Berner Fachhochschule
Haute école spécialisée bernoise

Hochschule für
Technik und Architektur Biel
École d'ingénieurs
de Bienne

TUT

112. Jahresbericht / 112e rapport annuel

15

März / Mars / Marzo 2003

Special Issue

Impact of new technologies on privacy and data protection

D.-O. Jaquet-Chiffelle received his Ph.D. degree in Mathematics in 1991. Then he went to Harvard University to pursue his research where he was also lecturer in the Department of Mathematics. From 1992 to 1994, he was a scientific associate at the University of Neuchâtel and worked in collaboration with the University of Bordeaux.

In 1994, he joined the Swiss Federal Section of Cryptology (Swiss Government) as a scientific expert and in 1996 developed a concept to anonymize the patients in official medical statistics. His concept is now being used by all Swiss hospitals to transmit their data to the Federal Statistical Office.

Since 1997, he has been a full professor of Mathematics and Cryptology at the University of Applied Sciences of Bern (Switzerland). In 2001, he founded V.I.P (Virtual Identity and Privacy research center).

In Switzerland, V.I.P proposes services and audits in security, privacy and data protection. V.I.P is active at a European level as well, for example, in the RAPID project (Roadmap for Advanced Research in Privacy and IDentity Management Technologies).

www.vip.ch
contact@vip.ch

Editorial

Several months ago, two of the head editors of the TILT – Gabriella Scorrano and Giampaolo Possagno – asked me to prepare a special issue on data protection. As I am in charge of V.I.P (Virtual Identity and Privacy research center), the theme particularly interested me. We finally decided to concentrate on the impact of new technologies on privacy and data protection.

The themes and points of view presented in this issue are multiple. Their purpose is to enable the reader to better understand the extent of this field. For in fact this subject cannot be reduced to a mere question of technology; it concerns law, economics, and the fight against crime as well. For each one of these aspects, we are fortunate to be able to include in this issue of TILT the contributions of specialists of international renown. As a matter of fact, one of the objectives of V.I.P is to favor interdisciplinary exchange; its cooperation with the IPSC (Institute of scientific police and criminality of the University of Lausanne) is an excellent illustration of this dimension of its activity.

Several colleagues, who are members of V.I.P, have also accepted to contribute to this issue by presenting various activities of our school that are directly related to this theme. In particular we must mention the project Cod-IT, under the direction of Lorenz Müller, in which other colleagues of the computer science division participate, as well as MicroLab, the microelectronic laboratory of our school.

As new information technologies develop, new services – seemingly very attractive – are created. In parallel the impact of these new technologies on privacy and data protection increases in importance.

Let us take the example of e-commerce and m-commerce, two fields with very high potential. It is easy to perceive the advantages of being able to obtain appropriate information on a PDA or a cellular phone, in function both of our interests and our location. The other side of

Il y a plusieurs mois déjà, deux des principaux rédacteurs du TILT – Gabriella Scorrano et Giampaolo Possagno – m'ont proposé de présenter un dossier spécial sur la protection des données. En tant que responsable de V.I.P (Virtual Identity and Privacy research center), le thème m'intéresse tout particulièrement. Finalement, nous avons décidé de traiter plus spécialement l'impact des nouvelles technologies sur la sphère privée et la protection des données.

Les thèmes et les points de vue abordés dans ce dossier sont multiples. Ils devraient permettre au lecteur de mieux comprendre l'étendue de ce domaine. En effet, ce domaine ne se résume pas à une simple question de technologie ; il concerne également le droit, l'économie, la lutte contre la criminalité. Pour chacun de ces aspects, nous avons la chance de publier, dans ce numéro du TILT, les contributions de spécialistes internationalement reconnus. Favoriser cette interdisciplinarité et la communication entre les acteurs concernés, est d'ailleurs un des buts de V.I.P ; la collaboration avec l'IPSC (Institut de Police scientifique et de criminologie de l'Université de Lausanne) illustre par exemple cette volonté.

Plusieurs collègues, membres de V.I.P, ont également accepté d'enrichir ce numéro en présentant certaines activités de notre école, directement en rapport avec la thématique de ce dossier : en particulier, le projet Cod-IT, dirigé par Lorenz Müller et dans lequel participent entre autres des collègues de la division informatique, ainsi que Micro-Lab, le laboratoire de microélectronique de notre école.

À mesure que se développent les nouvelles technologies de l'information, de nouveaux services – très attractifs en apparence - voient le jour. Parallèlement, l'impact de ces nouvelles technologies sur la sphère privée et la protection des données devient plus important.

Prenons l'exemple du e-commerce et du m-commerce, deux domaines qui possèdent un très grand potentiel. Nous percevons facilement les avantages de pouvoir rece-

the coin is too often neglected: in most of the e-commerce or m–commerce applications, personal information is transmitted (see also the article by Jos Dumortier - professor in Law and IT at K.U.Leuven -, pages 66-69 in this issue of TILT). This information may seem harmless, but as applications are developed and generalized, it becomes possible to establish a more and more detailed profile of the users and their habits. This constitutes a definite threat to the protection of privacy. And it would be a mistake to underestimate its importance. A recent European report[1] insists upon the fact that this is one of the main obstacles to the development of these new applications; the report advocates the reinforcement of measures to preserve the protection of privacy. In short, "to be or not to be… spied upon", that is the question !

I would like to thank all the people who, directly or indirectly, have made this special issue possible – first of all, the authors themselves who responded to my invitation. The broad scope of their informative articles represents the state of the art in the field of privacy and data protection. My thanks also go to Christine Beerli, head of our school; without her support, V.I.P – and consequently this special issue – would never have been created. Finally, I would like to thank my colleagues Gabriella Scorrano and Giampaolo Possagno, who have helped and advised me throughout this project and who have made a considerable effort to transform it into a TILT publication.

I hope that you, all the readers of TILT, will find that the time spent reading this special issue has been fascinating and enriching. •|

---

1 "Future Bottlenecks in the Information Society" June 2001 Report to the European Parliament, Committee on Industry, External Trade, Research and Energy (ITRE)

voir une information ciblée sur un assistant digital personnel (PDA) ou sur un téléphone portable, en fonction de nos intérêts et de l'endroit où nous nous trouvons. Le revers de la médaille est trop souvent négligé : dans la plupart des applications actuelles en rapport avec le e-commerce ou le m-commerce, des informations personnelles sont transmises (voir également, dans ce numéro du TILT, l'article de Jos Dumortier – professeur de Droit et des Technologies de l'information à l'Université K.U. Leuven – pages 66-69). Ces informations peuvent paraître anodines, mais à mesure que les applications se développent et se généralisent, elles permettent d'élaborer un profil de plus en plus détaillé des utilisateurs et de leurs habitudes ; elles présentent alors une réelle menace pour la protection de la sphère privée. Et il serait regrettable de sous-estimer leur impact. Un récent rapport européen[1] souligne qu'il s'agit là d'un des principaux obstacles au développement de ces nouvelles applications et préconise le renforcement des mesures qui préservent la protection de la sphère privée. En résumé, "être ou ne pas être… espionné", telle est la question !

Pour terminer, j'aimerais remercier toutes les personnes qui, directement ou indirectement, ont permis la réalisation de ce dossier. Mes remerciements vont tout d'abord aux auteurs eux-mêmes qui ont répondu à mon appel et qui donnent à travers leurs articles une vision large et actuelle de l'impact des nouvelles technologies sur la sphère privée et la protection des données. J'aimerais également remercier, Christine Beerli, directrice de notre école, sans le soutien de laquelle V.I.P – et par conséquent ce dossier spécial – n'aurait jamais vu le jour. J'aimerais finalement remercier mes collègues Gabriella Scorrano et Giampaolo Possagno, qui m'ont aidé tout au long de ce travail et qui ont fourni un effort considérable pour le transformer en une publication du TILT.

A vous toutes et à vous tous, lectrices et lecteurs du TILT, je souhaite une lecture passionnante et enrichissante. •|

Legal considerations with regard to privacy protection and identity management in the information society

Jos Dumortier

Nobody will contest that the protection of individual privacy is becoming one of the most crucial issues of modern, networked information society. It is also clear that our legal framework in this area, having been conceived in the seventies and eighties of the past century, is not very well adapted to the new challenges and has to be thoroughly redesigned. Future regulation, in order to be effective, should be developed at the global network level and preferably be integrated into the technology itself.

Jos Dumortier graduated in Law at K.U.Leuven (1973). After postgraduate studies in Nancy (Centre Européen Universitaire, 1974) and Heidelberg (DAAD, 1975), he became research fellow at K.U.Leuven.

From 1981 until 1983 he studied Information Sciences (INFODOC) at the Université Libre de Bruxelles. Between 1984 and 1992 he was part-time lecturer in Information Science at the University of Antwerp.

In 1985 he became part-time lecturer and in 1993 full-time Professor in Law and IT at K.U.Leuven. In 1990 he founded the Interdisciplinary Centre for Law and Information Technology (ICRI) of which he became the first Director (for more details about the Centre, see http://www.icri.be)

Since 1991 he is active in lecturing, research and consultancy in the area of Law and ICT and published several books and articles on this subject. He is a board member of several scientific and professional organisations such as the European Academy (Bad Neuenahr, Germany), BELTUG (Belgian Telecommunications Users Association) and EEMA (European Electronic Messaging Association) and he participates in the editorial board of several national and international periodical publications.

Professor Dumortier is the editor of the International Encyclopaedia of Cyberlaw (Kluwer International Publishers). He is an associate member of the American Bar Association, member of the Belgian Internet Observatory, member of the Flemish Strategic Digital Forum, of many other committees and advisory bodies. Professor Dumortier is regularly working as an expert for the Belgian federal government, the Flemish government, the European Commission and several national and international organisations on issues relating to Law and ICT.

Comprehensive laws for privacy protection are the favored type of regulation in the European Union. The directive on data protection constitutes a general framework regulation on the collection, use and transfer of personal data, underlining the obligations of the data controllers and the rights of the data subjects. Independent public supervisory authorities monitor compliance. Countries such as the United States favor more the adoption of sector-specific laws regulating, e.g. cable communication privacy, public records privacy, financial privacy or children's privacy. In many countries with general data protection laws, sector-specific laws are used as a complement by providing more detailed protection for certain categories of information, for example for consumer credit or health records.

On both sides of the Atlantic, research studies and regular polls indicate an inadequate compliance and understanding of data protection regulation from the side of the business and a lack of trust from the side of consumers. However major business organisations realise that there is an inherent risk in not complying with elementary data protection rules. Nevertheless, privacy issues are still mostly perceived as 'compliance' issues and not yet as a priority in daily business processes and practices.

Legal rules are generally very abstract and it therefore remains quite delicate to translate this general legal framework into specific, operational guidelines directly applicable to the context of electronic business. Another difficulty is the fact that current legislation has no effective impact and is not adequate in respect with a growing global digital economy and its inherent complexities.

Privacy codes of all kinds have been developed with varying quality relating to enforcement mechanisms, redress and communication. Accordingly their adequacy is variable. Seal programmes are of diverse quality and are submitted to auditing methods following unequal quality standards. There is a lack of transparency: consumers are not in the position to appreciate the differences and understand what level of protection they offer. Regarding standardization, the efforts have initially been welcomed with mixed feelings. Its potential in the field of privacy is presently still at the stage of very general recommendations.

Towards new regulatory mechanisms

More and more insiders start to think that the current regulatory framework should be adapted and that there is a need for new mechanisms and techniques in this area. In such a new framework traditional rulemaking has to be combined with privacy enhancing technology. Technological protection should not simply be developed and put on the market but it has to be integrated in the regulatory framework, in a way that is very much similar to what is being done in a sector such as automobile traffic regulation. Everyday we notice how difficult it is to make automobile drivers comply with traffic rules, especially those regarding speed limits. Rules

alone are clearly insufficient in this situation. They have to be combined with other measures such as artificial obstacles in densely populated areas or with speed limitation devices that are built-in into the cars themselves.

Privacy protection has to be promoted in a much similar way. The use of privacy enhancing technology has to be made obligatory in specific circumstances and compliance control should be built-in into the network. Legal rules should be restricted to general principles and refer to technical specifications and other standardization documents for further details.

Additionally privacy threats have to be considered as important as other security threats. In order to fight against computer viruses, denial of service attacks and other unlawful intrusions, a network of "Computer Incident Response Teams" (CERT) has been put in place. Similar teams and networks – "Privacy Incident Response Teams" (PIRT) are probably needed in the area of privacy protection. The establishment of such a network could perfectly be integrated into the work package of the independent supervisory authorities – generally called "data protection commissioners" - who play an important role in the implementation of privacy protection rules in Europe.

Monitoring technology development

A primary challenge in this area will be to avoid the development of privacy decreasing technologies and applications and to intercept them timely. Over the last years a number of technologies and applications have been introduced without sufficient awareness of negative privacy-related consequences.

One of the most striking examples is the mobile communications sector and more particularly the location-based services that are presently conquering the market. It is almost difficult to believe that these kinds of services are being developed and put on the market without any privacy-protecting framework. Ideally the development of such technology and services should be monitored from the beginning and constantly being evaluated from the privacy perspective.
The same mistake has been made during the launch of public key infrastructures (PKI), which is the technology used to guarantee security and reliability of electronic exchange of information. A very detailed and complex European regulatory framework has been set up in order to promote PKI for electronic signatures. This framework heavily relies on the systematic use of "identity certificates". Alternative – less privacy-intrusive – procedures, such as anonymous credentials, have almost never been considered during the development of the regulatory framework.

Another example can be found in the area of digital rights management (DRM). DRM technologies are originally designed to protect the rights of copyright holders through technical detection of copyright law infringements and technical restriction of use of digital files. They involve all aspects of content distribution, such as access control (frequency, length of views), control of certain uses, usage metering (to track frequency of access), payment processes and record keeping. DRM technologies usually require identification to access copyright protected content, exercise control over purchases and facilitate profiling of users preferences. Many solutions in this area have been developed without taking into account privacy issues and consequently without incorporating privacy enhancing technologies although this appears to be technically feasible.

There is a tendency towards increasing control over network users. More control is needed to combat network attacks and illegal activities, protect intellectual property rights, etc. Technological solutions are at present being developed to facilitate control. One of the examples is "Palladium", the code name for Microsoft's evolutionary set

of features for the Windows operating system, which - combined with a new breed of hardware and applications - will give individuals and groups of users greater data security and system integrity. Palladium is presented as a system that creates a 'trusted' computing platform. In order to avoid that 'trusted' computing platforms actually become 'controlled' computing platforms, we will have to invent ways to monitor their development and evaluate them from a privacy perspective from the very early start. Users' behavior in the global online environment will be less and less steered by rules originated by parliaments and governments but primarily be ruled through technological solutions and constraints. Technology developers will increasingly be able to decide which kind of users' behavior will be possible, permitted and tolerated in the online environment, without being submitted to elementary forms of democratic control.

Identity management

With the development of e-business, organizations need to manage secure access to information and applications spread over a wide range of network systems. Organizations also have to manage secure access to a great number of users, both inside and outside the organisation according to agreed authorizations and in respect with data protection rules. Identity management services enable administrators to control user access and conducted business through authentication methods (passwords, digital certificates, hardware or software tokens) and authorization rights.

On the other side, users are confronted with a large variety of systems and applications requiring different degrees of identification, access controls and credentials. Consequently they need tools to manage their identities and control the use of their personal data. This explains the present success of "passport" services on the Internet.

It is evident that identity management has to be combined with effective privacy protection. Users and supervisory authorities must have the possibility to control the activities of service providers who manage large databases with all kinds of personal data concerning individual network users. From the European perspective it is important to understand that getting the consent of the data subject to use his personal data for certain purposes, is often not sufficient to be compliant with privacy laws and regulations. As an employee, a soldier, a patient, etc. the individual person is not always in a position where he can freely and autonomously express his opinion, and the regulatory framework is specifically designed to compensate the dependency of the data subject via additional control and protection by independent supervisory authorities.

