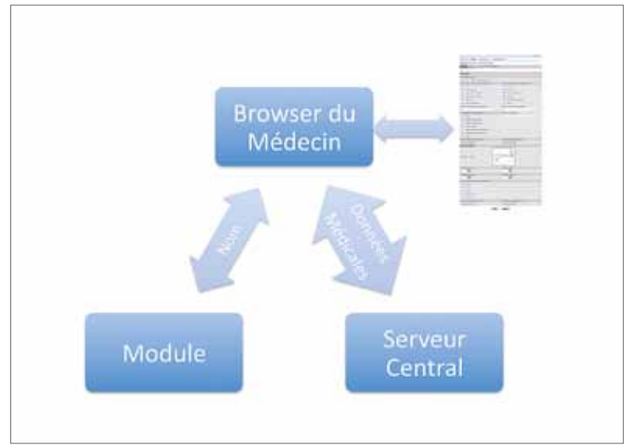
Collecter une grande quantité de données tout en respectant le secret médical.

Dans le cadre de la coopération avec l'équipe de l'Université de Berne dirigée par le Professeur Max Aebi, les informaticiens de la HES bernoise ont développé une solution novatrice permettant de rassembler une grande quantité de données tout en respectant le secret médical. La collection de données médicales requiert une attention toute particulière à tout ce qui concerne la protection des données. L'équipe a mis au point un système permettant la ségrégation des informations démographiques sur un serveur et des informations médicales sur un autre.

Le médecin a donc à disposition une page web se connectant d'un côté à un serveur central qui rassemble les données médicales arrivant du monde entier et d'un autre côté à un autre serveur (appelé module) qui rassemble, lui, uniquement les données relatives à l'identité du patient (nom, prénom, date de naissance, adresse, téléphone, ...). Les données ne sont combinées que dans le browser du médecin.

Quel a été le problème? La société a besoin de registres médicaux pour résoudre cette question.
Photo : IEFM

[1] Voir le site web http://www.memdoc.org
[2] Le système décrit dans cet article fait l'objet de la demande de brevet EP09157735.3 du 9 avril 2009



Les données médicales et celles relatives à l'identité du patient ne sont regroupées que sur le browser du médecin.
Graphique : E. Benoist

L'idée dans cette architecture est que le module peut être placé n'importe où. Par exemple, certaines sociétés médicales mettent à disposition de leurs membres un module pour un pays. Mais dans certains cas, il faut un module par région. Certains hôpitaux, qui souhaitent préserver la confidentialité des dossiers médicaux, installent un module directement sur place. Dans ce cas, les données nominatives ne franchissent jamais les portes (ou plutôt le firewall) de l'hôpital.

La page web détermine automatiquement quelle information envoyer vers quel serveur.

L'architecture mise en place permet toutes ces combinaisons. Mais comme les médecins ne doivent pas être gênés dans leur travail, l'équipe a développé un système permettant de rendre cette ségrégation totalement transparente. Un médecin entre les données médicales et les données relatives à l'identité dans une même page. La page web détermine automatiquement quelle information envoyer vers quel serveur. De même, lorsque le médecin cherche un patient dont le nom commence par N et qui a été opéré de la hanche, des données provenant des deux serveurs doivent être mélangées. Tout ceci est fait en JavaScript directement à l'intérieur du browser du médecin, de sorte que ni le serveur central, ni le module n'aient à connaître les autres données.

Le module, qui peut être déployé partout dans le monde, est volontairement resté très petit et fonctionne en utilisant une combinaison Linux, Apache, MySQL et PERL. Le serveur, qui contient toute la partie complexe de l'application, a été programmé avec une solution Java basée sur Java Server Faces (JSF) pour la présentation, TopLink pour la partie persistance et Oracle pour la base de données.

Le temps des médecins étant très précieux (et cher), le système propose plusieurs aides à la saisie de données. Les données déjà présentes dans le système d'information de l'hôpital (CIS, en anglais) sont transférées automatiquement via un web service à la fois à un module et au serveur central, les données manquantes sont ensuite complétées à l'aide de l'interface web. Pour les registres les plus utilisés, les médecins peuvent utiliser un formulaire avec des cases à cocher (OMR - Optical Markup Reader) pour noter, dès la salle d'opération, les informations importantes. Cette feuille est ensuite scannée par quelqu'un d'autre (secrétaire/infirmière) qui n'a plus qu'à compléter les informations écrites à la main. Toutes les tentatives de reconnaissance automatique de l'écriture des médecins s'étant révélées infructueuses, cette solution est la seule permettant d'accéder aux champs textuels.

Le système MEMdoc a été créé pour gérer de très gros registres nationaux ou multinationaux. Il permet à chaque clinique de gérer elle-même les noms de ses patients si elle le souhaite, et offre donc une protection optimale de la sphère privée des patients. Elle permet cependant de centraliser rapidement une très grande quantité de données, et donc d'atteindre une taille critique pour des données statistiquement intéressantes. Combiner le besoin de secret médical d'un côté et le besoin d'études très larges est actuellement un des gros challenges de la médecine moderne, l'évaluation de la qualité d'une thérapie, d'un produit et même d'un hôpital ou d'un médecin devenant obligatoire en ces temps d'explosion des coûts médicaux. ■

Contact :
> emmanuel.benoist@bfh.ch
> infos : www.memdoc.org.

E-Voting – Risiko oder Chance?

Abstimmen und Wählen mit dem Stimmzettel im Wahllokal ist einfach und sicher. Um die gleiche Sicherheit bei der elektronischen Umsetzung zu erreichen, muss aufwändige Kryptographie eingesetzt werden. Im Gegenzug wird das Abstimmungs- und Wahlverfahren für die Stimmbürgerinnen und Stimmbürger transparenter.

Prof. Dr. Eric Dubuis
RISIS, E-Voting Group
Foto: www.arteplus.ch

Prof. Dr. Stephan Fischli
RISIS, E-Voting Group
Foto: Kathrin Blumenthal

Prof. Dr.Rolf Haenni
RISIS, E-Voting Group
Foto: www.arteplus.ch

Die rasanten Entwicklungen der Informationstechnologien verändern viele Bereiche des täglichen Lebens. Sie betreffen zunehmend auch den Informationsaustausch zwischen Bürgern und Behörden. Vor diesem Hintergrund hat man sich in der Schweiz vor Jahren entschlossen, das Abstimmen und Wählen zukünftig auch mittels elektronischer Verfahren anzubieten. In den Kantonen Genf, Neuenburg und Zürich wurden drei E-Voting-Pilotprojekte gestartet, die mehrfach bei Abstimmungen und Wahlen eingesetzt wurden. Die Schweiz nimmt damit weltweit eine Pionierstellung ein.

Einfache Anforderungen – einfacher Prozess

Das Wählen und Abstimmen gehört zu den Grundrechten der Bürgerinnen und Bürger einer Demokratie und ist in entsprechenden Verfassungs- und Gesetzestexten verankert. Aus diesen ergeben sich folgende Grundprinzipien:

- Nur berechtigte Personen dürfen stimmen.
- Eine berechtigte Person kann maximal eine Stimme abgeben.
- Jede korrekt abgegebene Stimme wird gezählt.
- Die Stimme ist geheim.
- Das Resultat bleibt bis zum Ende der Wahl oder Abstimmung geheim.

Diese Grundprinzipien lassen sich mit Papier und dem klassischen Wahllokal einfach bewerkstelligen. Der Ablauf, welcher von Wahlbeobachtern oder interessierten Stimmbürgern überwacht werden kann, lässt sich in drei Phasen aufteilen:

- In der ersten Phase werden mit dem Stimmregister die Stimmberechtigten festgelegt, die Stimmausweise gedruckt und den Stimmbürgerinnen und -bürgern verschickt.
- In der zweiten Phase geben die Stimmberechtigten ihre Stimme im Wahllokal ab (siehe Abbildung 1). Dabei belegt der Stimmausweis, dass eine Person berechtigt ist, an der Wahl teilzunehmen. Das Stimmgeheimnis wird durch das Ausfüllen des Stimmzettels in der Wahlkabine gewahrt, und der Wahlhelfer bei der Urne garantiert schliesslich, dass jede bzw. jeder Stimmberechtigte nur eine Stimme in die Urne legt.
- Nach Ablauf des Wahl- oder Abstimmungsvorgangs wird durch die Mitglieder der Wahlkommission der Inhalt der Urne gezählt und das Ergebnis publiziert.

Abbildung 1
Der/die Stimmberechtigte gibt den Stimmausweis dem Wahlhelfer ab (1). Danach geht er/sie in die Wahlkabine (2), füllt einen leeren Stimmzettel aus, faltet ihn und verlässt die Wahlkabine. Er/sie geht zur Urne und legt den Stimmzettel hinein (3) und verlässt danach das Wahllokal.
Grafiken:
E-Voting Group

Mit dem Internet wird es viel schwieriger

Das Abstimmen übers Internet macht alles viel komplizierter. Wir greifen zwei Probleme heraus. Das erste ist die scheinbare Unvereinbarkeit des Stimmgeheimnisses mit der Forderung, dass nur berechtigte Personen stimmen dürfen. Denn um letzteres zu erreichen, muss das Wahlsystem den Stimmbürger zuerst eindeutig identifizieren. Das Wahlsystem «kennt» also den Stimmbürger oder die Stimmbürgerin und kann somit die abgegebene Stimme mit der entsprechenden Identität verknüpfen. Gerade dies muss aber verhindert werden, um das Stimmgeheimnis zu wahren. Wie aber kann man die Identität der Stimmberechtigten von der jeweiligen Stimme entkoppeln?
Das andere Problem ist, dass das Wahlsystem und seine Betreiber erst in der dritten Phase wissen dürfen, welche Stimmen abgegeben wurden. Dies bedeutet, dass bis zu diesem Zeitpunkt die Stimmen verschlüsselt bleiben müssen. Wie kann dies sichergestellt werden, und welche Schlüssel sollen dafür verwendet werden?

Ein Ziel – zwei Lösungsansätze

Für diese Probleme gibt es zwei Lösungsansätze. Der erste wurde bei den in der Schweiz eingesetzten Wahlsystemen verfolgt: Man baut ein Wahlsystem, betreibt es an einem sicheren Ort, und die Stimmberechtigten bringen den Betreibern das entsprechende Vertrauen entgegen.
Beim anderen Lösungsansatz wird fortschrittlichste Kryptographie eingesetzt. Damit kann man nicht nur die obigen Probleme lösen, sondern zusätzlich Transparenz für die Stimmberechtigten schaffen. Wir unterscheiden zwei verschiedene Verfahren:

- Beim Verfahren mittels blinder Signaturen (siehe Kasten «Blinde Signatur») erzeugt der/die Stimmberechtigte ein geheimes Pseudonym und lässt es von der Wahlbehörde blind signieren. Im zweiten Schritt verschlüsselt der/die Stimmberechtigte die Stimme und schickt sie, zusammen mit dem signierten Pseudonym, an die öffentlich einsehbare Urne; den Schlüssel schickt er/sie an den Kollektor (eine Art Schlüsselbrett). Am Ende des Wahlvorgangs werden die Stimmen mit den Schlüsseln des Kollektors entschlüsselt und gezählt. Das Ergebnis kann von allen Beteiligten verifiziert werden (siehe Abbildung 2).
- Beim Verfahren mittels homomorpher Verschlüsselung (siehe Kasten «Homomorphe Verschlüsselung») macht man sich erst gar nicht die Mühe, die Stimme vom Stimmenden zu trennen. Die Stimme wird vom Stimmenden verschlüsselt – und bleibt verschlüsselt, auch beim Zählen (siehe Abbildung 3).

Stand unserer Arbeiten und Ausblick

Im Projekt TrustVote entwickelten wir einen Prototyp auf der Basis der blinden Signaturen. Eine Weiterentwicklung soll den Einsatz für eine reale Abstimmung (z.B. eine studentische Wahl im Kontext einer Hochschule) ermöglichen. Gegenwärtig befassen wir uns mit den homomorphen Verfahren. Unser Ziel ist, diese praktisch umzusetzen und in zukünftige Wahlsysteme einfliessen zu lassen. ■

Kontakt:
> eric.dubuis@bfh.ch
> Infos: e-voting.ti.bfh.ch

Blinde Signaturen

Möchte jemand ein Dokument signieren lassen, ohne dessen Inhalt preiszugeben, so steckt er das Dokument mit einem Durchschlagpapier in einen verschlossenen Umschlag und lässt diesen signieren. Das Durchschlagpapier bewirkt, dass die Unterschrift auf das Dokument übertragen wird, so dass nach dem Entfernen des Umschlags das signierte Dokument vorliegt. In der Kryptographie wird dieses Prinzip durch sogenannte «blinde Signaturen» nachgebildet. Dabei wird zunächst eine «Verblindung» durchgeführt, welche das zu signierende Dokument unkenntlich macht (entspricht dem Umschlag). Dann wird das «verblindete» Dokument signiert. Durch das «Entblinden» (Entfernen des Umschlags) erhält man das mit der Unterschrift versehene Dokument zurück.

Homomorphe Verschlüsselung

Um das Gewicht von zwei Äpfeln zu bestimmen, kann man entweder beide Äpfel einzeln wägen und die Gewichte zusammenzählen, oder man kann beide Äpfel gemeinsam auf die Waage legen. Beim Wägen von Äpfeln handelt es sich also um eine «additiv homomorphe Funktion», bei welcher es keine Rolle spielt, ob man zuerst die Funktion berechnet und dann zusammenzählt oder zuerst zusammenzählt und dann die Funktion berechnet. In der Kryptographie gibt es Verschlüsselungsfunktionen, die genau diese Eigenschaft besitzen. Diese kann man verwenden, um die Summe von verschlüsselten Zahlen zu bestimmen, ohne die einzelnen Zahlen zu entschlüsseln.