It will therefore be necessary to develop identity management solutions combining these requirements. Future solutions will have to give data subjects, maximum possibilities to control and steer the use of their personal data. They should be flexible enough to offer possibilities for the data subject to reveal only the identification data that are necessary for particular circumstances. Anonymous use of network services should be guaranteed where it is reasonably admissible. If unconditional anonymity – whereby the identity of the user is irreversibly lost – is not feasible, privacy-protecting schemes for conditional anonymity have to be established. Consequently the use of multiple 'virtual identities' will have to be regulated. In particular, legal questions raise regarding accountability, legal representation - for instance when minors adopt 'virtual' identities -, regarding contractual and tort liability or law enforcement issues.

The field of privacy and identity management will be an important laboratory where we can experiment how the law will function in our future global information society.

Digitale Evidenz oder die Krux mit der digitalen Signatur*

Prof. Dr. Ueli Maurer, ETH Zürich

Prof. Dr. Ueli Maurer

Ueli Maurer ist ordentlicher Professor für Informatik an der ETH Zürich und Leiter der Forschungsgruppe für Informationssicherheit und Kryptographie. Zur Zeit ist er Vorsteher des Instituts für theoretische Informatik. Seine Forschungsschwerpunkte sind Informationssicherheit, Kryptographie in Theorie und Anwendungen, Anwendungsgebiete wie digitale Signaturen, Public-Key Infrastrukturen, digitale Zahlungssysteme und E-Voting, das Management von Vertrauen und digitaler Evidenz, mathematische Sicherheitsbeweise, theoretische Informatik, diskrete Mathematik und Informationstheorie.
Maurer diplomierte 1985 als Elektroingenieur an der ETH Zürich und promovierte 1990. Bis 1991 war er DIMACS Research Fellow an der Princeton University und kam 1992 an das Informatikdepartement der ETH. Er nimmt viele Aufgaben als Editor und Programmkomiteemitglied wahr, ist Editor-in-Chief des Journal of Cryptology, Editor-in-Chief (mit Ronald Rivest) der Springer-Buchserie Information Security and Cryptography, Direktor der International Association for Cryptologic Research (IACR) sowie Mitbegründer des seit 1996 jährlich in Zürich stattfindenden Symposiums on Privacy and Security. Maurer ist IEEE Fellow.
Er patentierte mehrere kryptographische Verfahren und ist im Rahmen verschiedener Verwaltungsrats-, wissenschaftlicher Beirats- und Beratungsmandate in der Wirtschaft verankert. Er ist Mitgründer der Zürcher Sicherheitssoftwarefirma Seclutions AG sowie Verwaltungsrat der Tamedia AG.

Persönliche Information: 1960 geboren, verheiratet, zwei Töchter (17 und 13). Hobbies: Delta fliegen, Ski fahren, Violine spielen und Weine.

* Erstmals erschienen in digma 2002.1, Zeitschrift für Datenrecht und Informationssicherheit (Verlag Schulthess Jurtische Medien AG, Zürich).

Kein Zweifel: In wenigen Jahren werden wir digitale Signaturen standardmässig verwenden. Trotzdem: So einfach, wie die Sache aussieht, ist sie leider nicht. Erstens unterscheiden sich digitale Signaturen grundlegend von handschriftlichen Unterschriften. Zweitens stellt sich das bekannte Huhn-Ei-Problem: Es braucht Anwendungen, um den Aufbau einer Public-Key Infrastruktur (PKI) zu rechtfertigen und dafür ein valables Businessmodell zu definieren, und es braucht eine PKI, damit entsprechende Anwendungen überhaupt Sinn machen. Drittens bestehen beim Thema PKI noch konzeptionelle Missverständnisse.

Die Grundidee – eine geniale Erfindung der Kryptografie der späten 1970er Jahre – ist einfach: Eine digitale Signatur für ein bestimmtes Dokument kann nur mit Kenntnis des geheimen Schlüssels eines Benutzers erzeugt werden. Die Korrektheit der Signatur kann hingegen mit Hilfe des sogenannten Public Keys des Benutzers durch jedermann – insbesondere auch durch ein Gericht – verifiziert werden. Ein Benutzer kann sich zu einem Public Key verpflichten, d.h. zu allen mit diesem Public Key verifizierbaren Signaturen. Diese Verpflichtung bedeutet, dass rein digitale Evidenz – eine Bitfolge oder eine Zahl – darüber entscheidet, ob der Benutzer haftet.
Offensichtlich muss verhindert werden, dass eine Signatur ohne Willensakt des Benutzers erzeugt werden kann. Insbesondere muss der geheime Schlüssel vor Dritten geschützt werden, z.B. durch Einbettung in einem sehr sicheren Gerät. Zudem muss das Benutzerinterface klar darstellen, welcher Akt des Benutzers die Erzeugung der Signatur bewirkt. Aus Sicht des Benutzers bleibt aber das Risiko bestehen, dass jemand eine digitale Signatur präsentiert, ohne dass sich der Benutzer bewusst sein kann, eine solche geleistet zu haben. Technische Massnahmen können dieses für den Benutzer sehr abstrakte Risiko nicht völlig eliminieren, zumal letztlich auch nicht ausgeschlossen werden kann, dass das kryptografische Verfahren gebrochen wird.

Der tiefgreifende Unterschied zur handschriftlichen Unterschrift ist, dass der Akt des regulären Unterschreibens als Dokumentation des Willensaktes interpretiert werden kann. Eine Person muss sich gezwungenermassen bewusst sein, ob eine vorliegende Unterschrift echt oder gefälscht ist. Sie kann darüber – z.B. unter Eid – aussagen. Eine solche Garantie des Bewusstseins besteht bei der digitalen Signatur nicht, da zwischen einer Signatur und ihrer Erzeugung kein realer Zusammenhang besteht. Einer Bitfolge sieht man unmöglich an, wann, wo, durch wen und unter welchen Umständen sie erzeugt wurde.

Dieses Problem könnte zumindest für bestimmte Anwendungen gelöst werden, indem der Willensakt speziell dokumentiert wird, z.B. durch die Aufzeichnung der Stimme der Person, die sich mündlich mit den Eckdaten des Vertrages einverstanden erklärt, oder durch ein Bild oder eine Videosequenz. Diese Information kann zusammen mit dem Vertrag signiert werden. Somit besteht für den Benutzer die beruhigende Gewissheit, im Streitfall das Vorspielen der Stimme verlangen zu können. Selbst wenn das Stimmsignal – wie eine Unterschrift – möglicherweise gefälscht sein kann, so ist für die betroffene Person zumindest klar, ob eine Fälschung vorliegt oder nicht.

Obwohl digitale Evidenz im Kontext der umfassenden Digitalisierung ein zentrales Thema wird, ist sie noch nicht genügend verstanden. Das hindert uns allerdings nicht, erste Erfahrungen mit digitalen Signaturen und PKI zu sammeln, wenn wir bereit sind, auf Grund der Erfahrungen die technischen Systeme und die Gesetzgebung laufend zu überarbeiten. •

Web et sphère privée

Dr Emmanuel Benoist
Membre de V.I.P

Emmanuel Benoist

L'anonymat sur Internet est un leurre. Du fait de son absence physique, l'internaute se croit à l'abri derrière son écran. Cet article présente quelques techniques qui peuvent être mises en jeu pour rechercher des informations personnelles. C'est le cas par exemple des cookies et des sessionIDs. La récolte d'informations sur Internet se différencie de ce qui se fait dans le monde réel par la possibilité de noter tous les faits et gestes des visiteurs et par l'internationalisation des échanges qui interdit pratiquement tout recours à une instance judiciaire. Mais la protection de la sphère privée est maintenant devenue un sujet à étudier et l'instance chargée d'écrire les normes du Web (le W3 Consortium) vient de publier un nouveau standard, la Platform for Privacy Preferences (P3P).

• Depuis 1999 Professeur à l'Ecole d'Ingénieurs de Bienne (HTA Biel)

Spécialisté dans les techniques du Web
-> Protocole HTTP
-> Applications PHP
-> Java Server Pages (Tomcat, Servlet, JSP, Struts)
-> Flash,
-> ...

Projets en cours ou déjà réalisés:
-> Prototype de e-Voting
-> Internet Tracking System
-> Revue de Presse Quotidienne On-Line
-> Solution Intranet de Facturation pour micro-entreprises

• 1997-1999 Co-Fondateur de la société de création de sites Web Normanet
• 1995-2000 Doctorat de l'Université de Caen (France) en Algorithmique
"Génération à délai polynomial pour le problème SAT"
• 1995 Travail de Diplome à l'Université de Paderborn
"Generator of Random Formulas"
• 1990-1995 Etudes d'informatique à l'Université de Caen - France

Sur Internet, s'est super, on peut surfer comme on veut, on est complètement anonyme. Personne ne sait qui est qui. Cette phrase mainte fois entendue ne reflète qu'une partie de la réalité.

Sur le réseau, tous les faits et gestes des internautes sont enregistrés et peuvent être étudiés et ensuite utilisés à des fins plus ou moins avouables. Nous allons ici présenter quelques techniques qui, utilisées par des personnes mal intentionnées peuvent être dévastatrices pour la sphère privée des internautes. Le principal outil utilisé pour récolter

des données est le cookie. Il s'agit d'une petite information qui est envoyée depuis le serveur vers le browser pour y être stockée. Elle sera ensuite incluse automatiquement dans toute requête du browser vers ce même serveur (et vers aucun autre). Ce principe peut être utilisé par le serveur pour stocker un peu d'information sur la personne qui surfe, par exemple sa langue, pour que celle-ci soit automatiquement activée lors de chaque visite. C'est aussi un cookie qui est utilisé pour empêcher une personne de participer plusieurs fois à un sondage en ligne. On envoie une information "a déjà voté" vers le browser qui ensuite, à chaque nouvelle tentative de participer au scrutin, renvoie "a déjà voté" vers le serveur, lequel ne l'autorise donc pas à voter une seconde fois.

Ces données doivent rester très petites, car elles doivent être renvoyées lors de chaque requête vers le serveur (c'est-à-dire lors du téléchargement de chaque nouvelle page ou de chaque nouvelle image). Comme les données personnelles sont de plus en plus grandes, on a dû trouver une solution permettant de les stocker directement sur le serveur. Cela est fait en utilisant un cookie unique contenant un nombre, appelé sessionID, qui permet d'accéder à toutes les données concernant le client qui sont conservées sur le serveur. Par exemple les sites de commerce électronique utilisent un sessionID pour conserver les articles insérés dans le panier virtuel du client. Un sessionID est aussi utilisé pour identifier le visiteur d'un site qui est protégé par un mot de passe. Ce sont donc les cookies qui sont utilisés pour récolter les informations les plus privées sur les internautes.

Internet est international, c'est sa force, mais aussi une grande faiblesse

En Suisse de très nombreux clients de supermarchés utilisent une carte de fidélité lors de chacun de leurs passages en caisse (cartes Cumulus ou Supercard par exemple). Dans ce cas, le client vend au magasin le droit d'utiliser ses données personnelles en échange de promotions et d'un rabais sur le total des achats. Ces données sont très sensibles.

On pourrait par exemple imaginer qu'un employeur serait intéressé de savoir si une de ses employée a acheté un test de grossesse. Qu'une compagnie d'assurance voudrait connaître la consommation d'alcool et de tabac d'un nouvel assuré avant de l'admettre. Mais dans ce cas, l'utilisateur pourrait se retourner contre le supermarché. La carte de fidélité a fait l'objet d'un contrat écrit entre le client et la chaîne de magasins, ceux-ci étant tous deux en Suisse, tout cela se terminerait très vite devant un tribunal. Mais il en va tout autrement sur Internet. Internet est international, c'est sa force, mais dans le cas de la protection des clients, c'est une grande faiblesse. Pourquoi un site basé aux Etats-Unis ou aux Bahamas devrait se conformer aux règles édictées en Suisse?

Lorsque l'on fait des achats dans un magasin, les informations collectées concernent uniquement les articles achetés. Sur le net, bien évidemment ces articles sont répertoriés, mais l'administrateur peut de plus avoir accès à toutes les pages visitées, ainsi qu'au temps passé sur chaque page. Il peut donc connaître les points d'intérêts du client avant même qu'il n'achète la marchandise. Et donc, lui présenter la bonne promotion au bon moment. Certains utilisateurs peuvent accepter que ces données soient utilisées en interne à des fins promotionnelles, mais de nombreux sites vendent ces données à des tiers. Que se passera-t-il si les données arrivent chez un banquier, un assureur ou un employeur potentiel?

Cela ressemble un peu à de la science-fiction

Des données encore plus personnelles car concernant les opinions politiques, les préférences sexuelles ou l'avenir professionnel de l'internaute se trouvent sur des sites tels que les journaux, les sites pornographiques ou les sites d'offre d'emploi. Il est très rare

qu'un client laisse ses coordonnées sur de tels sites. Comme les cookies, qui sont le principal moyen pour récolter des données personnelles sont spécifiques à chaque site, il n'est pas possible de les utiliser pour regrouper les données de plusieurs serveur (et donc associer un nom aux opinions politiques ou sexuelles). Mais il existe une solution techniquement un peu compliquée pour regrouper les données de plusieurs sites. Il faut créer un site "espion" qui sera chargé de regrouper les données personnelles des internautes depuis plusieurs sites.

Tous les sites participant incluent dans chacune de leurs pages une image invisible (1 pixel sur 1 pixel) qui est téléchargée automatiquement depuis le site espion. L'échange d'informations personnelles entre les sites se fait par l'intermédiaire de ces images.

Tout cela ressemble un peu à de la science-fiction. Revenons un peu les pieds sur terre, ou plutôt sur le net. Allons maintenant sur le site de TF1 (un des plus visités de la francophonie). Une fois la première page chargée faisons "View Source" dans le browser. Le code HTML de la page s'affiche, après une courte recherche, nous allons trouver le bout de code suivant:

```
<img width="1" height="1"
  src="http://logp3.xiti.com/hit.xiti?c
c=2&cs=1&cs2=1&p=/home" />
```

Chaque internaute visitant une page quelconque du site de TF1 envoie ainsi un message au serveur xiti.com. Il en est de même pour tous ceux qui visitent les sites suivants: Nestle, Bouygues Telecom, Aventis-Pasteur, Heineken, 20th Century Fox, Roche, Sanofi-Synthelabo, Bayer, ANPE, La Poste (France), Cadremploi, Zdnet, Sopexa, Ecole Nationale des Télécoms, Shisheido, Sisley, Essec, Hec, Sup de CO Bordeaux, Corsica Ferries, Sernam, Mamounia (Marrakech), Canalclub, Le Matin. On imagine la combinaison des données venant de l'ANPE (Agence Nationale Pour l'Emploi) de Heineken et de TF1! Si l'on regarde encore plus bas sur le site de la chaîne française TF1, on tombe encore sur un lien du même style vers le site de l'institut de sondage Médiamétrie qui rassemble tous les médias français.

Les cookies sont indispensables au commerce électronique

Une solution simpliste pour protéger la vies privées des internautes est de bannir totalement tous les cookies d'Internet. Mais cela est impossible, ils sont totalement indispensables au commerce électronique ainsi qu'à de très nombreux autres sites. Le W3 Consortium (l'organisme chargé d'écrire les futurs standards du Web) a défini une Plateforme pour la Protection de la vie Privée (P3P) qui permet à chaque site web de décrire l'usage qu'il fait des données qu'il collecte.

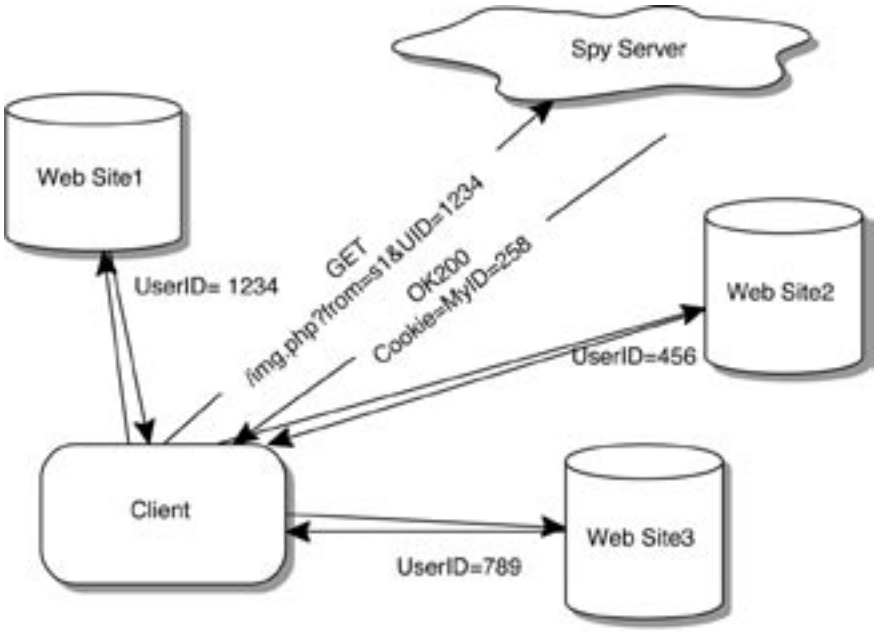
L'administrateur doit répondre à des question comme:

- Quelles données collectez-vous?
- Au bout de combien de temps les données sont-elles effacées?
- Dans quel but sont-elles gardées (Marketing ou statistique)?
- Ces données sont-elles revendues à des tiers?
- Qui peut certifier que le site respecte bien ses engagements?
- Auprès de quelle instance peut-on porter plainte en cas d'abus? …

Ensuite de plus en plus de browser (Netscape7 le fait déjà partiellement) permettront à l'utilisateur de définir le degré de protection qui lui convient pour ses données personnelles. Ainsi il pourra stopper automatiquement toute transaction avec les sites ne respectant pas sa vie privée.

Les sites de TF1, xiti et médiamétrie implémentent déjà cette nouvelle norme, et l'on peut donc vérifier que l'usage prévu pour les données semble correspondre à ce que l'on attend d'eux. Dans la "privacy policy" ces sites donnent de plus l'instance auprès de laquelle on peut déposer plainte en cas de problème.

Depuis les débuts d'Internet, la protection de la sphère privée n'a jamais été une priorité. Elle semble enfin devenue un sujet digne d'intérêt (du moins sur le vieux continent). Il reste maintenant à sensibiliser les internautes aux risques pour qu'ils deviennent des consommateurs critiques de toutes ces technologies. •|



Computergestütztes Identitätsmanagement für mehr (Selbst-)Datenschutz

Marit Hansen

Marit Hansen

In diesem Beitrag wird dargestellt, welche Funktionalität ein datenschutzförderndes Identitätsmanagementsystem erfüllen kann. Aspekte der Architektur eines Identitätsmanagers in Nutzerhand werden ebenso angesprochen wie die Rollen und Aufgaben weiterer Akteure, die zu einem funktionierenden Identitätsmanagement beitragen können. Danach wird skizziert, wie sich das Konzept von umfassenden datenschutzfördernden Identitätsmanagementsystemen in die Praxis umsetzen lässt.

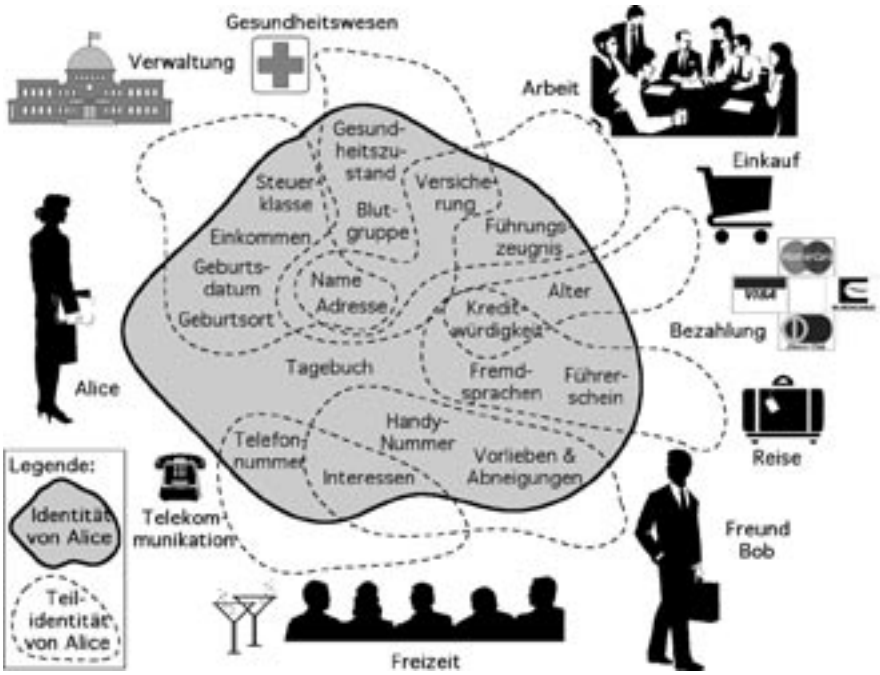
Marit Hansen ist Informatikerin und Leiterin der Abteilung "Privacy Enhancing Technologies (PET)" am Unabhängigen Landeszentrum für Datenschutz Schleswig-Holstein (staatliche Datenschutzaufsichtsbehörde). Seit ihrem Diplom 1995 befasst sie sich mit Datensicherheits- und Datenschutzaspekten insbesondere in Bezug auf das Internet, Anonymität, Pseudonymität, Identitätsmanagement, Biometrie, mehrseitige Sicherheit und e-Privacy, und zwar sowohl aus technischer als auch aus rechtlicher Perspektive. Im Rahmen mehrerer Projekte waren sie und ihr Team aktiv am Technologiedesign beteiligt, um PET zu unterstützen und Gesetze zu kommentieren.

Marit Hansen is a computer scientist and is head of the "Privacy Enhancing Technologies (PET)" Section at the Independent Centre for Privacy Protection Schleswig-Holstein (the state privacy commission), Germany. Since her diploma in 1995 she has been working on security and privacy aspects especially concerning the Internet, anonymity, pseudonymity, identity management, biometrics, multilateral security, and e-privacy from both the technical and the legal perspectives. In several projects she and her team actively participate in technology design in order to support PET and give feedback on legislation.

Menschen verhalten sich je nach Kontext und Situation unterschiedlich. Beispielsweise teilen sie ihren Kommunikationspartnern Unterschiedliches über sich selbst mit, je nachdem, was sie gerade für richtig halten. Damit nehmen sie ihr Recht auf informationelle Selbstbestimmung, das besagt, dass jeder wissen soll, wer was wann über ihn weiß,[1] selbst in die Hand: Sie bestimmen, wem sie welche Information geben. Dies ist Identitätsmanagement.

Die Abbildung zeigt verschiedene Gruppen von Daten, die Alice in unterschiedlichen Kontexten und gegenüber unterschiedlichen Parteien preisgibt. Diese Datengruppen stehen für die sog. Teilidentitäten [ClKö_01], die zusammengenommen die Identität von Alice bilden.[2] Identitätsmanagement bedeutet also die Verwaltung von eigenen Teilidentitäten.[3]

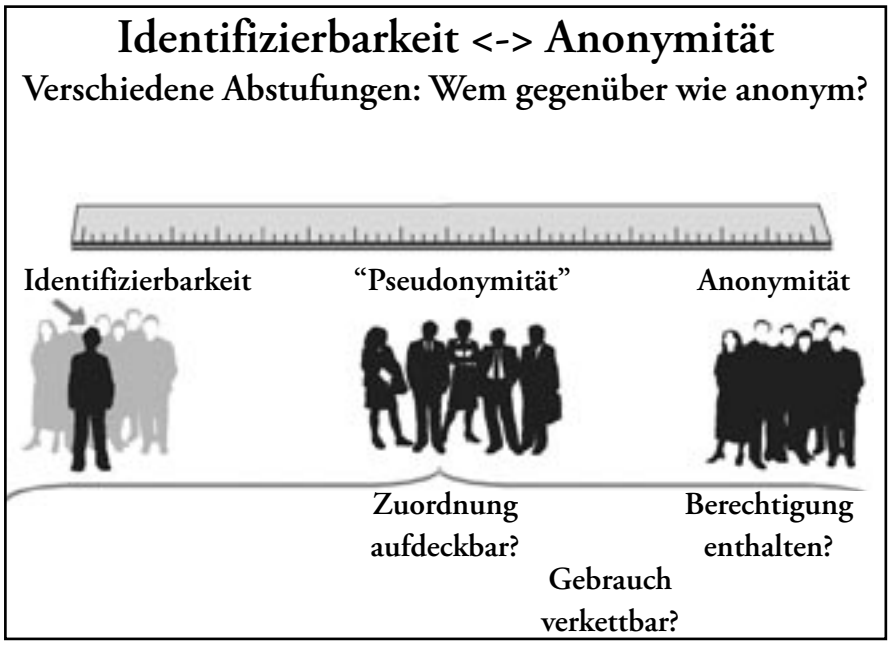
In der digitalen Welt können Identitätsmanagementsysteme Nutzer bei der Entscheidung unterstützen, wem sie in welchem Kontext und unter welchen Bedingungen welche Daten über sich offenbaren wollen. Dies bedeutet, dass der Nutzer bei der Preisgabe Auswahl und Umfang seiner personenbezogenen Daten steuern kann oder – sofern er hierüber nicht frei entscheiden kann, z.B. weil diese Freiheitsgrade rechtlich oder von der Applikation nicht vorgesehen sind – dass er zumindest darüber informiert ist, welche Daten wem zur Verfügung zu stellen sind. Auch der Personenbezug lässt sich mit einem datenschutzfreundlichen Identitätsmanagementsystem[4] steuern, indem verschiedene pseudonyme Kennungen verwendet werden.[5] Damit zielt ein solches Identitätsmanagementsystem ab auf eine nutzergesteuerte (Un-)Verkettbarkeit seiner eigenen Daten im Sinne des Selbstdatenschutzes [KöPf_01].

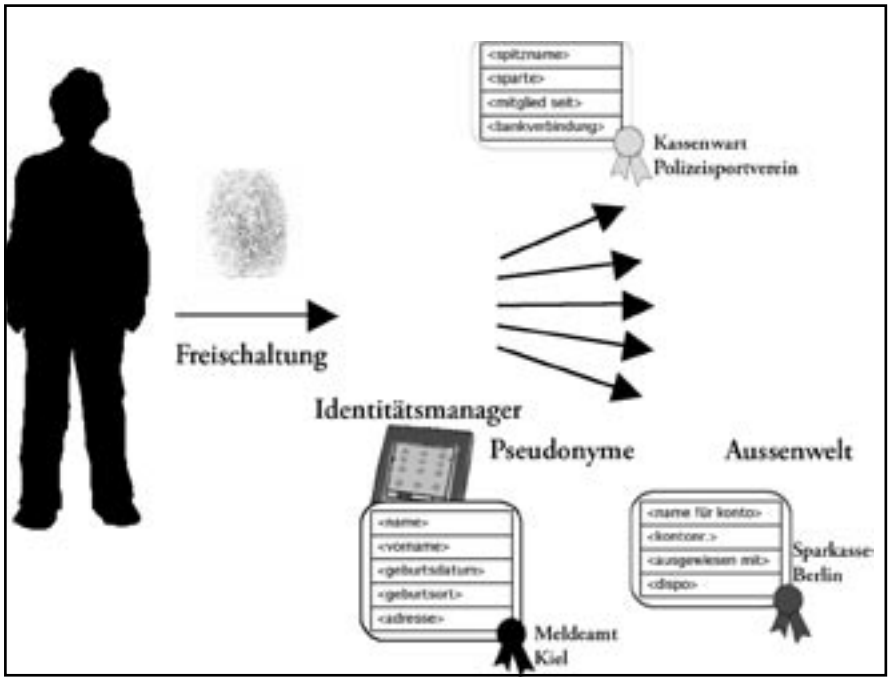


Identitätsmanagement – wie geht's?

Ein Identitätsmanager kann nur dort beim Verwalten der Teilidentitäten helfen, wo er auch in die Kommunikation eingeschaltet wird. Für ein umfassendes Identitätsmanagement in der digitalen Welt bietet sich eine Realisierung in einem Gerät an, das der Nutzer in der Regel bei sich hat, z.B. in einem Handy oder in einem Personal Digital Assistant (PDA). Natürlich kann Identitätsmanagement im Internet auch über den Browser beim Nutzer oder über vertrauenswürdige Proxies realisiert werden.

Der Identitätsmanager sollte alle Freiheitsgrade zwischen Anonymität und Identifizierbarkeit modellieren können. Beispielsweise sollte er dem Nutzer dort, wo kein Personenbezug





notwendig oder wünschenswert ist, Anonymität bieten. Wo Authentizität und Zurechenbarkeit bedeutsam sind, sollte er beispielsweise mit Zertifikaten und digitalen Signaturen arbeiten. Dies steht nicht unbedingt im Widerspruch zur Anonymität: Ein Mechanismus, um auch Autorisierungen unverkettbar zu realisieren, sind Credentials. Bei Credentials handelt es sich um umrechenbare Beglaubigungen im digitalen Format, durch die sich Autorisierungen, die ein Nutzer unter einem Pseudonym erworben hat, auf andere seiner Pseudonyme übertragen lassen, ohne dass sie auf die anderer Nutzer transferiert werden können [Chau_85]. Mit Hilfe der gleichen Credentials unter verschiedenen Pseudonymen kann einer Verkettbarkeit entgegengewirkt werden.

Die ganze Bandbreite zwischen Identifizierbarkeit und Anonymität wird umfasst von Pseudonymität [PfKö_01]. Die gewählten Pseudonyme, die die Teilidentitäten repräsentieren, können verschiedene Eigenschaften aufweisen. Von besonderer Bedeutung ist das Wissen über die Zuordnung zwischen einem Pseudonym und seinem Inhaber und damit verbunden auch die Möglichkeit der Aufdeckung durch die Parteien, denen diese Zuordnung bekannt ist. In einigen Applikationen werden die Nutzer verpflichtet sein, Pseudonyme zu verwenden, die in vorher definierten Fäl-

len, beispielsweise im Falle eines Missbrauchs, aufgedeckt werden können. Ein anderer Punkt besteht in der Verkettbarkeit bei Verwendung des Pseudonyms in verschiedenen Kontexten: Als Standard könnte ein Identitätsmanagementsystem stets Transaktionspseudonyme verwenden und nur dann Pseudonyme wiederverwenden, wenn der Nutzer dies ausdrücklich wünscht, um z.B. an vorigen Pseudonymgebrauch anzuknüpfen und ggf. eine Reputation aufzubauen oder einen Bonus in Anspruch zu nehmen.

Es ist in den Applikationen zu definieren, welche Anforderungen an das Pseudonym und seine Verwendung gestellt werden und in welchem Bereich der Nutzer über Freiheitsgrade in Bezug auf die Pseudonymwahl und –verwendung verfügt.

Um den Nutzer zu informierten Entscheidungen über die Preisgabe seiner Daten zu befähigen, muss der Identitätsmanager ihm möglichst viel Transparenz bieten. Insbesondere soll der Nutzer die Möglichkeit haben, die Verarbeitung seiner Daten (oder zumindest die von ihm getroffenen Entscheidungen sowie die zugehörigen Entscheidungsgrundlagen) auch später noch nachvollziehen zu können. Diese zu diesem Zweck angelegten Logdateien sollen den Nutzer auch darüber informieren, was die Kommunikationspartner bisher über ihn in Erfahrung gebracht haben. Dabei kann ihn ein "Privacy Information Service" unterstützen, der ggf. zusätzliche Informationen über die Datenverarbeitung oder ihr Umfeld zuliefert. Außerdem kann ein Identitätsmanager den Nutzer beim Wahrnehmen seiner Datenschutzrechte, z.B. dem Abwickeln von Auskunfts-, Berichtigungs- oder Löschungsbegehren sowie von Einwilligung und Widerspruch, unterstützen.