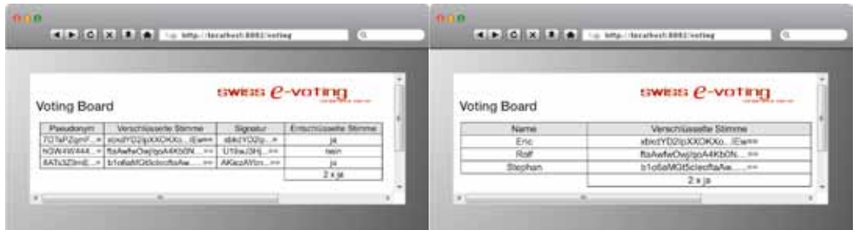


Abbildung 2
Nach Abgabe ihrer Stimme können die Stimmberechtigten das öffentliche Anschlagbrett anschauen, auf dem sie ihr Pseudonym und ihre verschlüsselte Stimme finden. Die Spalte «Entschlüsselte Stimme» ist noch leer. Die Signaturen der Wahlbehörde garantieren, dass nur Stimmen von Stimmberechtigten vorhanden sind. Nach der Abstimmung werden die Stimmen mit den Schlüsseln des Kollektors entschlüsselt, und jedermann kann das Ergebnis ermitteln.

Abbildung 3
Bei dieser Variante des Anschlagbretts wird die verschlüsselte Stimme mit dem Namen des/der Abstimmenden veröffentlicht. Dank der homomorphen Verschlüsselung bleibt aber die Stimme für immer verschlüsselt. Am Ende wird nur die Summe der verschlüsselten Stimmen entschlüsselt und publiziert.

SuisseID – Der digitale Identitätsträger der Zukunft

Die SuisseID soll ab Mai 2010 das erste standardisierte Produkt für den sicheren elektronischen Identitätsnachweis werden. Damit sollen künftig Geschäfte von Privatpersonen zu Firmen, von Firmen untereinander sowie vom Bürger zur Verwaltung direkt über das Netz sicher abgeschlossen werden können.
Das Staatssekretariat für Wirtschaft (SECO) – verantwortlich für die Einführung der SuisseID – hat das e-Government Kompetenzzentrum der BFH beauftragt in Zusammenarbeit mit dem Departement TI einen Vorentwurf des geplanten SuisseID-Zertifikatinhalts mit ähnlichen Produkten anderer europäischer Länder zu vergleichen und zu bewerten. Im folgenden Artikel sollen die Eigenschaften der SuisseID näher vorgestellt werden.

Prof. Gerhard Hassenstein
Dozent für Internet Security
Foto: Kathrin Blumenthal

Die SuisseID ist eine Infrastruktur, welche künftig von **ZertES**[1] **anerkannten Anbietern**[2] **von Zertifizierungsdiensten (CSP**[3]**)** bereitgestellt werden kann. Sie besteht grundsätzlich aus:

- einem sicheren Datenträger (Token), ausgestellt für eine natürliche Person mit folgendem Zertifikat-Set:
  - einem **ZertES-konformen Zertifikat (QC)**, um damit Dokumente elektronisch und rechtsverbindlich unterschreiben zu können.
  - einem **standardisierten Authentisierungs-Zertifikat (IAC)**, welches vom Inhaber zur sicheren Authentisierung gegenüber Online-Services, sowie zum Signieren von E-Mails verwendet werden kann.
- einer **eindeutigen SuisseID-Nummer**
- einem nur vom SuisseID-Inhaber abrufbaren **Identity-Provider-Service (IdP)**, welcher zusätzliche Daten liefert, die im Zertifikat nicht eingetragen sind (Geburtsdatum, Bürgerort, Funktionsbezeichnung gemäss Handelsregister usw.)

[1] ZertES «Bundesgesetz vom 19. Dezember 2003 über die elektronische Signatur»
[2] Die vier Anbieter: Bundesamt für Informatik und Telekommunikation (BIT), Quo Vadis, Swisscom und die Schweizerische Post / SwissSign
[3] Certification Service Provider

Was muss ich mir unter einem SuisseID-Token vorstellen?

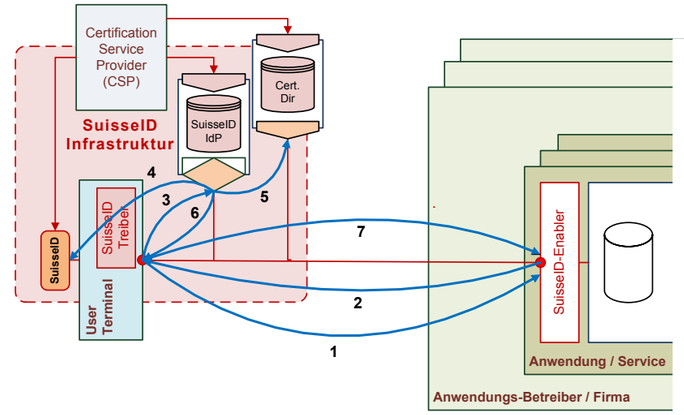
Der Träger (USB-Stick oder SmartCard) beinhaltet immer das gesamte Zertifikats-Set und muss gemäss Verordnung strengen Sicherheitsstandards bezüglich Zugangs-, Fälschungs- und Kopiersicherheit entsprechen. Alle administrativen Operationen – wie die Ausgabe, Sperrung und Erneuerung der SuisseID – müssen immer auf beide Zertifikate (QC und IAC) angewandt werden. Die physische und visuelle Ausgestaltung des Trägers ist dem CSP überlassen.

Was werde ich als Besitzer mit meinem SuisseID-Token machen können?

- Die SuisseID dient nicht der Identifikation einer Person, wie ein amtlicher elektronischer Identitätsausweis (eID oder ePass), sondern ermöglicht es dem Inhaber sich gegenüber einer breiten Palette von staatlichen und privaten Anwendungen sicher elektronisch zu authentisieren.
- Mit dem SuisseID Signatur-Zertifikat nach ZertES (QC) können Dokumente elektronisch signiert werden, was gemäss OR der eigenhändigen Unterschrift gleichkommt.

Abbildung 1:
SwissID-Token
Quelle: SECO

Abbildung 2:
Die SwissID-Authentizierungsarchitektur
Quelle: SECO



- Das Zertifikats-Set (QC und IAC) der SuisseID erlaubt E-Mails zu signieren, jedoch nicht die Verschlüsselung von E-Mails. Ein CSP kann aber für diesen Zweck ein dafür geeignetes Verschlüsselungs-Zertifikat einem SuisseID-Token hinzufügen.

Welche Benutzerinformationen werden auf dem SuisseID-Token gespeichert?