Identitätsmanagement – was tun?

Die Bausteine für ein datenschutzgerechtes Identitätsmanagementsystem sind vorhanden. Jetzt gilt es, solche Systeme auch tatsächlich zu entwickeln und verfügbar zu machen. Allerdings reicht es nicht aus, dem Nutzer Tools an die Hand zu geben, die er auf seinem Rechner installiert. Statt dessen muss ein wirklich funktionierendes Identitätsmanagement auch von der Umgebung des Nutzers unterstützt werden [CHHP_02].

Dazu gehört, dass die Kommunikationspartner, z.B. Webserver-Betreiber, die Nutzer über die Verwendungsmöglichkeiten von (möglichst unverkettbaren) Pseudonymen informieren (z.B. im Rahmen von Datenaustauschprotokollen, bei denen Anfang und Ende von Transaktionen, in denen eine Verkettbarkeit erforderlich ist, gekennzeichnet sind oder bei denen Kontextwechsel angekündigt werden). Weiterhin können sie in ihre Applikationen unmittelbar Datenschutzkontrollfunktionalität für den Nutzer einbauen, so dass dieser online und ohne zusätzlichen Aufwand seine Datenschutzrechte, wie z.B. Auskunft, Berichtigung, Löschung, Einwilligung und Widerspruch, wahrnehmen kann.

Ferner bedarf es eines anonymen Fundaments, also einer Netzinfrastruktur, die eine Beobachtung des Nutzer(verhaltens) durch Dritte wie z.B. Telekommunikations- und Netzbetreiber ausschließt. Sonst macht eine differenzierte Behandlung von Teilidentitäten und eine Kontrolle über (Un-)Verkettbarkeit auf Anwendungsebene nur eingeschränkt Sinn.

Auch andere Infrastruktur ist beim Identitätsmanagement gefragt, z.B. Credential-Aussteller und eine PKI für alle möglichen Arten von digitalen Signaturen und Zertifikate. Ebenso können Treuhänder einbezogen werden, die in bestimmten Fällen die Pseudonymzuordnung zu Personen verwalten oder einen Haftungsservice realisieren. Schließlich können datenschutzfreundliche Bezahl- und Lieferservices das Identitätsmanagement unterstützen. Nutzer können nur dann ihre eigenen Datenschützer mit Hilfe von Identitätsmanage-

mentsystemen sein, wenn ihnen ihre Rechte und die jeweiligen Situationskontexte bewusst sind. Daher ist die Usability der Identitätsmanagementsysteme und die Ausbildung, wie man mit ihnen umgehen sollte, von großer Bedeutung. Hier muss der Staat künftig unterstützen, möchte er die mündigen Bürger fördern, die die Verantwortung über den eigenen Datenschutz souverän übernehmen. •|

Literatur

- [Chau_85] David Chaum: Security Without Identification: Transaction Systems to Make Big Brother Obsolete. In: Communications of the ACM, Vol. 28 No. 10, Oktober 1985; 1030-1044.
- [CHHP_02] Sebastian Clauß, Marit Hansen, Els Van Herreweghen, Andreas Pfitzmann: Privacy-Enhancing Identity Management; in: IPTS-Report 67 (September 2002); JRC Seville, 2002; 8-16.
- [ClKö_01] Sebastian Clauß, Marit Köhntopp: Identity Management and Its Support of Multilateral Security; in: Computer Networks 37 (2001), Special Issue on "Electronic Business Systems", Elsevier, North-Holland 2001; 205-219.
- [KöPf_01] Marit Köhntopp, Andreas Pfitzmann: Informationelle Selbstbestimmung durch Identitätsmanagement; in: it+ti Informationstechnik und Technische Informatik, Schwerpunktthema "IT-Sicherheit" 5/2001; Oldenbourg Wissenschaftsverlag, München, September 2001; 227-235.
- [PfKö_01] Andreas Pfitzmann, Marit Köhntopp: Anonymity, Unobservability, and Pseudonymity – A Proposal for Terminology; Draft v0.12, 2001-06-17, http://www.koehntopp.de/marit/pub/anon/; v0.8 in: Hannes Federrath (Hrsg.): Designing Privacy Enhancing Technologies; Proc. Workshop on Design Issues in Anonymity and Unobservability; LNCS 2009; 2001; 1-9.

1. In Deutschland grundlegend im Volkszählungsurteil, BVerfGE 65, S. 1 ff., 1983.

2. Genau genommen ist die eigene Identität noch komplexer, als die Abbildung suggeriert, denn die Identität lässt sich nicht auf Datenfelder reduzieren. Außerdem sind die dargestellten Parteien keinesfalls als monolithisch zu interpretieren, sondern sie können diverse Kommunikationspartner umfassen, die wiederum nur eine Sicht auf gewisse Ausschnitte des gesamten Datenumfangs von Alice' Identität haben. Auch kann das Bild, das sich ein Kommunikationspartner von einem macht, wiederum Einfluss auf die eigene Identität haben oder lässt sich ihr zurechnen.

3. Daher wird manchmal auch von "Identitätenmanagement" gesprochen.

4. Der Begriff "Identitätsmanagement" wird heutzutage für sehr unterschiedliche Anwendungen benutzt. Die aktuell verfügbaren Systeme sind häufig jedoch nicht auf Datenschutz ausgerichtet und in einigen Fällen sogar als datenschutzfeindlich einzustufen.

5. Dies ist in der digitalen Welt von besonderer Bedeutung, da bei einer Verwendung desselben Namens all diese Vorkommen grundsätzlich verkettbar sind. Damit ließen sich Profile über alle Lebensbereiche hinweg anlegen. In der Tradition der Offline-Welt sind Pseudonyme hauptsächlich als Künstler- oder Spitznamen verbreitet; ansonsten ist man gewohnt, seinen Namen zu nennen oder ganz namenlos zu bleiben.

Die sogenannte digitale bzw. elektronische Identität

Bemerkungen eines Datenschützers

Michael Schnyder

Michael Schnyder

Michael Schnyder ist lic. iur. (Uni BS 1984) und dipl. inf. (Uni FR 1994). Mit Informatik beschäftigt er sich seit 1986, ursprünglich mit Schwergewicht Information Retrieval und Sprachverarbeitung und seit annähernd 10 Jahren im Bereich Informatiksicherheit und Datenschutz. Er ist IBM certified Security Consultant und beim EDSB unter anderem für den Bereich e-Government zuständig.

Wer sich mit Vor- und Nachteilen sogenannter digitaler oder elektronischer Identität befasst, riskiert auf einer undifferenzierten Ebene der Schlagworte zu verharren. Deshalb setzt sich der erste Teil des folgenden Beitrags zusammen aus Überlegungen zum begrifflichen Fundament und zu den Schwierigkeiten, welche aus dessen Mängeln entstehen. Insbesondere fragt sich, welches der Bedeutungsgehalt der Ausdrücke "Identität" und "Identifikation" ist. Im zweiten Teil werden einige – nicht nur technische – Lösungsansätze skizziert, soweit diese heute realistisch erscheinen.

Begriffliches und Problemschilderung "Identität" hat mehrere Dimensionen und entsprechend gibt es für das Wort verschiedene Definitionen. Die allgemeine Definition nach Brockhaus ("völlige Übereinstimmung einer Person oder Sache mit dem, was sie ist oder als was sie bezeichnet wird") scheint auf den ersten Blick klar. Bei genauerem Hinsehen erweist sich, dass sich daraus für die spezifischen Bereiche nur wenig ableiten lässt. Zwar gibt es präzisere Definitionen für die Bereiche der Logik und Mathematik sowie in beschränkterem Rahmen für Psychologie und Soziologie. Für den Bereich der Bürokratie sind aber gerade unter dem Gesichtspunkt von Sicherheit und Datenschutz bisher keine Definitionen erarbeitet, welche einen nützlichen Sinngehalt aufweisen. Hier schwingt stets die Vorstellung aus dem allgemeinen Sprachgebrauch mit, wonach "man weiss, um wen es sich handelt". Diese Vorstellung trifft jedoch bloss einen der wesentlichen Aspekte von Identität, den man einen umfassenden nennen kann. Es mag sein, dass der Sprachgebrauch intuitiv mit der Identitätsdefinition aus dem Bereich der Logik verbunden ist und deshalb nur die "äussere Grenze" von Identität betont. Auf jeden Fall besteht die Tendenz zu übersehen, dass jedes Individuum mehrere Teil-Identitäten besitzt. Diese Tendenz ist verbunden mit der (Wunsch-)Vorstellung, es gäbe so etwas wie absolut sichere Identität sowie mit dem im Zeitalter des Krieges gegen Terrorismus wachsenden Bestreben, Individuen möglichst vollständig zu überwachen. Mit solcher Betrachtung wird jedoch das (Erfolgs-)Resultat der Bestrebungen vorausgesetzt und implizit negiert, dass die historisch gewachsene Situation von Individuen mit Teil-Identitäten eine grundsätzlich sinnvolle Sache ist. Nicht ganz unwesentlich ist in diesem Zusammenhang auch, dass unsere Rechtsordnung das Recht, unter Pseudonymen zu handeln in gewissem Rahmen durchaus akzeptiert. Wenn nun aufgrund staatlich verordneter Ausgabe von Identitätszertifikaten an die Bürger diese verschiedenen Teilidentitäten "zusammengelegt" werden sollten,

so wäre dies für den Datenschutz eine bedenkliche Entwicklung[1]. Damit ist in keiner Weise gesagt, dass wir in der Schweiz schon soweit wären. Die Versuchung auf Seiten der Bürokratie ist jedoch gross, eine relativ moderne Technologie unter dem Titel "elektronische Identität" einzuführen und dabei in erster Linie an Datenaustausch "Information Sharing" zwischen Behörden zu denken[2].

Zu den Unbestimmtheiten von "Identität" kommen bei "Identifikation[3]" noch weitere, und zwar auch wenn wir uns auf den Bereich der Verwaltung bzw. Amtshandlungen beschränken. Zum einen sind hierbei verschiedene Konstellationen möglich, z.B.:

- Wachtmeister Studer identifiziert eine Leiche.
- Ich gehe zum Amtschalter und identifiziere mich.
- Die Flughafenpolizei identifiziert einen gesuchten Verbrecher mittels einer Überwachungskamera in Verbindung mit einem Gesichtserkennungssystem.
- Ein Unique Airport Checkin-System identifiziert mich aufgrund einer Kennung meines Mobiltelefons.

Es ist also nicht so, dass aus dem Wort Identifikation schon hervorgeht, ob die identifizierte Person dabei eine aktive oder eine passive Rolle spielt. Ebenso sagt uns das Wort nicht, ob die zu identifizierende Person aus einer Menge heraus identifiziert wird oder nicht[4].

Für Datenschutz und Datensicherheit ist sodann bedeutsam, dass Identifikation für sich allein wenig bedeutet, sondern immer in einem bestimmten Zusammenhang geschieht. Identifiziert wird immer im Hinblick auf etwas, etwa die Inanspruchnahme einer Dienstleistung oder die Verfolgung einer Straftat. Mit der Formulierung, eine elektronische Identitätskarte würde nur zu Identifikationszwecken eingesetzt, ist so gesehen kaum etwas gesagt. Es kommt eben darauf an, im Hinblick worauf identifiziert wird. Dies gilt insbesondere für die jeweiligen Anforderungen an die Sicherheit in all Ihren Dimensionen. Im Zusammenhang mit Identifikation für eGovernment und eBusiness ist Roger Clarkes Definition von "Identity Authentication" vielleicht die nützlichste. Er definiert dies als "den Prozess, wodurch ein genügendes Mass an Vertrauen hergestellt wird, dass die Identifikation ein korrektes Resultat geliefert hat[5]". Welches Mass ein genügendes ist, hängt sehr stark vom Umfeld bzw. von den mit dem aktuellen Geschäftsfall verbundenen Risiken ab.

Zusammenfassend ist zu sagen, dass das begriffliche Fundament für die untersuchten Ausdrücke im hier interessierenden Bereich recht dürftig ist. Diese Tatsache muss sich jeder vor Augen halten, der mit diesen Worten operiert. Wer sie übersieht, riskiert durch undifferenzierte Äusserungen Missverständnisse zu propagieren und im Resultat auch schlechten "Lösungen" Vorschub zu leisten, welche u.U. nur Kosten und mangels Akzeptanz keinen bzw. kaum Nutzen bringen.

Weiter muss aus der Sicht von Datensicherheit und Datenschutz vor der fehlerhaften Annahme gewarnt werden, es gäbe eine Möglichkeit zur absolut sicheren Feststellung von Identitäten. Einerseits wäre die Basis zur allfälligen Einführung eines solchen Systems in den herkömmlichen papierbasierten Systemen, deren Mängel und Fehler weitervererbt würden. Andererseits könnten auch dann Identitäten irrtümlich verwechselt oder absichtlich gefälscht werden[6]. Im übrigen ist nicht zu vergessen, dass die kriminelle Energie, welche für sogenannten Identitätsdiebstahl (Identity Theft) eingesetzt wird, umso grösser sein wird, je mehr sich mit einer gestohlenen Identität machen lässt. Dieses Element des Risikomanagements geht in den meisten Überlegungen zu sogenannten elektronischen Identitäten vergessen, weil die ebenfalls fehlerhafte Annahme dominiert, es liesse sich durch Technik allein Sicherheit herstellen.

Lösungsansätze

Nachfolgend werden einzelne Elemente eines aus Datenschutzsicht wünschbaren Vorgehens aufgezeigt. Ein vollständiger und umfassender Ansatz kann im Moment nicht präsentiert werden, weil die Folgen einer Einführung von digitalen Identitäten sogar noch weniger geklärt sind als die Bedeutung der oben untersuchten Ausdrücke. Entsprechend fordern denn auch Riedl und Richter ein Forschungsprogramm zum Thema digitale Identität[7].

Ein erster Punkt ist das Beseitigen der erwähnten Fehlannahme, es gäbe absolute Sicherheit bezüglich Identität. Wenn schon von Identitätsnachweisen oder gar – beweisen gesprochen wird, muss stets klar sein, dass es sich dabei nicht um Beweise im Sinne von mathematischer Logik handeln kann, sondern eher um solche wie sie im Rahmen Gerichtsprozessen vorkommen. Irrtum ist dabei nie vollständig ausgeschlossen und die Frage, welches Mass an Gewissheit z.B. ein Vertragspartner bezüglich der Identität des anderen braucht, gehört zum Kontext seines Risikomanagements. Eine Analyse aus der Optik des Risikomanagements zeigt, dass je nach konkretem Anwendungsfall ganz unterschiedliche Grade von Gewissheit erforderlich sind. Als Beispiel für solche Unterschiede möge der Vergleich zwischen – vorläufig hypothetischen und schon realen – Geschäftsfällen des "eGovernment" dienen: Sehr strenge Anforderungen dürften gelten mit Bezug auf elektronisches Unterzeichnen einer Initiative oder Online-Einsichtnahme ins Strafregister, weitaus weniger strenge dagegen fürs elektronische Bestellen einer Wohnsitzbestätigung oder ein Gesuch um eine Parkkarte mit Anmeldung zur Dauerparkiergebühr.

Sodann scheint im Anschluss an diese Überlegung und vor dem tatsächlichen Einsatz von digitalen Identitäten folgender Schritt sinnvoll: Die Kategorisierung von Geschäftsfällen – sei es im eBusiness oder im eGovernment – mit dem Ziel diejenigen zu bezeichnen, welche überhaupt keine Identitätsfeststellung erforderlich machen. Wo dies der Fall ist, würde eine Arbeit mit Identitätsfeststellung das Verhältnismässigkeitsprinzip verletzen und dem daraus abgeleiteten Grundsatz der Datenminimierung widersprechen. Als Illustration für die durchaus relative Bedeutung einer Identitätsfeststellung mag die Bemerkung von Rolf Oppliger dienen, wonach der Online-Händler nicht in erster Linie wissen will, ob auf der anderen Seite ein Hund am PC sitzt. Ihn interessiert bedeutend mehr, das Risiko der Nichtbezahlung möglichst gering halten[8].

Als weiterer Ansatzpunkt liegt für den Datenschützer auf der Hand, sich bei Konzeption und Einführung an diejenigen Teil-Identitäten anzulehnen, welche bisher schon bestehen. Dieser Ansatz stellt zugegebenermassen das Konzept einer umfassenden digitalen Identität – d.h. ohne Segmentierung in Teil-Identitäten – in Frage. Er könnte sich aber für die Akzeptanz und Praktikabilität von elektronischen Identitäten als unentbehrlich erweisen. Zumindest für den Bereich der Privatwirtschaft ist der Akzeptanzaspekt ein zentraler, während man ihn im Bereich des Behördenverkehrs zumindest auf den ersten Blick ausser Acht lassen könnte, weil ja die Bürger zur Benutzung der elektronischen Identität für bestimmte Aktionen verpflichtet werden können.

Nebst den erwähnten Teil-Identitäten gibt es für den Datenschutz noch eine weitere Facette im Geschäftsverkehr, bei welcher sich datenschutzfreundliche Technologie einsetzen lässt. Es geht hierbei um die Geschäfte, bei welchen die eine Partei über bestimmte Eigenschaften (z.B. Volljährigkeit und Zahlungsfähigkeit) verfügen muss, die andere aber abgesehen davon nichts über sie zu wissen braucht. Im Hinblick auf die technische Implementation solcher datenschutzfreundlicher Systeme existieren erfolgversprechende Lösungsansätze[9], welche gedanklich auf David Chaums

Credentials basieren. Chaum definiert diese als "Aussagen betreffend ein Individuum, welche durch eine Organisation herausgegeben und in der Regel anderen Organisationen gezeigt werden[10]". Ausschlaggebend für den datenschutzspezifischen Nutzen der erwähnten Ansätze ist zunächst die Tatsache, dass die Aussagen von der letzteren Organisation geprüft werden können, ohne dass sie die Identität der betroffenen Personen kennen. Sodann können solche Credentials derart ausgestaltet werden, dass mehrere Credentials von einer Person einer Organisation "gezeigt" werden können, ohne dass die Organisation diese Aktionen untereinander zusammenführen kann (unlinkability property). Die neueren unter diesen Ansätzen erlauben durch zusätzliche Features wie "optional anonymity revocation" sogar den Einsatz in Gebieten, wo z.B. eine nachträgliche Notwendigkeit der Rückverfolgbarkeit von Anfang an eine für bestimmte Fälle absehbare Entwicklung darstellt. Es zeigt sich also, dass die Möglichkeiten zum Aufbau von sogenannten Identity Management Systemen sehr vielfältig sind. Damit allerdings "Identity Management" über die Schlagwortebene hinauskommt, braucht es nicht bloss technische Instrumente, sondern auch weitere Arbeiten auf dem Gebiet der Konzeption. Es sollte nicht eine in erster Linie durch Technik getriebene Entwicklung stattfinden. Der Vorrang gebührt vielmehr dem konkreten Beschreiben des Wünschbaren also der Anforderungen, welche das technisch zu unterstützende System erfüllen soll. Nebst der schon erwähnten Anforderung, dass das System schliesslich auf Akzeptanz stossen muss, dürften Anforderungen an die Benutzerfreundlichkeit – welche sich ebenfalls nur im konkreten Zusammenhang sinnvoll beschreiben lassen – eine der grössten Herausforderungen darstellen. •|

---

1 Zu den Gefahren der Linkability von Transaktionen des Benutzers einer PKIs mit Identitätszertifikaten vgl. Stefan A. Brands, "Rethinking Public Key Infrastructures and Digital Certificates: Building in Privacy", MIT Press Cambridge & London, 2000, ISBN 0-262-0249-8), S. 20 - 31

2 Reinhard Riedl und Lutz Richter erwähnen als primäre Ziele der Einführung digitaler Identitätskarten die Vorreiterrolle innnerhalb Europas und mehr Wissen über die Bevölkerung, als sekundäres Ziel eine Kostenreduktion und als seltenes Ziel den Bürgernutzen, vgl. «Digitale Identität – die unbekannte grosse Herausforderung" (http://www.ifi.unizh.ch/egov/egov-riedl-richter.pdf; gedruckte Publikation in: Wimmer, M. (Hrsg.): Impulse für e-Government: Internationale Entwicklung, Organisation, Recht, Technik, Best Practices. Tagungsband zum ersten eGov-Day des Forums eGovat, 15. Januar 2002. Wien).

3 "Identifikation" und "identifizieren" werden hier als Beschreibung des Prozesses der Identity Authentication (Definition vgl. Fn 5) verstanden.

4 Ein etwas klarerer Sprachgebrauch wurde im Zusammenhang mit biometrischen Systemen eingeführt: "Identification" bedeutet hier aus einer Menge heraus, während für die 1:1 Identifikation der Begriff "Identity Verification" geschaffen wurde. Dass aus solcher "Verification" hier immer nur ein bestimmtes Mass an Gewissheit entstehen kann, ist zwar der Biometriespezialistin völlig klar, geht aber aus dem Wort nicht hervor. Zusammen mit der Tatsache, dass manche Anbieter von Biometrieprodukten von "Proof of Identity" sprechen, stützt dieser Sprachgebrauch die fehlerhafte Annahme, es gäbe so etwas wie absolut sichere Identität.

5 "… process whereby a sufficient degree of confidence is established that the identification process has delivered a correct result." Vgl. Roger Clarke, Certainty of Identity: A Fundamental Misconception, and a Fundamental Threat to Security, http://www.anu.edu.au/people/Roger.Clarke/DV/IdCertainty.html

6 Vgl. Stefan A. Brands, a.a.O. (Fn 1) S. 11; Roger Clarke a.a.O. (Fn 5)

7 Reinhard Riedl und Lutz Richter a.a.O. (Fn 2), S. 9

8 Rolf Oppliger, «Von der PKI zum Trust Management – Möglichkeiten und Grenzen einer Schweizer PKI aus technischer Sicht", in digma Zeitschrift für Datenrecht und Informationssicherheit, 2001.2. S. 70-77

9 Vgl. dazu Stefan A. Brands, a.a.O. (Fn 1) und Jan Camenisch, Anna Lysyanskaya, "Efficient non-transferable anonymous multi-show credential system with optional anonymity revocation. In Birgit Pfitzmann, editor, Advances in Cryptology – EUROCRYPT 2001, volume 2045, pages 93-118. Springer Verlag, 2001; fast identischer Beitrag online verfügbar unter http://theory.lcs.mit.edu/~cis/pubs/lysyanskaya/cl01a.pdf; sowie Jan Camenisch und Els van Herreweghen «Design and Implementation of the Idemix Anonymous Credential System"(wird in naher Zukunft publiziert)

10 David Chaum, "Security without identification: Transaction system to make Bib Brother obsolete" in Communications of the ACM,28(10):1030-1044, October 1985, zitiert nach Stefan A. Brands, a.a.O. (Fn 1)

Privacy Rules for Intelligent Software Agents

Drs John J. Borking [1]

Drs John Borking (1945) (married, two daughters) is Director of Borking Consultancy established in 2002 and Associate Board Member of the Dutch Data Protection Authority. Till 1 January 2002 he was vice president of the Dutch Data Protection Authority (privacy commissioner) in The Hague (The Netherlands) and accountable for technology assessments, privacy audits and specific legal (ICT related) issues. He is member of the CEN IPSE standards steering group in Brussels. He is also arbitrator/ mediator and the secretary of the Dutch/ Belgian Foundation for Alternative Dispute Resolution for ICT disputes (SGOA). Further he is Board member of the Netherlands Gaming Control Board. He was till 1994 the General Manager of COSSO, the Dutch Association for Information & Telecommunication Technology Providers. He was also a former senior legal counsel for Xerox Corp. in Amsterdam, Venray, Lille and London.

He is author of "Third Party Protection of Software and Firmware" (1985 Amsterdam, New York), author and co-author of several Dutch books and many articles relating to computer law, software, data protection and computer contracts, etc in Dutch, English and German language.

He studied law, philosophy and social psychology at the Leyden university (Master degree Philosophy 1970 (Harlem) and Master degree Laws 1973 (Leyden) and computer law in 1983 at the Norwegian research center for computers and law at the Oslo university under supervision of Prof Dr J.Bing .

Coordinates:
Address for correspondence: LANGE KERKDAM 27 – 2242BN WASSENAAR- THE NETHERLANDS
Telephone numbers: HOME: 0031 70 517 94795, FAX: 0031 70 517 8936, OFFICE: 0031 62 958 2789,
EMAIL: jborking@euronet.nl

Intelligent Software Agent and the Objective of PISA

An Intelligent software agent or personal electronic butler (ISA) has been described[2] as software and/or hardware that are capable of acting autonomously in order to accomplish a task on behalf of its user in a complex network environment[3]. Thus it can act on its own without interference of the user. The ISA may have properties and attributes like mobility, deliberative behavior, and interaction with other ISAs, possibilities for identification and learning. ISA can appear in the role of a benevolent digital butler or a malicious digital criminal or as a means for constant surveillance. In order to perform properly ISAs need personal data, a profile of personal preferences and aversions for goods and services and non-personal identifiable information. The ISA gathers relevant task information, and personal data of both its user and others. The ISA will reveal personal data of the user according to his or her privacy protection level preferences. As the ISA processes automatically personal data the Directive 95/46/EC (DPD) or the national privacy legislation are applicable. Researchers are trying to prove in EU funded PISA project that personal data of the user is protected in all kinds of processes by incorporating privacy-protecting features into an ISA[4]. The question is: How to achieve this?

First we have to look at the question: What are personal data? In legal terms, personal data means any piece of information regarding an identified or identifiable natural person. Whether we can talk of 'personal data' depends on a number of elements of which, within the scope of this article, 'identification' is the only significant element. According to Article 2 of the EU Directive 95/46/EC, a natural person can be identified "directly or indirectly". Direct identification requires basic details collected in the PII (personal identifiable information). PII is name, address, a personal number, a widely known pseudo-identity, a biometric characteristic such as a fingerprint, etc. Indirect identification requires other unique characteristics or attributes or a combination of both, to provide for sufficiently identifying information[5].

Non-identification is assumed if the amount and the nature of the indirectly identifying data are such that identification of the individual is only possible with the application of disproportionate effort[6]. Whether we can talk of disproportionate effort depends, on the one hand, on the nature of the data and the size of the population; and on the other hand, the resources of time and money one is willing to spend in order to be able to identify the person[7].

Internet identifiers such as an IP address, browsing activities of a user, session login data and the listing of websites visited by an Internet user are classified as personal data.

The Privacy Threat Analysis (PTA)

There are various ways in which software agents can threaten privacy and related interests. Related interests denote interests that privacy helps to promote and which help to promote privacy like autonomy, integrity and dignity of an individual. Deliverable 7 of Work Package 2.1 of the PISA project contains an analysis of all relevant world-wide privacy legislation and in section 6.2 a methodology

for a privacy risk analysis[8]. It gives a description of a privacy consolidation approach to be built into software agents[9].

The PTA generates the following eight threats:

1. Secret possession of personal data [files];
2. Secret processing of personal data;
3. Out of bounds processing (violation of personal data constraints);
4. Out of law processing;
5. Out of jurisdiction processing;
6. Irresponsiveness to discontent;
7. Personal data deterioration;
8. Poor personal data constraints management.

Privacy-Enhancing Technologies (PET)

In order to achieve privacy protection at the DPD level the deployment of PET is required. ICT offers solutions in the shape of privacy protection for users, consumers and citizens. The application of ICT to protect privacy has become widely known under the name Privacy-Enhancing Technologies (PET or PETs)[10].

PET stands for a coherent system of ICT measures that protects privacy by eliminating or reducing personal data or by preventing unnecessary and/or undesired processing of personal data, all without losing the functionality of the data system[11]. PETs incorporated systems use Identity Protectors and create, anonymity, pseudonymity, unobservability and unlinkability[12]. As ISAs needs personal data to perform properly, PET as described here above isn't enough to protect privacy adequately. ISA needs also trust, secure environments and built-in knowledge about privacy law, privacy preferences of the user and an Agent Practices Statement, that is the privacy policy of the controller under whose responsibility the ISA moves though Internet. Furthermore transfer rules for personal data have to be formulated to allow the dissemination of personal data according to the preferences of the user of the agent.

Privacy Knowledge Engineering (PYKE)

In order to translate privacy law into machine-readable code and into the ISA a method has been developed to realize privacy knowledge engineering (PYKE). As the legislation is often complex and laced with many exceptions, the solution is found in working with a simplification of the data protection legislation by using the privacy principles as adopted in the 1981 Convention 108 of the Council of Europe, while retaining the capacity to integrate more aspects of the law, as they would be applied when circumstances require so. For example: medical personal data are considered to be privacy sensitive data and the law requires therefore a strict regime while processing these data[13]. In PYKE first privacy principles are determined. Then a "simplification" of the law is realized through the linking together ("chaining") of selected articles of the DPD that belong to the chosen privacy principles. Some articles are not "translated" into principles and are not implemented into the MAS design but play a role for explanation and interpretation like articles 2 a till h (definitions) and may influence the architecture. One of the following steps is to formulate the privacy ontology[14] a formal machine understandable description of terms and relations in the data protection domain in an unambiguous way to achieve shared understanding and neutralizing the problem of two databases using different identifiers for what is the same concept, such as transparency or purpose binding. This will achieve that all ISAs act in the same way while transferring preferences and privacy policies[15].

Structure of the privacy incorporated agent (PISA)

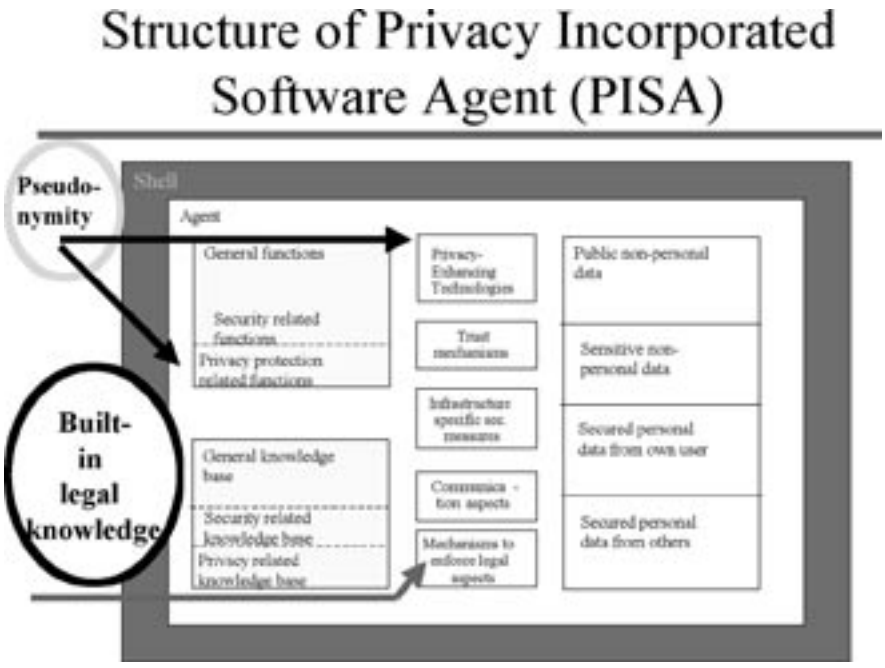
In order to protect the ISA against attacks, security risks and privacy intrusion the ISA has an anonymity shell and built-in privacy protection

related functions, Privacy-Enhancing Technologies (PETs) for pseudo identities, built-in legal know-how by ontologies and other mechanisms to enforce legal aspects. PISA offers two privacy limit options: an ISA operation under anonymity or under the DPD. Once a contact is to be made with the organization the task agent had been set up for, the PET protected (encrypted) personal data are transferred to that organization in accordance with the transfer rules embedded in the ISA. This organization is now in a position to negotiate with the indicated trusted third party, or digital notary (TTP) to decrypt the contact information of the user of the ISA and a limited amount of personal data. The whole process is designed to be within the boundaries of the DPD.