Nebst vielen rein technischen Definitionen müssen beide SuisseID-Zertifikate eine **SuisseID-Nummer** (eine eindeutige, durch den CSP vergebene Nummer) beinhalten und das Feld SubjectDN mit der eigentlichen Namensgebung. Der Subject DN darf minimal den **Namen des Zertifikatsinhabers (CN)** oder ein **Pseudonym** enthalten. Es ist dem Benutzer und dem CSP überlassen, weitere standardisierte Attribute der Inhaberin oder des Inhabers dem SubjectDN hinzuzufügen.

Attribute im SubjectDN

CN = Hans Muster oder
pseudonym = Mein Name ist Hase
serialNumber = 0001-9472-9142-8359
optional:

emailAddress	= hans.muster@bfh.ch
organization	= Berner Fachhochschule
organizationalUnit	= Administration
surname	= Muster
givenname	= Hans

Wie kann ich mich – als Besitzer einer SuisseID – gegenüber einer Anwendung (Service-Provider) sicher authentisieren?

In Abhängigkeit der Anforderungen eines Anwendungs-Betreibers können verschiedene Authentisierungsverfahren mit unterschiedlichem Datenfluss zum Einsatz kommen. Im einfachsten Fall muss zur Authentisierung nur das **Authentisierungs-Zertifikat (IAC)** eingesetzt werden. Diese Art eignet sich meistens dann, wenn bereits eine Vertrags- bzw. Vertrauensbeziehung (z.B. bei e-Banking) zwischen einem Kunden und einer Anwendung besteht. Beim Betreiber muss dazu die SuisseID des Benutzers vorgängig registriert werden.
Benötigt die Anwendung für die erstmalige Authentifizierung mehr identifizierende Merkmale (z.B. einen Altersnachweis), können diese Informationen vom zentralen **SuisseID Identity Provider (IdP)** angefordert werden (siehe Abbildung 2). Die Anwendung des Betreibers antwortet dabei auf einen Authentifizierungsvorgang (1) mit einer Profildaten-Bestätigungs-Anforderung (2). Diese wird vom Benutzer an den IdP weitergeleitet (3). Nach erfolgter Authentifizierung des SuisseID Benutzers (4) und Validierung seines Zertifikats (5), stellt der IdP die angeforderte Bestätigung zusammen. Der Benutzer lässt sich die von der Anwendung verlangten Attribute anzeigen und – falls er mit der Auslieferung einverstanden ist – vom IdP signieren (6). Im letzten Schritt sendet der Benutzer die gewünschte Bestätigung selbst an die Anwendung des Betreibers (7).

Wie steht es um den Schutz der persönlichen Daten?

Die SuisseID-Spezifikation ist darauf ausgelegt, die Anzahl identifizierender Attribute des Inhabers auf dem Träger selbst möglichst klein zu halten. Die Ausgabe zusätzlicher Merkmale oder weiterer persönlicher Informationen eines Benutzers erfolgt immer über den SuisseID-Inhaber selbst und mit dessen Einverständnis.
Die SuisseID-Nummer hat keine Referenz zu einem staatlichen Personenidentifikator wie z.B. der neuen Sozialversicherungsnummer. Die SuisseID-Zertifikate unterstützen die Verwendung von Pseudonymen in der Namensgebung (nur der IdP und der CSP kennen in diesem Fall den echten Namen zur SuisseID-Identität). Eine Person kann bei Bedarf mehrere SuisseIDs erwerben, um diese in verschiedenen persönlichen Kontexten einzusetzen.
Alle diese Eigenschaften sollen dem Benutzer grösstmögliche Flexibilität und Sicherheit im Umgang mit der SuisseID geben, bei gleichzeitig bestmöglicher Wahrung seiner Datenschutzinteressen. ■

Kontakt:
> gerhard.hassenstein@bfh.ch
> Infos: www.suisseid.ch

Aktuell (Stand 9. Januar 2010) haben sich ca. 80 Firmen verpflichtet als Anwendungs-Betreiber die SuisseID zu unterstützen. In einer ersten Phase des Projekts wird der SuisseID-IdP zusammen mit einem Toolkit für die Anwendungs-Betreiber (SuisseID Enabler) entwickelt. In einer weiteren Phase soll die hier vorgestellte Authentisierungsarchitektur durch eine **Claim Assertion Infrastructure (CAI)** erweitert werden. Damit können auch externe Quellen zur Bestätigung weiterer Eigenschaften (Befähigungen, Zulassungen, Berechtigungen) eines SuisseID-Inhabers einbezogen werden.

ID Quantique SA
Une entreprise au service de la confidentialité

L'essor des technologies de l'information a révolutionné l'organisation et le fonctionnement des entreprises en permettant la délocalisation de l'information, qui peut être traitée ou stockée dans différents sites de façon transparente. Cette évolution a été rendue possible par la mise en place de réseaux informatiques rapides et performants qui irriguent les entreprises. Mal maîtrisée, elle peut toutefois créer de nouveaux risques liés à la perte d'informations sensibles. Il existe, heureusement, des moyens qui permettent de garantir la confidentialité des informations véhiculées par ces réseaux informatiques.

Grégoire Ribordy
Directeur général, ID Quantique SA
Photo: ID Quantique SA

Les technologies de chiffrement consistent à combiner les informations sensibles avec une clé de chiffrement avant leur transmission. Un adversaire qui souhaiterait accéder à ces données chiffrées, mais ne connaîtrait pas la clé, n'aurait pas d'autre choix que d'essayer toutes les clés, une par une. Si la clé est suffisamment longue, le temps nécessaire pour réaliser une telle tâche devient si grand que l'on peut la considérer comme impossible. Quant au destinataire légitime de l'information, il dispose d'une copie de la clé et peut, donc, déchiffrer les informations et les rendre à nouveau intelligibles.
Dans un tel scénario se pose le problème de la distribution de la clé de chiffrement: comment échanger cette dernière entre l'émetteur et le récepteur sans qu'elle puisse être interceptée par un adversaire, ce qui lui permettrait de déchiffrer les communications? L'invention, au milieu des années septante, des techniques de cryptographie à clé publique a apporté une première solution. On utilise deux clés différentes, la clé publique permettant de chiffrer les données et la clé privée servant à les déchiffrer. La clé publique peut être transmise sur un réseau non sécurisé puisqu'elle permet uniquement de chiffrer des données. Si elle venait à être interceptée par un adversaire, ce dernier ne pourrait pas l'utiliser pour déchiffrer les informations.
Bien que très pratiques et largement utilisées, par exemple pour sécuriser les transactions sur Internet, ces techniques de cryptographie à clé publique n'offrent qu'une sécurité limitée dans le temps. Leur sécurité est en effet basée sur la complexité de certains problèmes mathématiques. Du fait de l'augmentation de la puissance de calcul des ordinateurs, les ressources nécessaires pour résoudre ces problèmes mathématiques diminuent avec le temps. La sécurité du chiffrement dépend de la longueur de la clé utilisée et il est donc nécessaire d'augmenter progressivement cette longueur pour maintenir le même niveau de sécurité. Cette réalité a récemment été illustrée par l'exploit du groupe du Professeur Lenstra qui est parvenu à casser une clé de 768 bits, qui était considérée comme parfaitement sûre il y a seulement quelques années.