Article 17 paragraph 1 of the DPD on the protection of individuals with regard to the processing of personal data and the free movement of such data regulates the PETs components and further the security functions of the ISA and the PII. Article 17 of The DPD requires data controllers (a natural person or legal entity which alone or jointly with others determines the purposes and means of the processing of personal data), for data protection implementation, to implement "appropriate technical and organizational measures" to protect personal data. Recital 46, in explaining the meaning of Article 17, highlights the requirement that these measures should be taken "both at the time of the design of the processing system and at the time of the processing itself". Thus indicating that security and data protection cannot simply be bolted onto data systems, but must be built into them. Although this provision mainly concerns data security, it is generally intended as a safeguard against other forms of unlawful processing[16].

Consent

The DPD requires in article 7 (a) that personal data may be processed if the data subject has given his or her unambiguous consent. Consent can be described as any freely given specific and informed indication of the data subject's wishes by which the data subject signifies agreement to personal data relating to him or her being processed. There are three aspects to be taken into account concerning consent. A general-purpose consent



is not acceptable under the DPD. An affirmative answer can be given to the legal question whether the ISA can give unambiguous consent required by the law for legitimate processing of the PII on behalf of the user. Our opinion is that the instructions to the agent should be very specific; this has been addressed within the task Agent. As our PISA Demonstrator design works with a generic personal ISA (maintaining and managing the PII of the user, likes and dislikes and non-PII in conformity of the privacy preferences) from which specific one time tasks ISAs with a pseudo-identity generated for a specific transaction or piece of work imposed, the actions of this unique task ISA carrying around no more personal data than strictly necessary will be proof of the required unambiguous consent for that transaction or imposed piece of work only.

Disclosure of PII – different legal regimes

Disclosure of personal data by a sending ISA to a receiving, task or generic, agents should only be permitted when the privacy policy of the recipient of the personal data fits the privacy preferences of the sending task agent. Therefore the sending agent should ensure that the receiving agent adheres to the minimum provisions of the DPD as stated in the APS of the receiving agent. With regard to onward transfers to regions and countries that are subject to different legislation the ISA has to verify whether the privacy protection regime is compliant with the EU DPD. Personal data traffic between EU and USA are ruled by the Safe Harbor arrangements that has to be closed by each specific company and the EU in order to permit onward transfer of personal data[17]. Some countries, like Canada[18], are considered under article 25 paragraph 2 of the DPD as providing an adequate level of protection for personal data transferred from the EU to recipients in Canada. If the privacy preferences are not matched by an ISA then either the exchange of non-PII doesn't occur or other possibilities as mentioned in article 26 1 DPD, or a special contract for protecting the personal data has to be negotiated[19]. •|

Conclusions

Although an ISA can't be held liable for violations itself as it lacks a legal personality, personhood[20], it has to have its built-in privacy protection features to ward off privacy intrusion risks. Furthermore it's a necessity in the expression of the privacy preferences of the user of the ISA, but also in the receiving of the PII of others and the handling of personal data. The PII of the user and the received PII of others have to be managed and processed according to the law. Moreover since the user of an ISA is informed on the capabilities and risks of the ISA the ISA is a tool that may be used by a data subject and a controller, processor or provider. These users of the ISA are liable for violations with respect to privacy and other legislation. This implies that the ISA does not perform a role of his own but acts on behalf of its user, within the limits of the DPD. From a point of view of product liability, the developer is liable for privacy infringing code and from privacy point of view malfunctioning ISAs intruding the privacy of others or damaging the privacy of its user makes the controller accountable.

[1] *John Borking is Associate board member of the Dutch Data Protection Authority and Privacy Consultant*

[2] *J.J. Borking, M. van Eck, P. Siepel, Intelligent Software Agents and Privacy - A&V # 13- The Hague 1999 p. 6,9-10*

[3] *Many definitions of agent technology exist. Living Systems AG summarises all the important characteristics of ISA as: "software objects that proactively operate on behalf of their human masters in pursuing delegated goals"*

[4] *See PISA contract no IST-2000-26038 – see www.pisa.nl*

[5] *See J.J. Borking, C.D. Raab, Laws, Pets and Other Technologies For Privacy Protection -Journal of Information, Law and Technology (JILT) January 2001*

[6] *See Recital 26 of the EU Directive 95/46/EC.*

[7] *We can only note in passing here that the concepts of 'identification' and 'identity' are essentially contested in theory and often arbitrary and ambiguous in practice. See C.D. Raab, 'Identity Checks - and Balances', in E. Bort and R. Keat (eds.), The Boundaries of Understanding: Essays in Honour of Malcolm Anderson, Edinburgh: International Social Sciences Institute, 1999, pp. 87-95.*

[8] *Accepted by the PISA consortium July 2001and EU IST project management*

[9] *The description is an adaptation and extension to a privacy context of the more basic figure related to risk assessment for information security in: BS 7799 (Code of Practice)*
CRAMM - CCTA Risk Analysis & Management Method Information Security Handbook

[10] *See revised edition By R. Hes and J. Borking, Privacy-Enhancing Technologies: The Path to Anonymity, The Hague: Registatiekamer 1998*

[11] *See J. Borking, 'Der Identity Protector', Datenschutz und Datensicherheit, 11, 1996, pp. 654-658.*

[12] *See ISO 15408*

[13] *See article 8 of the DPD, which defines the special categories of data, of which personal health data is one of them.*

[14] *See A.Maedche, Ontology Learning for the Semantic Web, Boston 2002 and T. R. Gruber. A translation approach to portable ontologies. Knowledge Acquisition, 5(2): p.199-220, 1993 http://ksl-web.stanford.edu/KSL_Abstracts/KSL-92-71.html; http://www.w3.org/2001/sw/ http://www.w3.org/TR.webont-req/; http://www.semanticweb.org/knowmarkup.html#ontologies; http://protege.stanford.edu/publications/ontology_development/ontology101.html*

[15] *See S.Kenny, J.J.Borking, The value of Privacy Engineering, The Journal of Information, Law and Technology (JILT) 2002 (1)*

[16] *See Working Document of the EU Article 29 Data Protection Working Party: WP 37: Privacy on the Internet – An integrated EU approach to On-line Data Protection, chapter 9 (Brussels, 21 November 2000)*

[17] *Safe Harbour Principles, US Department of Commerce 21 July 2000*

[18] *EU Commission Decision 2002/2/EC of 20 December 2001 PIPEDA*

[19] *There is a EU Commission Decision and standard contract clauses for such transfers available. See http:// europa.eu.int/commm/internal_market/en/dataprot/modelcontracts/index.htm*

[20] *See Solum, Legal Personhood for Artificial Intelligence (1992) 70 North Carolina Law review pp 1231-1287*

Le projet NADK

Pascal Betz, Fabien Girardin, Claude Fuhrer*, Jean-Paul Dubois*
***Membres de V.I.P**
claude.fuhrer@hta-bi.bfh.ch
jean-paul.dubois@hta-bi.bfh.ch

de g.à d.: Jean-Paul Dubois, Claude Fuhrer

Jean-Paul Dubois
Date de naissance : 3.9.48

Etudes : Ingénieur-physicien EPFL (diplôme en 1973)
Spécialisation en informatique: IBM (Genève), puis Digitron (Bienne) en tant qu'ingénieur software, puis responsable de projets informatiques
Professeur d'informatique à l'Ecole d'ingénieurs de Bienne depuis 1992
Spécialisation: systèmes basés sur les technologies Java

Claude Fuhrer est ingénieur en microtechnique et en informatique.

Depuis 1999 il est chargé de cours à l'Ecole d'ingénieurs de Bienne où il enseigne la programmation dans les divisions d'informatique et de technique automobile.

Ses domaines d'intérêts sont la robotique virtuelle, la sécurité des applications informatiques, particulièrement en Java, la programmation Java de "small devices" et le logiciel libre.

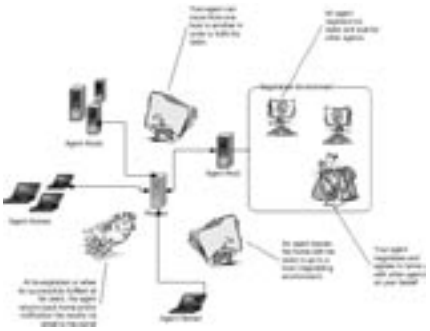
Le terme d'agent est un terme que l'on retrouve régulièrement dans la littérature informatique actuelle. Mais qu'est-ce exactement qu'un agent ? Il existe plusieurs définitions qui ne sont malheureusement pas toujours compatibles entre elles. Par exemple, Jacques Ferber définit un agent comme:

- *une entité autonome, réelle ou abstraite, qui est capable d'agir sur elle-même et sur son environnement, qui, dans un environnement multiagent, peut communiquer avec d'autres agents, et dont le comportement est la conséquence de ses observations, de ses connaissances et des interactions avec les autres agents.*

Une autre définition, plus sommaire, définit un agent autonome comme:

- *un système logiciel avec un ensemble de buts qu'il essaie de satisfaire dans un environnement complexe et dynamique.*

Dans ces deux définitions, on remarque que les points importants couvrent les notions d'autonomie, de perception de l'environnement et de réaction (comportement) à cette perception. De plus, la plupart du temps, on travaille avec une population d'agents dans des systèmes appelés multiagents (SMA pour les intimes). Dans ces systèmes, les agents doivent avoir également la possibilité de communiquer entre eux, pour pouvoir atteindre l'ensemble des buts qui leur ont été assignés.



Le framework NADK

Le projet NADK(acronyme de Negociating Agent Development Kit) a été développé à l'Ecole d'ingénieurs de Bienne par Pascal Betz et Fabien Girardin dans le cadre d'un travail de diplôme de la division informatique. Le but de ce projet était de construire un framework, c'est-à-dire un ensemble d'outils, permettant de créer et d'utiliser des agents négociateurs. Les agents négociateurs sont des programmes qui, par un dialogue avec d'autres agents, négocient et arrangent des activités conjointes ou complémentaires. Il peuvent aussi établir entre eux des relations mutuelles, par exemple dans le cas d'un échange de biens. Pour satisfaire ce but, ils doivent représenter de manière efficace et adéquate les intérêts de leur propriétaire dans le domaine où aura lieu la négociation.

Comment le système fonctionne-t-il? Selon le schéma ci-dessus, nous remarquons plusieurs éléments principaux. Nous avons tout d'abord les homes. Un home est en quelque sorte le lieu de naissance de l'agent négociateur. Physiquement, le home correspond souvent à l'ordinateur du propriétaire de l'agent.

Lors de sa création, l'agent négociateur reçoit toutes les informations qui lui permettront d'accomplir la tâche qu'on désire lui confier. Ces informations pourront, par exemple, contenir l'algorithme de négociation ainsi que les limites dans lesquelles un accord est possible. Lorsque l'agent aura terminé ses négociations, qu'elles aient été fructueuses ou non, il devra en informer son propriétaire. Pour cela plusieurs solutions sont possibles. Le système NADK en propose deux: soit l'agent retourne à sa base, où son propriétaire pourra apprendre directement le résultat des négociations, soit il signale la fin de son travail en envoyant un email à son propriétaire, avant de continuer son travail ou de disparaître.

Le deuxième composant important est dénommé host. Les hosts forment les agoras dans lesquelles les agents se retrouvent pour communiquer et négocier. Lorsqu'un agent arrive sur un host, il doit s'y annoncer. Cela permet au host de connaître tous les agents qu'il héberge et ainsi de présenter les uns aux autres les agents dont les tâches sont compatibles, afin qu'ils puissent entamer leurs négociations.

Le troisième élément composant cet ensemble est un lookup service, c'est-à-dire une sorte de super annuaire connaissant la totalité des hosts disponibles. Cet élément provient de la technologie Jini qui nomme l'implantation standard de son lookup service: "reggie". Lorsqu'un agent veut migrer d'un host vers un autre, il s'adresse à un reggie afin que celui-ci lui communique l'adresse d'un autre host disponible. Naturellement, chaque fois qu'un nouveau host est créé, il s'annonce auprès de reggie et de ses "frères" (car il peut y en avoir plusieurs) afin ceux-ci puissent tenir à jour la liste des hosts disponibles dans le système.

Le dernier élément à mentionner est bien entendu l'agent lui-même. Un agent négociateur est un code mobile qui peut migrer d'un host à l'autre. Pour cela, il va copier à la fois son code et son état dans le nouveau host. Lorsque cette copie a été effectuée correctement, l'agent est désactivé sur le host courant avant d'être réactivé sur le nouveau.

Les agents comprennent aussi un mécanisme leur permettant de survivre à un arrêt du système. Pour sauver l'état d'un agent, et ainsi pouvoir le restaurer au redémarrage du host, le système utilise le mécanisme de sérialisation de Java.

De plus, pour se protéger du monde extérieur, les agents ne communiquent pas directement avec leurs interlocuteurs, mais passent au travers d'un proxy. Cela permet d'éviter que les interlocuteurs accèdent à certaines informations sensibles mémorisées dans chaque agent (comme par exemple l'identité de sa base). •|

Pour plus d'informations au sujet du projet NADK, veuillez vous reporter au site Web http://www.hta-bi.bfh.ch/Projects/nadk.

Privacy in the Electronic Society

Sabrina De Capitani di Vimercati and Pierangela Samarati
Università di Milano, Dipartimento di Technologie dell'Informazione
decapita@dti.unimi.it
samarati@dti.unimi.it

Pierangela Samarati is a professor at the Department of Information Technology of the University of Milan. Her main research interests are in data and application security, information system security, access control policies, models and systems, and information protection in general. She has been Computer Scientist in the Computer Science Laboratory at SRI, CA (USA). She has been a visiting researcher at the Computer Science Department of Stanford University, CA (USA), and at the ISSE Department of George Mason University, VA (USA). She is co-author of the book ``Database Security,'' Addison-Wesley, 1995. She is co-recipient of the ACM-PODS'99 Best Newcomer Paper Award.

Sabrina De Capitani di Vimercati is an associate professor at the Department of Information Technology of the University of Milan. She received her Laurea and PhD degrees both in Computer Science from the University of Milan in 1996 and 2001, respectively. Her research interests are in the area of information security, databases, and information systems. She has been an international fellow in the Computer Science Laboratory at SRI, CA (USA). She is co-recipient of the ACM-PODS'99 Best Newcomer Paper Award.

Introduction

Protecting privacy in today's electronic society requires the investigation of different aspects, including: the classical problem of protecting the *confidentiality of information when transmitted over the network* (e.g., in electronic commerce when we communicate a credit card number over the web); the problem of *controlling the use and dissemination of information* collected or available through the web; the problem of *managing the identity and profile information* given to remote parties in a trustworthy and responsible way; and the problem of protecting against inference and linking (computer matching) attacks, which are becoming easier and easier because of the increased information availability and ease of access as well as the increased computational power provided by today's technology. In this article we briefly discuss these problems (although we recognize the importance of providing communication secrecy, we will not discuss this - more consolidated - problem any further).