ID Quantique a d'abord développé un prototype qui a été testé sur un réseau de fibres optiques. Puis, l'appareil a permis d'échanger une clé de cryptage entre deux stations connectées chacune à un PC par un port USB.

De la cryptographie quantique à la fondation d'ID Quantique

La physique quantique apporte une solution à ce problème grâce à la cryptographie quantique. Cette technologie exploite un principe fondamental de la physique quantique – toute observation cause une perturbation – pour transmettre des clés sur un réseau de fibre optique et vérifier qu'elles n'ont pas été interceptées. Cette technologie permet de garantir la sécurité des clés de chiffrement sans qu'aucune hypothèse sur la puissance de calcul à disposition d'un adversaire ne soit nécessaire.
Inventée dans les années quatre-vingt par deux chercheurs nord-américains, cette technologie a été mise en pratique au début des années nonante par le groupe du Professeur Nicolas Gisin à l'Université de Genève. Après une dizaine d'années de recherche, la société ID Quantique a été fondée par quatre chercheurs de ce groupe en vue de commercialiser cette technologie, ce qui a été réalisé avec succès. Dans le cadre d'une première mondiale, en automne 2007, les équipements développés par ID Quantique ont déjà servi à sécuriser le réseau utilisé par le Canton de Genève pour le dépouillement de ses élections.
En 2009, ID Quantique a déployé, en collaboration avec plusieurs partenaires dont l'Université de Genève et la HES-SO, le réseau SwissQuantum, un prototype de réseau quantique permettant un test à long terme de ces nouvelles technologies et la démonstration de leur compatibilité avec les réseaux modernes (plus d'information sous http://www.swissquantum.com).

ID Quantique aujourd'hui

ID Quantique emploie aujourd'hui une quinzaine de personnes dans la région genevoise et propose une vaste gamme de produits de chiffrement permettant de sécuriser les réseaux de données à haute vitesse, tant au moyen de la cryptographie conventionnelle que quantique. Ces équipements sont utilisés par des clients, par exemple dans les domaines bancaire ou gouvernemental.
Au moment de la fondation d'ID Quantique en 2001, ses fondateurs étaient conscients des difficultés liées au financement des nouvelles entreprises et ils ont mis en place une stratégie visant à développer des activités permettant de générer des revenus à court terme et donc de financer le développement des produits de chiffrement de la société. C'est pourquoi ID Quantique est aussi présente dans le secteur des instruments de mesures optiques et dans celui de la génération d'aléas. Dans ce dernier domaine, ID Quantique a développé des périphériques informatiques – cartes ou module – exploitant un processus quantique pour produire des nombres aléatoires parfaits. La physique quantique indique, en effet, que certains de ces processus sont fondamentalement aléatoires. Ces générateurs sont utilisés dans le monde entier pour de nombreuses applications, telles que la production de codes uniques pour la téléphonie prépayée ou le tirage de nombres gagnants pour des loteries. ■

Contact:
> info@idquantique.com
> Infos: www.idquantique.com

Noeud du réseau SwissQuantum situé à l'Université de Genève.
Photos: Roland Keller/ High-News Sàrl (www.top-news.ch)

Security in the Information Society

Security challenges in the Information Society cannot always be solved by technical means only. A multidisciplinary approach is very often required to find solutions at the intersection of forensic sciences and the legal and technical domains. Moreover, the political, the societal and the ethical dimensions of these challenges should not be underestimated. Our newly created Research Institute for Security in the Information Society (RISIS) at the BFH-TI offers the necessary technical expertise in this multi-dimensional research environment.

Prof. Dr. David-Olivier Jaquet-Chiffelle
RISIS
Head of founder of V.I.P.
Virtual Identity, Privacy and Security[1]
Photo: www.arteplus.ch

Shopping in the Ambient Intelligence Space
Photo: ©Nmedia, fotolia

Our team of researchers includes internationally recognized experts in computer, network and web security, in cryptology, but also in trust, in identity and in privacy. We are now involved in CACE, an FP7 EU-project on zero-knowledge protocols[2] and we have been leading joint activities in FIDIS, an FP6 EU Network of Excellence on the **Future of IDentity in the Information Society[3]**. Within FIDIS, security in the Information Society has been investigated from the identity perspective, by means of an interdisciplinary approach. Topics include, but are not limited to, profiling, privacy in e-business and in e-government, e-voting, the biometric passport and forensic implications of new forms of identities.

Profiling[4], for example, turns the plethora of available data in the Information Society into usable knowledge about individuals, about their habits and their expected behavior or preferences. This knowledge leads to new forms of identities and to categorization, a fundamental building block for the **Ambient Intelligence Space**. Such a personalized, interactive environment, identifying or even anticipating our needs, seems promising in terms of convenience and efficiency, but also conveys fear in terms of privacy and ethics. How far can the environment anticipate our needs without influencing them? What is the impact of targeted advertisement on our real choices to modify our habits or our preferences? Categorizations in the Information Society can also restrain common opportunities: a medical insurance refuses to cover a calculated «bad risk», a bank does not grant a mortgage to some categories of customers, etc. What if a system places us in a wrong category? We understand here the risk that the victim of an identity-theft could suffer long term consequences. In the fight against terrorism, a false categorization can even threaten the physical security of an honest citizen or of the society itself.

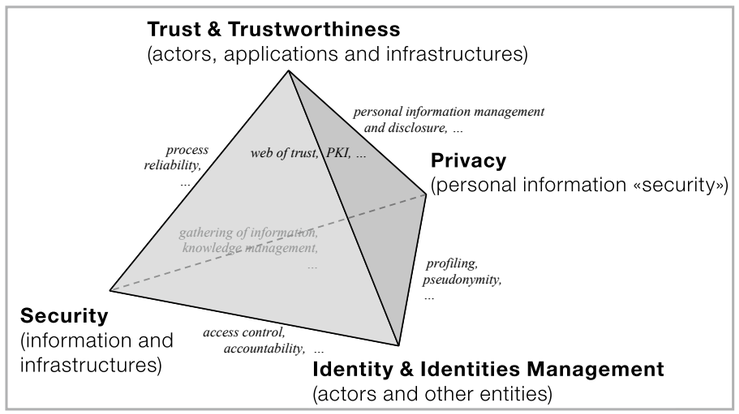


Fig. 1 Security in the Information Society: interwined concepts

Electronic voting[5] over the Internet is another topic which is very challenging in terms of security in the Information Society. Switzerland intends to play a leading role in this field and some pilot trials have already been successfully conducted in Geneva, Neuchâtel and Zürich. However, frauds can be extremely difficult, if even possible, to detect. Moreover, scalability and repeatability of an electronic fraud is much easier to achieve than for its paper counterpart. Trust in the voting mechanism is a cornerstone of our direct democracy. It is not yet clear if a trustworthy electronic voting system, which is at least as secure as its paper counterpart, is or will ever be achievable.

With the development of the Internet towards the **Internet of Things** or even the **Internet of Entities**, the digital world appears as a significant component of the real world. The frontier between the physical world and the virtual one is becoming fuzzy. Security in the Information Society cannot be reduced to traditional computer and network security or even to information security anymore. The security of persons and of the society itself should be taken into consideration starting at the very conception of new systems or applications. New paradigms bring the concept of security in the Information Society to new level where traditional security of information and infrastructures is intertwined with privacy (personal information «security»), with secure identification of (acting) entities, as well as with trust and trustworthiness of actors, applications and infrastructures (See Fig. 1). ■

Contact:
> david-olivier.jaquet-chiffelle@bfh.ch
> infos: www.vip.ch

Résumé
La sécurité dans la société de l'information ne peut se réduire à la sécurité informatique au sens strict du terme.
La protection des données personnelles, par exemple, dépasse largement le cadre technique de la cryptologie et de la protection de l'information. La sécurité dans la société de l'information doit être abordée de manière globale et multidisciplinaire : droit, sciences techniques et sciences criminelles collaborent pour assurer la sécurité non plus seulement de l'information, mais de l'individu et de la société elle-même.

Zusammenfassung
Sicherheit kann man in unserer Informationsgesellschaft nicht auf Informatiksicherheit im engen Sinn reduzieren.
So geht etwa der Schutz der persönlichen Daten weit über den technischen Rahmen der Kryptologie und des Informationsschutzes hinaus. Sicherheit in der Informationsgesellschaft erfordert einen globalen und multidisziplinären Ansatz: Recht, technische Wissenschaften und Kriminalwissenschaften arbeiten zusammen, um nicht nur die Sicherheit der Daten, sondern mehr noch die des Individuums und sogar der Gesellschaft selbst zu schützen.

[1] www.vip.ch
[2] www.cace-project.eu
[3] www.fidis.net
[4] We authored several contributions in the book «Profiling the European Citizen, Cross-Disciplinary,Perspectives», published by Springer in 2008 (editors M. Hildebrandt and S. Gutwirth, ISBN 978-1-4020-6913-0).
[5] We are leading the Swiss e-voting competence center (www.e-voting-cc.ch).

Mini-Spektrometer leistet Detektivarbeit

Die ARCoptix SA, ein von der STI gefördertes Unternehmen, gewinnt den mit CHF 500 000 dotierten Innovationspreis der Neuenburger Kantonalbank. Mit ausgeklügelter Microtechnologie realisierte ARCoptix das kleinste Fourier-Infrarotspektrometer der Welt. Damit setzt das Spin-off der BFH-TI und des IMT Neuchâtel neue Massstäbe für die Entdeckung minimalster Mengen von Substanzen in einem weiten Spektrum.

Viele toxische Stoffe bleiben oft unerkannt von Auge und Nase. Entsprechend rege ist der Ruf nach Verfahren, welche schädliche Substanzen in Luft, Wasser, Lebensmitteln oder Kosmetika rasch und sicher identifizieren. Das ist die Domäne des miniaturisierten Fourier Transformations-Spektrometers (FTS), entstanden als Kooperation zwischen IMT Neuchâtel und BFH-TI, kommerzialisiert mit dem Spin-off ARCoptix SA.
ARCspectro ANIR ist mit einem mikro-betriebenen lamellaren Beugungsgitter ausgerüstet. Im Gegensatz zu dispersiven Systemen, wo ein Prisma oder Beugungsgitter das Licht in seine Spektralanteile zerlegt, arbeitet das System interferometrisch, misst simultan den ganzen Spektralbereich. Da es ein breiteres Spektrum misst als Gitter- und Fabry-Perot-Geräte, erschliessen sich neue Anwendungsmöglichkeiten dort, wo hohe Auflösung und ein grosser Spektralbereich gefragt sind. Die Innovation besteht darin, ein vollintegriertes, robustes FTS mit einem lamellaren Interferometer und vergleichbar hoher Auflösung zu realisieren. Dies geschah mit MOEMS-Technologie, einer Kombination von Mikrooptik, Mikromechanik und Mikroelektronik, welche die Fertigung einer ganzen Reihe integrierter Systeme ermöglicht. Das tragbare Gerät ist mit einem einzigen Photodioden-Detektor ausgerüstet, braucht wenig Energie und lässt sich über den USB-Anschluss des Laptops betreiben. Die aktive Kontrolle durch einen Laser sichert höchste Präzision und Wiederholbarkeit der Messungen, der modulare Aufbau ermöglicht eine spezifische Anpassung an spezielle Messprobleme. ■

Kern des Geräts: Hermetisch verpacktes miniaturisiertes Interferometer und Elektronik zu dessen Ansteuerung.
Foto: ARCoptix

Team ARCoptix
(von links nach rechts: Fabrice Merenda, Toralf Scharf, Gerben Boer, Steeve Bühler, Hicham Farah; nicht abgebildet: Christophe Ackermann)
Foto: BCN

Kontakt:
> sti-stiftung@bfh.ch und info@arcoptix.com
> Infos: www.sti-stiftung.ch und www.arcoptix.com

Der Arbeitsmarkt für Jungingenieure

Obwohl die Rezession das Bild trübt, sind Absolventinnen und Absolventen technischer Studienrichtungen weiterhin sehr gefragt und dürfen mit einer positiven Lohnentwicklung rechnen.

«Das grösste Problem bei der Stellensuche war für mich die Qual der Wahl», erzählt Georg Nef, der im September 2008 sein Studium als Holzbauingenieur an der Berner Fachhochschule BFH abschloss. Auch Simon Flepp erhielt noch 2008 als Student der Elektrotechnik an der Stellenbörse der Hochschule Rapperswil HSR viele Angebote. «Aber schon 2009 stellte ich bei den gleichen Firmen einen Einstellungsstopp fest», berichtet er. Tatsächlich stieg die Arbeitslosigkeit in den Ingenieurberufen in den letzten Monaten überdurchschnittlich: Im Dezember 2009 waren in der Schweiz doppelt so viele Ingenieurinnen und Ingenieure arbeitslos gemeldet als im Vorjahresmonat – während die Zunahme erwerbsloser Personen über alle Berufsgruppen in diesem Zeitraum nur 46% betrug. «Dies zeigt, wie stark die Industrie von der Rezession betroffen ist», kommentiert Antje Baertschi, Medienspre-cherin des Staatssekretariats für Wirtschaft SECO. Somit befindet sich der Arbeitsmarkt in der paradoxen Situation, dass einerseits viele Ingenieure auf Stellensuche sind – andererseits aber auch die Unternehmen einen gravierenden Mangel an Fachkräften beklagen.