Privacy issues in data collection and disclosure

The increased power and interconnectivity of computer systems available today provide the ability of storing and processing large amounts of data, resulting in networked information accessible from anywhere at any time. It is becoming increasingly easier to collect, exchange, access, process, and link information. Information about us is collected every day, as we join associations or groups, shop for groceries, or execute most of our common daily activities. Information bureaus such as TRW, Equifax, and

Trans Union hold the largest and most detailed databases on American consumers. There are also the databases maintained by governmental and federal organizations, DMVs, HMOs, insurance companies, public offices, commercial organizations, and so on. Typical data contained in these databases may include names, Social Security numbers, birth dates, addresses, telephone numbers, family status, and employment and salary histories. These data often are distributed, or sold. This dissemination of information has been in some cases a matter of controversy (as an example remember the open debates about the plan of America On Line to provide telephone numbers of its subscribers to "partner" telemarketing firms, which resulted in AOL canceling the plan). In other cases, this dissemination of information is becoming common practice. Although one may claim that the information these databases contain is officially public, the restricted access to it and expensive processing (in both time and resources) of it represented, in the past, a form of protection. This is less true today. Concerns are voiced by individuals who are annoyed by having their phone numbers and addresses distributed, resulting in the reception of junk mail and advertisement phone calls. Even more of a concern is that these data open up the possibility of linking attacks to infer sensitive information from data that are otherwise considered "sanitized" and are disclosed by other sources.

Even if only in statistical, aggregate, or anonymous form, released data too often open up privacy vulnerabilities through data mining techniques and computer matching (record linkage). Tabular and statistical data are vulnerable to inference attacks. By combining information available through different interrelated tabular data (e.g., Bureau of Census, Department of Commerce, Federal and Governmental organizations) and, possibly, publicly available data (e.g., voter registers) the data recipient may infer information on specific microdata that were not intended for disclosure. Anonymous data are microdata (i.e., data actually stored in the database and not an aggregation of them) where the identities of the individuals (or organizations, association, and so on) to whom the data refer have been removed, encrypted, or coded. Identity information removed or encoded to produce anonymous data includes names, telephone numbers, and Social Security numbers. Although apparently anonymous, however, the de-identified data may contain other identifying information that uniquely or almost uniquely distinguishes the individual. Examples of such identifying information may be age, sex, and geographical location. By linking such information to publicly available databases associating them to the individual's identity, the data recipients can determine to which individual each piece of released data belongs, or restrict their uncertainty to a specific subset of individuals.

The threat represented by inference and linking attacks is also of great concern because of the fact that statistical, aggregate, and anonymous data are often exempted from privacy protection regulations. More than others, these data may therefore open up the possibility of potential misuses.

Digital identity management

Nowadays, a global information infrastructure connects remote parties worldwide through the use of large scale networks, relying on application level protocols and services such as the World Wide Web. Execution of activities at various levels is increasingly based on the use of remote resources and services, and on the interaction between different, remotely located parties. Digital identity management is becoming of paramount importance for supporting successful interaction in this scenario. Digital identity is the electronic representation of the personal information of an individual or organization. The term digital identity is usually used to

refer to two (non-disjoint) concepts: *nyms and partial identities*. Nyms can be used to give a user a different identity under which operate at any interaction. A partial identity is any subset of the properties (e.g., name, age, credit-card, employment, etc.) associated with a user. Partial identities may or may not be named (i.e., may or may not be related to the human identity of the user).

Digital identity management supports privacy as it allows carrying out interaction on the Net without requiring identification of the human user and therefore the disclosure of all her properties (directly or possible through correlation with the identity). The use of digital identity also provides increased convenience: it does not require users to register at every step of complex network interactions and avoids the need of costly and error-prone profile maintenance at different servers.

To ensure successful identity management, a digital identity solution should support at least the following basic requirements.

Reliability and dependability. Identity theft is one the fastest growing electronic crime and it is expected to accelerate. Digital identity must offer protection against forgery and related attacks. While their main goal is to protect and preserve individual users' anonymity, digital identities should fully guarantee other parties (e.g., suppliers and brokers in the framework of an e-business transaction) that the identity can be relied upon, and therefore obligations to the digital identity deriving from such a transaction will eventually be met by someone.

Controlled information disclosure. Users must be given control on what identity to use in specific circumstances. Control must also be given with respect to possible replication and misuses of the identity information a party reveals in a transaction.

Mobility support. The mobile computing infrastructure can keep track of an individual's physical location. In addition, mobile computing bears some peculiarity such as limited bandwidth and limited display size.
In a context where parties may interact disclosing different nyms or only part of their identities, innovative models must be developed that identify under which conditions a party can trust others for their security and privacy. Trust models is one of the techniques be evaluated. In this context *digital certificates* (statements certified by given entities) can be used to establish properties of their holder (such as identity, accreditation, or authorizations). Also, methods for trust management based on *reputations* are currently receiving considerable interest: *reputation models* can be devised that allow the reliable association of reputations with nyms. Development of reputation models that allow trust establishment in anonymous or pseudo-anonymous systems (e.g., peer-to-peer systems) requires the development of techniques and protocols to measure reputations, store and share reputation information, and providing their reliability.

Specifying privacy constraints

Privacy laws and regulations are currently being enforced, and new laws are still under study. They establish privacy policies to be followed that regulate the use and dissemination of private information. A basic requirement of a privacy policy is to establish both the responsibilities of the data holder with respect to data use and dissemination, and the rights of the individual to whom the information refers. In particular, individuals should be able to control further disclosure, view data collected about them and, possibly, make or require corrections. These last two aspects concerning the integrity of the individual's data are very often ignored in practice.

The application of a privacy policy requires corresponding technology

to express and enforce the required protection constraints, possibly in the form of rules that establish how, to/by whom, and under which conditions private information can be used or disclosed. With respect to the specification of use and release permissions, authorization models available today prove inadequate with respect to privacy protection and, in particular, to dissemination control or protection by inference. An authorization model addressing privacy issues should provide the following features.

Explicit permission. Private and sensitive data should be protected by default and released only by explicit consent of the information owner (or a party explicitly delegated by the owner to grant release permission).

Purpose specific permission. The permission to release data should relate to the purpose for which data are being used or distributed. The model should prevent information collected for one purpose from being used for other purposes.

Dissemination and secondary usage control. The information owner should be able to control further dissemination and use of the information.

Conditional permission. Access and disclosure permissions should be limited to specific times and conditions.

Fine granularity. The model should allow for permissions referred to fine-grained data. Today's permission forms for authorizing the release of private information are often of a whole/nothing kind, whereby the individual, with a single signature, grants the data holder permission to use or distribute all referred data maintained by the data holder.

Linking and inference protection requirements. The model should allow the specification and enforcement of privacy requirements with respect to inference and linking attacks. Absolute protection from these attacks is often impossible, if not at the price of not disclosing any information at all. For instance, given some released anonymous microdata, the recipients will most certainly always be able, if not to determine exactly the individual to whom some data refer, to reduce their uncertainty about it. Privacy requirements control what can be tolerated, for example, with respect to the size of the set to whom this uncertainty can be reduced.

It is worth noticing that simple concepts, traditionally applied in authorization models, become more complicated in the framework of privacy. An example is the concept of information owner. The answer to this question is not easy and perhaps belongs more properly to the public policy domain. For instance, there have been open debates concerning whether a patient or the hospital owns the information in the patient's medical records maintained by the hospital. Perhaps the notion of owner as traditionally thought does not fit in such context and instead should be revised or substituted by one or more other concepts expressing the different parties involved (data holder vs. individual). A good privacy model should allow the expression of these different parties and of their responsibilities. To the public policy domain will then belong the answer as to how to express such responsibilities (e.g., whether the specification of privacy constraints must remain with the data holder, the individual, or both).

Conclusions

The protection of privacy in today's global infrastructure requires the combined application solution from technology (technical measures), legislation (law and public policy), and organizational and individual policies and practices. Ethics also will play a major role in this context. The privacy problem therefore covers different and various fields and issues on which much is to be said. As society discusses privacy concerns and needs, it is clear that research is needed to develop appropriate technology to allow enforcement of the protection

TO BE OR NOT TO BE IN THE NEXT GENERATION INTERNET

Dr. Alberto Escudero-Pascual, aep@kth.se

Alberto Escudero-Pascual

Dr. Alberto Escudero-Pascual is researcher at the Royal Institute of Technology in Sweden since 1999 in the area of privacy in mobile Internetworking. His research interests vary from security in wireless networks to legal aspects of data retention and cybercrime.
Further info at http://www.it.kth.se/~aep

Motivation of article: this short article is written as a response to document Opinion 2/2002: on the use of unique identifiers in telecommunication terminal equipments: the example of IPv6_. The document was released the 30 May 2002 by the European Union's Article 29 Data Protection Working Party, an independent advisory body on data protection and privacy set up under Article 29 of Directive 95/46/EC.

The global telecommunication infrastructure will slowly converge toward an integrated packet switched network using the Internet Protocol as the common communication technology.

First evidence of this convergence is the deployment of the third generation wireless infrastructure that brings together the radio access network and core network by introducing the next generation Internet Protocol IPv6.

Although there have been many technical efforts to insure data confidentiality in the next generation Internet, it is still not known if the new IPv6 security and mobility features will actually be enough to empower users and protect their privacy or if in fact just the opposite will occur.

One open question still remains: will the deployment of the next generation Internet bring more security and privacy to the users or the opposite will occur?

As an example, the article considers the controversial issue of the global unique identifiers in IPv6. After explaining the possible treat for privacy and the limitations of the suggested privacy extension of stateless address autoconfiguration (RFC3041), we also illustrate the new opportunities for privacy that IPv6 brings as the use of Cryptographically Generated IPv6 Address for identity management and pseudonymity. Complex problems sometimes require no simple answers: When one door closes another door opens wide. New tools for new challenges.

Background

As evidence of the strategic importance of the development of the Internet, in year 2002 the European Union released a statement recommending a European plan of action to accelerate the implementation of IPv6, a key technology for the Next Generation Internet[1].

In response to the technology changes the European Union has also introduced a new regulatory framework that is intended to provide a coherent, reliable and flexible approach to the legal regulation of electronic communication networks and services in fast moving markets. The package of directives will be applied in all Member States from 25 July 2003 with the exception of the Directive on privacy and electronic communications, for which the date is 31 October 2003.

The Data Protection Directive (2002/58/EC)[2] on 'processing of personal data and protection of privacy in the electronic communication sector' is part of the package of new proposals and aims to adapt and update the previous Data Protection Telecommunications Directive (97/66/EC) to take account of technological developments. However, it is not well understood how this policy and the underlying Internet technology can be brought into alignment[3].

Although the Internet is rapidly becoming "the" communication network, it was not really engineered to preserve certain types of privacy. In keeping with the European Union policies regarding data protection there is a need to understand the benefits and to reduce the privacy risks of this new generation of Internet technology.

Maintaining proper confidentiality with respect to location information, traffic information, and the actual data traffic itself are three of the key provisions of the new European regulatory framework for electronic communications infrastructure and associated services.

This article presents one timely and important privacy area identified during our late research at the Royal Institute of Technology (KTH) in Sweden: unique identifiers in telecommunication terminal equipments and identity management.

Short introduction to IPv6

The Internet Protocol Version 6 (IPv6), also known as IPng (IP Next Generation), is the latest version of the Internet Protocol (IP). Formally, IPv6 is a set of specifications from the Internet Engineering Task Force (IETF). IPv6 is being designed as an evolutionary set of improvements to the current IP Version 4. The most obvious improvement in IPv6 over the IPv4 are that IP addresses are lengthened from 32 bits to 128 bits which anticipates the future growth of the Internet and provides relief for what was perceived as an impending shortage of network addresses.

Besides, IPv6 offers technical advantages over IPv4, including self-configuration mechanisms, enhanced security, quality of service features and native mobility support.

IPv6 aims to be the protocol capable of bringing together access and core networks, the 'glue' for the deployment of the future 'all-IP' telecommunication network.

IPv6 includes a security protocol in the network layer that provides cryptographic security services that supports combinations of authentication, integrity, access control, and confidentiality. The IP Encapsulating Security Payload (ESP) and the IP Authentication Header (AH) are part of the IP Security architecture (IPSEC) described in RFC 2401[4].

Both ESP and AH are mandatory parts of IPv6 and make sure that a third party eavesdropping on the channel can not read and/or modify any IP datagrams.

The IP Authentication Header seeks to provide security by adding authentication information to each IP datagram whilst confidentiality requires the use of ESP. Nevertheless, neither AH nor ESP hide the source and destination IP addresses of the communicating parties and hence their network location.

The protocol operation defined for mobility in IPv6 is known as MobileIPv6[5] and allows a mobile node to move from one link to another without changing the mobile node's IP address. A mobile node is always addressable by its "home address", an IP address assigned to the mobile node within its home subnet, i.e., with the network prefix of its home link. Packets may be routed to the mobile node using this address regardless of the mobile node's current point of attachment to the Internet, and the mobile node may continue to communicate with other nodes while using this address, even after moving to a new link. With specific support for mobility in IPv6, packets destined to a mobile node would be able to reach it even while the mobile node is away from its home network. The home IP address identifies the mobile device regardless of its current location.

In summary, IPv6 provides new security opportunities which include message integrity, authentication, and confidentiality (IPSEC) and the possibility for a mobile node to be always addressable by its "home address" (MobileIP). All these functionalities rely on treating the fixed IP address of the node as an identifier. In the case of IPSEC end-to-end security uses the fixed IP address as part of the security association and mobility requires to the mobile node to send the fixed home address included in a destination option.

In the next section we describe how a possible threat for privacy occurs when an IP identifier can be linked with personal identifiable information as a "personal device" and how the existing privacy extension (RFC3041) has not taken into consideration that the user might be also interested in hiding the fact that is using the privacy extension itself.

After presenting two limitations of the RFC3041 we briefly introduce the role that Cryptographically Generated Addresses (CGA) can play as a technical solution for identity management.

Stateless address autoconfiguration and privacy extension

The stateless address autoconfiguration defines the mechanism for a IPv6 device to generate a global unique address (128 bits) without the need of an external DHCP server. The IPv6 address is formed by using the information of the network interface identifier (IID) as right-most 64 bits and the network prefix received in a router announcement as the left-most 64 bits. For example, if we consider a device with an Ethernet the Interface Identifier is based on the EUI-64 identifier derived from the interface's built-in 48-bit IEEE 802 address (MAC address).

In summary, the IPv6 addresses generated via Stateless Autoconfiguration contain the same interface identi_er regardless of the location the mobile node is attached to the Internet. The right-most 64 bits are persistence and hence devices can be tracked regardless of the point of attachment to the Internet[6].

A privacy extension for stateless address autoconfiguration was introduced in the RFC3041 based on the idea of generating random interface identifiers periodically instead of using the built-in MAC address of the network device. If we consider the definition of privacy introduced by Alan Westin in 1967[7]:

"Privacy is the claim of individuals, groups and institutions to determine for themselves, when, how and to what extent information about them is communicated to others."

While the RFC3041 represents a clear privacy improvement with respect to the stateless address autoconfiguration proposal, we found that the proposed privacy extension has two important limitations:

- ***Privacy preference observability***: the use of the RFC3041 also implies that the so called universal/local bit or "u" bit needs to be set to 0. As shown in[7], the fact that a device is using the privacy extension is observable (i.e. an address generated using the privacy extension differ in structure from the others and hence the user's privacy option is public to any communicating party).
- ***IP identifier vs. IP identity***: while in absence of any other information a set of RFC3041-addresses originated during a period of time can not be linked to one single user (device), but it is far more desirable that the users could determine for themselves, when, how and to what extent the IP information about them is communicated to others. For example, the user could use the IPv6 information as a pseudoidentity. The desired goal is to provide a mechanism that enables authentication against any selected parties while concealing from any third parties that two IP addresses are associated to any given user.

In the following section we introduce the concept of Cryptographically Generated IPv6 Address as a technical mean to enhance privacy while providing authentication in IPv6.

Cryptographically Generated IPv6 Address

The Cryptographically Generated Identifiers and Addresses [8], otherwise known as Crypto-Based Identifiers (CBID's), are identifiers derived via a one-way function applied to a public key. Roughly, CBID = f(PK; i) (Eq. 1) where f() is a well known one-way function (typically involving a cryptographic hash function), PK is the public key used to produce the corresponding CBID and i is any other inputs to the one-way function. Hence, CBID's are secure representations of that public key.