Gute Absolventen bleiben gefragt

Diese sogenannte «Ingenieurlücke» zeigte sich erstmals im März 2006. Seitdem verschärft sich die Situation laufend, so eine Studie des Büros für arbeits- und sozialpolitische Studien BASS (2008). Im April 2008 wurden demnach 3000 fehlende Ingenieure verzeichnet. Die knapp 2000 arbeitslosen Ingenieure, die im Dezember 2009 gemeldet sind, vermögen diese Lücke nicht zu schliessen. Die Suche nach hoch qualifizierten Fachkräften gestaltet sich dabei insbesondere für jene Branchen schwierig, die dem handwerklich orientierten Gewerbe nahe stehen wie Heizung/Lüftung/Klima oder die Baubranche. Dies zeigt die aktuelle Salärerhebung des Berufsverbands Swiss Engineering STV (2009). Auch die Mitglieder des Vereins «IngCH Engineers Shape our Future», darunter ABB, Alstom, Nestlé oder Siemens, gehen davon aus, dass der Bedarf aufgrund der demographischen Entwicklung langfristig knapp bleiben wird. Die Situation werde allerdings genutzt, um sich die besten Talente zu sichern, bekundeten die Unternehmen an einer Veranstaltung des Vereins im März 2009. Die Stellenprofile werden wesentlich genauer definiert, und es werden auch häufiger Kandidaten aus dem Ausland rekrutiert.

Die Resultate der Umfrage sind in der Salärbroschüre 2009/2010 publiziert.
Quelle: Swiss Engineering

Salärumfrage von Swiss Engineering STV
Die Resultate der Umfrage sind in der Salärbroschüre 2009/2010 publiziert. Sie kann für 75 Fr. plus Porto bei Swiss Engineering STV bestellt werden (für Mitglieder gratis). Für Studierende und Absolventen im ersten Jahr ist die Mitgliedschaft bei Swiss Engineering STV kostenlos. Der führende Schweizer Berufsverband der Ingenieure und Architekten vertritt seit über hundert Jahren die Interessen seiner Mitglieder und unterstützt sie in ihrer beruflichen Entwicklung – mit vielfältigen Dienstleistungen, einem breiten Aus- und Weiterbildungsangebot, spezifischen Fachpublikationen und Veranstaltungen. 14 000 Fach- und Berufsleute, 28 Sektionen und 24 Fachgruppen bieten ein umfassendes Netzwerk.

Interdisziplinarität hoch im Kurs

Gut ausgebildete Ingenieurinnen und Ingenieure bleiben also auch in Zukunft sehr gefragt. Über 80% der Absolventen finden innert fünf Monaten nach Studienabschluss eine Stelle – nach einem Jahr sind es laut Salärerhebung von Swiss Engineering sogar über 95%. Die jungen Berufsleute sehen ihre berufliche Zukunft vor allem im interdisziplinären Bereich, gefolgt von unternehmerischen Tätigkeiten und einem verstärkten Engagement für Gesellschaft, Umwelt und Politik. Laut der Absolventenbefragung des Bundesamts für Statistik von 2007 arbeiten 32% der FH- und 16% der Uni-/ETH- Absolventen technischer Studienrichtungen im ersten Anstellungsjahr im Bereich «Verarbeitendes Gewerbe/Herstellung von Waren». 37% der Absolventen universitärer Hochschulen und 22% von Fachhochschulen waren in dem heterogenen Beschäftigungsbereich «Erbringung von freiberuflichen, wissenschaftlichen und technischen Dienstleistungen» tätig.

Positive Lohnentwicklung

Gemäss der Salärerhebung von Swiss Engineering lag der Einstiegslohn der Jungingenieure 2009 bei 74 000 Fr. (Median), wobei sich die Gehälter der mittleren 50% in einer Spannbreite von 12 000 Franken bewegen. Am meisten verdienen die Maschineningenieure mit 76 000 Franken – jedoch konnten sie den geringsten Gehaltszuwachs gegenüber dem Vorjahr ausweisen. Einen grossen Lohnsprung von 65 000 auf 72 000 Franken machten dagegen die Umweltingenieure. Über die Hälfte der befragten Absolventen beurteilt die zukünftige Lohnentwicklung als überdurchschnittlich oder gar glänzend – bei den erfahrenen Ingenieuren gelangte im Gegensatz dazu nur knapp ein Viertel zu dieser Einschätzung. Zudem zeigte sich, dass sich Auslandserfahrung langfristig in höheren Löhnen niederschlägt: Ab dem 36. Lebensjahr steigt das Salär von Berufsleuten mit Erfahrung im Ausland stärker als dasjenige ihrer Kollegen ohne Berufserfahrung ausserhalb der Schweiz.

Wege ins Management

Der Grossteil der Absolventinnen und Absolventen ingenieurwissenschaftlicher Fachrichtungen agiert im ersten Berufsjahr in Angestelltenpositionen ohne Führungsfunktion, wie eine Studie (2009) des Vereins IngCH zeigt. Später sind Ingenieure im Management aber gut vertreten. So besetzen sie in SLI-notierten Unternehmen 23% aller Geschäftsleitungs- und 16% aller Verwaltungsratspositionen. In den technologieorientierten Mitgliederfirmen von IngCH sind sogar 45% der Geschäftsleitungs- und 33% der Verwaltungsratspositionen mit Ingenieuren besetzt. Viele ergänzen ihr Fachstudium mit einer betriebwirtschaftlichen Weiterbildung oder einem MBA, um danach eine Führungsfunktion zu übernehmen. Die Führungsverantwortung zahlt sich gemäss Salärerhebung von Swiss Engineering auch finanziell aus: Im Durchschnitt über alle Branchen verdienen Mitglieder des Top-Managements fast 30 000 Franken mehr als jene des unteren Kaders. Doch welche Karriere man auch wählt, wichtig sind immer auch ein breites Fachwissen, fortwährende Weiterbildung und gute Sprachkenntnisse. Ingenieurinnen und Ingenieure – insbesondere solche auf Stellensuche – sind gut beraten, sich auch in anderen Bereichen als ihrem eigentlichen Fachgebiet weiterzubilden, um möglichst flexibel einsetzbar zu sein. ■

Kontakt:
> info@swissengineering.ch
> Infos: www.swissengineering.ch

Text: Stefan Arquint
Generalsekretär Swiss Engineering STV

Technische Studiengänge beliebt
Die Nachfrage nach Ingenieuren spiegelt sich auch in den Studierendenzahlen. Gemäss einer Studie von IngCH (2009) schrieben sich 2008 an den Fachhochschulen in den ingenieurwissenschaftlichen Fachbereichen markant mehr Studierende ein als im Vorjahr (+9%). Damit überflügelten die Ingenieurwissenschaften die meisten anderen Fachbereiche. Am stärksten zugenommen haben die Eintrittszahlen in den Studiengängen Informatik, Systemtechnik und Medieningenieurwesen. Ähnliches gilt für die universitären Hochschulen: Nach einem moderaten Wachstum 2006 (+4%) und einem leichten Rückgang 2007 (-1%) stieg die Anzahl der Studieneintritte in den Ingenieurfachrichtungen 2008 deutlich um 10%. Das Maschineningenieurwesen, die Informatik und Kulturtechnik/Vermessung wuchsen dabei überdurchschnittlich. Im Arbeitsmarkt dürfte sich der Anstieg der Studierenden jedoch erst in ein paar Jahren bemerkbar machen.

News

29. Face to Face Meeting
Der Forschungsschwerpunkt Energie, Verkehr, Mobilität der BFH befasst sich mit zukunftsweisenden Technologien bei erneuerbaren Energien, alternativen Antriebskonzepten und der Verkehrssicherheit von Fahrzeugen. Gewinnen Sie einen Einblick in den aktuellen Stand der Forschung bei elektrischen Energiespeichern und der Batterie-Technologie.
16. März 2010, 16.00 - 18.00 Uhr,
Quellgasse 21, Biel. **ti.bfh.ch > Events**

29 Meeting Face to Face
Le domaine principal de recherche Énergie, Transport, Mobilité de la Haute école spécialisée bernoise s'occupe des technologies futuristes des énergies renouvelables, des concepts de propulsion alternatifs et de la sécurité routière des véhicules. Découvrez la situation actuelle de la recherche relative aux accumulateurs d'énergie et à la technologie des batteries.
16 mars 2010, 16h00 - 18h00
HESB-TI, Rue de la Source 21, Bienne

Loksimulatoren im Verkehrshaus Luzern
Am 20. Januar 2010 fand die Inbetriebnahme der drei von der BFH sanierten Loksimulatoren im Verkehrshaus in Luzern im Beisein der CEOs der drei Sponsoren BLS, RhB und SBB statt.
Kontakt: **hansjuerg.rohrer@bfh.ch**

Découvrez les caractéristiques mécaniques des couches minces
dans le laboratoire des matériaux avec le FISCHERSCOPE HM2000. Il s'agit d'une indentation instrumentée pour mesurer la dureté universelle selon la norme EN ISO 14577, la référence dans ce domaine.
Contact: **jean-martin.rufer@bfh.ch**

Marktplatz Weiterbildung
An unserer neuen Veranstaltung «Marktplatz Weiterbildung» präsentieren wir Ihnen das gesamte Weiterbildungsangebot des Departements Technik und Informatik und des Fachbereichs Wirtschaft und Verwaltung. Verschaffen Sie sich einen Überblick über das Weiterbildungsangebot in InformationTechnology, Wirtschaft & Verwaltung, Management, Medizintechnologie und Medizininformatik.
22. Juni 2010, 16.00 - 20.00 Uhr
BFH Wirtschaft, Morgartenstrasse 2c,
3014 Bern

Neuer Bachelorstudiengang Medizininformatik
Die BFH Technik und Informatik hat einen neuen, in der Schweiz einzigartigen Studiengang lanciert. Zum Herbstsemester 2010 werden voraussichtlich die ersten Studierenden das Bachelor-Studium «Medizininformatik» beginnen. Das Gesuch wurde beim BBT deponiert.
Infos: **ti.bfh.ch/medizininformatik**

Privacy Respecting Electronic Identity Management and Forensics
La Commission européenne a organisé un meeting stratégique sur la thématique «Privacy Respecting Electronic Identity Management and Forensics», le 27 novembre 2009, à Bruxelles.
Prof. Dr. D.-O. Jaquet-Chiffelle a été invité non seulement à y participer, mais également à être le modérateur d'une des deux sessions.

2009 Best New Chapter Award
Das Schweizer Chapter der IEEE Engineering in Medicine and Biology Societey hat den «2009 Best New Chapter Award» gewonnen. Der Award wird nur einmal pro Jahr weltweit vergeben und ist mit 1500 USD dotiert. Das Chapter wurde von Prof. Dr. Volker M. Koch gegründet und wird seitdem auch von ihm geleitet.
Infos: **www.biomedeng.org.**

CAREER DAY BFH-TI 2009
Foto: Hans-Rudolf Burkhard

Infotage BFH-TI 2010
18.03.2010 / 29.04.2010 / 27.05.2010
Biel und Burgdorf: 15.00 – 17.00 Uhr
Bern: 17.30 – 18.30 Uhr

CAREER DAY TECHNIK UND INFORMATIK
Dienstag, 18. Mai 2010
9.00 bis ca. 17.00 Uhr
BFH-TI, Quellgasse 21, Biel
Kontakt: iris.smid@bfh.ch

Techdays / Ausstellung der Diplomarbeiten 2010
Öffnungszeiten:
Freitag, 24. September 2010
10.00 - 19.00 Uhr
Samstag, 25. September 2010
10.00 - 14.00 Uhr

Diplomfeier 2010
Samstag, 25. September 2010

Journées d'info HESB-TI 2010
18.03.2010 / 29.04.2010 / 27.05.2010
Bienne et Burgdorf: 15h00 - 17h00
Berne: 17h30 - 18h30

CAREER DAY TECHNIQUE ET INFORMATIQUE
Mardi 18 mai 2010
9.00 h à 17.00 h
HESB-TI, Rue de la Source 21, Bienne
Pour de plus amples informations:
Contact: iris.smid@bfh.ch

Techdays / Exposition des travaux de diplôme 2010
Heures d'ouverture :
Vendredi, 24 septembre 2010
10h00 – 19h00
Samedi, 25 septembre 2010
10h00 – 14h00

Cérémonie de remise des diplômes 2010
Samedi, 25 septembre 2010

Tropenhaus Frutigen erhält Idee-Suisse Award 2009
Das Tropenhaus Frutigen, wo eine sehr innovative Störzucht mit dem warmen «Abwasser» aus dem Lötschbergtunnel betrieben wird, erhält den Idee-Suisse Award 2009. Das Institut (ifms) war mit der automatischen und stressfreien Sortierung der Fische an diesem Erfolg beteiligt (siehe hitech 3/2009, S. 14).

CAS Coaching
Die BFH-TI bietet in Biel den CAS «Führen im Wandel – Die Führungskraft als Coach» an. Die sechste Durchführung startet im April 2010.
Kontakt: marylou.bregy@bfh.ch
Infos: **ti.bfh.ch /cas-coaching**

BKW

Die Liberalisierung im Strommarkt setzt Impulse frei und eröffnet neue Chancen. Wir verstehen sie als Aufforderung, uns dynamisch weiterzuentwickeln. Dazu sind wir auf engagierte Mitarbeiterinnen angewiesen wie beispielsweise Priska Zenklusen. Zie Ibewusst und beharrlich realisiert sie anspruchsvolle Projekte – und trägt so zur Unternehmensentwicklung bei.
Bei der BKW-Gruppe sorgen 2800 Mitarbeiterinnen und Mitarbeiter heute dafür, dass bei mehr als einer Million Menschen zuverlässig der Strom fliesst. Gehören Sie morgen dazu? Wir freuen uns, wenn Sie mit uns die Zukunft angehen.

BKW FMB Energie AG, Human Resources Management, Telefon 031 330 58 68,
info@bkw-fmb.ch, www.bkw-fmb.ch/karriere