In the context of IPv6, the term CBID is used to refer to either of the following two types of entities: a) Crypto-Based Address (CBA) is an address whose leftmost 64 bits are set to a valid prefix (as per normal IPv6 usage), and whose rightmost 64 bits (interface identifier) are set to a 64-bit entity obtained via a one-way function such as shown in Eq. (1) and, b) Crypto-Based Identifier (CBI) is a fixed length entity in which the entire identifier (typically 128 bits) is derived as shown in Eq. (1).

These identifiers have four very important properties:

1. They are statistically unique, because of the collision-resistant property of the cryptographic hash function used to generate them.
2. Since a node can prove ownership of its CBID. Thus, they are securely bound to a given node. A node accomplishes this "proof of ownership" by revealing the public key, PK, used to generate the CBID (along with any other values used as input to the one-way function). It then proves that it knows the corresponding private key, SK, by digitally signing a message.
3. They do not rely on any centralized security service such as a PKI or Key Distribution Center.
4. Their binding to any particular entity or user may be kept private at the discretion of the CBID creator (typically the entity or user itself).

Related work[8] shows how CBID's are very useful to secure Mobile IPv6. Further work[9] combines CBID's with SPKI-style authorization certificates to solve the proof-of-membership problem. In summary, the resultant scheme allows a user or host to prove to any third party that it is a member of a given group without the requirement of revealing its identity.

Conclusion

The default mechanism to obtain an IPv6 address based on stateless address autoconfiguration introduces a new threat for privacy as the interface identifier remains constant regardless of time and point of attachment to the network. While the privacy extension (RFC3041) is a clear privacy improvement with respect to the stateless address autoconfiguration proposal, it has important limitations as the users can not determine by simple means, when, how and to what extent the IP information about them is communicated to others.

While IPv6 introduces new possible threats for privacy it also provides the possibility to use new schemes as the Crypto Based Identifiers that can be well adapted to Privacy and Identity Management. For example, the use of CBA in IPv6 can not only solve the address ownership problem and secure Mobile IPv6, but also can be used as a privacy enhancement technology (PET)[6].

With this article we propose and encourage investigating the use and implementation of Crypto Based Identifiers as a Privacy Enhanced Technology (PET) in the context of ubiquitous networking and as promising technology that can be used to technically enforce the Directive on privacy and electronic communications (2002/58/EC).

Acknowledgments

To Claude Castelluccia (INRIA, Rhône-Alpes) and Gabriel Montenegro (Sun Microcrosystems Labs, Grenobe) for their input to the CBA section. See working document "Crypto Based Identifiers (CBID) for Privacy and Identity Management (PIM)", proposal for future research in IPv6, November 2002. http://www.it.kth.se/~aep/publications/aep-claude-gab-cbid-4-pim.pdf

References

[1] *European Commission, Next Generation Internet priorities for action in migrating to the new Internet protocol IPv6, COM(2002) 96 _nal, Brussels, 21st February 2002.*

[2] *European Parliament, European Telecommunication New Regulatory Framework, 2000-2002.*

[3] *Article 29 Working Party, Opinion 2/2002:*
on the use of unique identifiers in telecommunication terminal equipments: the example of IPv6, 30 May 2002.

[4] *S. Kent and R. Atkinson,Security Architecture for the Internet Protocol, RFC 2041.*

[5] *D. Johnson and C. Perkins, Mobility Support in IPv6, draft in progress.*

[6] *A. Escudero, Privacy in the next generation Internet, Data Protection in the context of European Union Policy. Conclusions of PhD Thesis. Royal Institute of technology, December 2002.*

[7] *A. F. Westin, Privacy and Freedom, Atheneum Press, New York, USA. 1967.*

[8] *G. Montenegro and C. Castelluccia, Statistically Unique and Cryptographically Verifiable*
Identifiers and Addresses, ISOC NDSS02, San Diego, February 2002.

[9] *C. Castelluccia and G. Montenegro, Dynamic and Secure Group Membership in Ad Hoc and*
Peer-to-Peer Networks (short paper), ACM MC2R, October 2002.

Evolution de la criminalité et nouvelles technologies

La recherche et l'enseignement au profit des différents composants du système judiciaire

Olivier Ribaux et Pierre Margot

Olivier RIBAUX, professeur extraordinaire, Institut de Police Scientifique et de Criminologie, Faculté de droit, Université de Lausanne

Pierre MARGOT, professeur ordinaire, Directeur de l'Institut de Police Scientifique et de Criminologie, Faculté de droit, Université de Lausanne

We shape our buildings; thereafter they shape us. Cette phrase de Churchill peut s'adapter aux nouvelles technologies et à l'ampleur de leurs effets sur l'évolution de la société. Leur utilisation est maintenant obligatoire dans beaucoup de situations, mais elles sont souvent subies plutôt que maîtrisées et créent des contextes dans lesquels la réalisation de crimes est facilitée.

Le futur ingénieur peut oublier que les usagers se trouvent souvent empruntés devant ces machines et ces logiciels qui constituent des passages obligés, comme des distributeurs de billets, des ordinateurs achetés à l'étalage ou des bases de données indispensables à nos activités privées et professionnelles dont les accès sont protégés par des listes de mots de passe impossibles à mémoriser.

Cette complexité imposée par les nouvelles technologies offre des occasions aux délinquants qui se rient de ces failles: les codes sont souvent carrément inscrits sur la carte de paiement, facile à dérober. D'autre part, n'importe quel individu est susceptible de croire qu'une machine comme un distributeur automatique de billets de banque souffre de pannes régulières (tout le monde sait que l'informatique se plante régulièrement!), alors qu'en réalité, elle a été trafiquée par des délinquants dans le but de voler. Même les meilleurs informaticiens perdent souvent la maîtrise des logiciels qu'ils développent, y introduisent des fautes et ouvrent ainsi des brèches exploitées par des délinquants de tout calibre, de l'étudiant en mal d'exploits aux terroristes susceptibles de déstabiliser un Etat par ces moyens.

Les malfaiteurs utilisent également l'informatique et les télécommunications pour préparer et réaliser leurs actions criminelles. Ainsi, l'utilisation des téléphones mobiles a modifié le déroulement d'un cambriolage ou encore les mécanismes de distribution de stupéfiants par des dealers. L'échelle géographique et temporelle des événements criminels est également bouleversée.

On ne peut pas quantifier les dégâts, mais quelques tendances se dégagent: les statistiques des délits liés aux cartes de paiement augmentent constamment et la révélation de quelques cas spectaculaires, comme l'affaire récente de pédophilie dont l'ampleur consterne (accès à des sites pédophiles aux Etats-Unis au moyen de cartes de crédits qui ont permis de confondre plusieurs centaines d'individus en Suisse), donnent une idée de ces évolutions.

Ainsi, qu'elles aident la réalisation de crimes traditionnels ou qu'elles provoquent le développement de formes de délinquances inconnues jusqu'ici, les nouvelles technologies posent la question fondamentale et récurrente de la capacité de notre société à orienter leur usage dans un sens positif tout en limitant leur exploitation à des fins criminelles.

Un traitement raisonné et complet de cette question nécessiterait évidemment bien davantage de place que celle dédiée ici. Nous emprunterons une perspective très limitée et résolument orientée vers le support que peuvent proposer des structures

de recherche et d'enseignement pour aider les organes judiciaires à intégrer les évolutions technologiques et ainsi à conserver son rôle central dans la lutte contre la criminalité. Cela nécessite préalablement de comprendre comment les nouvelles technologies ont été abordées par la police au cours de ces dernières années comme outils d'aide à l'investigation et comme objets à investiguer.

Nouvelles technologies et la police

L'intégration des nouvelles technologies en milieu policier s'est réalisée de manière rapide et parfois brutale. Elle n'est qu'un aspect des mutations récentes et profondes du système global de sécurité qui ont un impact considérable sur la distribution des compétences (quels genres d'affaires sont traités à quel niveau: communes, cantons, confédération), les règles légales, les organisations, les méthodes et les outils.

Le nouveau fichier signalétique basé sur l'ADN (plus de 2000 cas dont les auteurs ont été identifiés en deux ans d'utilisation en Suisse), le système automatisé qui compare les empreintes et traces digitales, ainsi que les systèmes d'information géographiques qui aident à analyser des délits sont des exemples qui illustrent le potentiel de ces nouveaux outils. Le système global de la police de la ville de New-York, appelé COMPSTAT, met en mouvement les forces en fonction de statistiques produites à grands renforts de technologies (ensemble de systèmes informatisés permettant d'analyser et de visualiser des situations criminelles). Les stratégies de lutte sont évaluées régulièrement en fonction de l'évolution des données et les responsables sont mis sous pression lorsque les statistiques d'une région se montrent indifférentes aux mesures opérationnelles mises en oeuvre. Ce système est considéré comme le prototype d'une démarche complète de renseignement qui s'appuie sur des moyens informatisés.

Une grande partie des investigations demandent également davantage de connaissances en matière d'informatique et de télécommunication, par exemple pour aborder un ordinateur sur une scène de crime ou extraire d'un téléphone mobile toute l'information nécessaire. De nouvelles structures de lutte contre le crime informatique ou de soutien technique centralisent ces compétences et prolongent l'activité des services de police scientifique.

Ces développements ébranlent des convictions et posent de nombreuses questions, parfois contradictoires, susceptibles de ralentir ces évolutions. En voici quelques exemples typiques qui montrent l'importance d'orienter les réflexions vers une meilleure compréhension du contexte d'utilisation des outils pour lever les doutes:

L'enquêteur judiciaire, souvent représenté dans les romans par un personnage bien intégré et imaginatif qui allume sa pipe pour déclencher des raisonnements élégants est-il devenu inutile ?

Les cartes de paiement volées et utilisées par des malfaiteurs peuvent aussi révéler des traces digitales… et permettre d'identifier un auteur au moyen de bases de données (photo Eric Sapin / IPSC)

Les visions new-yorkaise et romanesque un peu caricaturales du travail du policier ne s'opposent en fait pas. Elles sont toutes deux basées sur la constatation que l'analyse des données, effectuée à l'échelle de l'individu ou dans le cadre d'un système, est au cœur de l'activité policière. Une approche pour lier les deux perspectives consiste à comprendre comment l'enquêteur réfléchit : pourquoi Hercule Poirot et Sherlock Holmes aboutissent-ils systématiquement à la bonne solution ?

Sur la base de raisonnements bien décortiqués et formalisés, il est possible d'appliquer des méthodes d'enquête de manière beaucoup plus systématique et mieux coordonnée. Cette démarche qui est récente en milieu policier, est réalisée dans le cadre d'un nouveau domaine appelé analyse criminelle qui propose ainsi d'interpréter les questions à un niveau plus méthodologique que technique. Les nouveaux outils fondés sur les technologies récentes qui s'intègrent dans ces processus bien définis auront alors une meilleure chance de déployer toute leur efficacité.

Y a-t-il des risques de dérapages qui mettent en danger la sphère privée ?

L'exploitation de ces technologies alimente les inquiétudes du citoyen qui craint un traitement généralisé et systématique de données personnelles au travers de systèmes informatisés susceptibles de mettre en danger sa sphère privée. Les caméras de surveillance font peur, tout comme la base de données fondée sur les informations signalétiques extraites de l'ADN.

En réalité, en matière d'investigation, les risques résident davantage dans des raisonnements erronés et des renseignements transformés trop vite en actions irréparables que dans la possibilité d'accéder à de l'information.

Un témoignage, dont l'incertitude est difficilement évaluable, peut amener la police à intervenir lourdement dans la vie privée d'individus innocents. Pourtant, il paraît naturel de baser une enquête sur de tels renseignements, alors que la polémique se concentre sur des données stockées dans des systèmes informatisés particuliers qui ont un contenu dont les imperfections sont mieux maîtrisées, comme la base de données ADN.

Orienter le débat et les efforts vers la manière dont les informations sont traitées au cours d'une enquête offre donc une meilleure chance de protéger la sphère privée que d'aligner des obstacles pour accéder aux données. L'analyse criminelle peut fournir le cadre dans lequel ces questions peuvent être discutées de manière objective .

Les nouvelles technologies permettront-elles de résoudre les grands problèmes de criminalité et de terrorisme ?

Une attitude qui consiste exagérer le potentiel des nouvelles technologies dans la lutte contre le crime et le terrorisme se répand dangereusement. Il suffirait de financer des programmes de recherche ambitieux pour obtenir des solutions technologiques aux problèmes. Il en résulte une certaine frénésie et des propositions de financements désordonnés qui conduisent inévitablement à des dérapages. 30 ans de travaux intensifs en intelligence artificielle ont pourtant bien montré certaines limites qu'on croit pouvoir miraculeusement surmonter aujourd'hui. Par exemple, les systèmes automatiques de reconnaissance faciale ont été présentés récemment comme un composant important de la lutte contre le terrorisme; l'extraordinaire difficulté de reconnaître automatiquement des visages rend crédible ceux qui doutent de l'efficacité pratique de cet outil… il faut répéter que les technologies doivent s'intégrer dans un cadre cohérent qui explicite aussi leurs limites.

La police est-elle capable de maîtriser les nouvelles technologies ?

De nouvelles structures chargées d'aborder la criminalité informatique ont été construites et l'analyse crimi-

nelle a pris un essor considérable. Le chemin parcouru en peu de temps est donc significatif. Toutefois, cette maîtrise reste partielle comme le montrent les échecs de plusieurs projets informatiques qui ambitionnaient la résolution de problèmes trop complexes. Encore une fois, ce sont les démarches qui permettent de déterminer plus clairement la place des nouvelles technologies dans le système qui méritent une attention particulière.

L'enseignement et la recherche

Le système judiciaire ne peut clairement pas absorber ces bouleversements sans s'appuyer sur des compétences externes qui l'aident à accéder aux connaissances indispensables et à maintenir une veille technologique. Toutefois, les expériences réalisées et ce qui précède montrent que les technologies ne servent à rien si elles ne sont pas bien intégrées dans leur contexte d'utilisation. Ce dernier combine des stratégies liées à la politique criminelle, des règles légales et un enchevêtrement de processus qui dépendent entre autres des organisations et des ressources disponibles. En plus, l'ensemble du système est confronté à une situation criminelle susceptible d'évoluer rapidement, qu'il doit, bien évidemment, aborder en temps réel.

Cela rend indispensable d'inscrire dans une architecture qui tienne compte de cette complexité les programmes de recherche et d'enseignement destinés à produire et à diffuser des connaissances utiles aux différents composants du système judiciaire. C'est ce qui caractérise les domaines des sciences criminelles et en particulier des sciences forensiques enseignées à l'Institut de Police Scientifique et de Criminologie de l'Université de Lausanne.

Le nouveau DEA en droit, criminalité et sécurité des nouvelles technologies, lancé à l'Université de Lausanne dans le cadre des programmes IRIS (réunissant les Universités de Lausanne et de Genève et l'Ecole Polytechnique Fédérale de Lausanne. Le programme bénéficie d'apports financiers de la CUS et des institutions partenaires.) durant l'année écoulée, vise, entre autres, à répondre à ce besoin. L'enseignement s'adresse particulièrement aux juristes, aux gestionnaires d'entreprises et aux criminalistes concernés par les risques liés à l'usage généralisé de l'informatique et des télécommunications. Spécifiquement, le cours de criminalistique insiste sur les concepts de base du domaine et s'articule autour de l'analyse criminelle qui détermine le cadre dans lequel la nature et la place des nouvelles technologies dans l'investigation sont discutées. Plus généralement, il s'agit aussi de stimuler les échanges entre des chercheurs et praticiens travaillant selon des perspectives et au moyen de champs de connaissances différents, mais qui sont tous au contact des problèmes sécuritaires engendrés par les nouvelles technologies.

Ce projet se combine valablement avec le développement du centre VIP (Virtual Identity and Privacy research center), conçu par le Professeur Jaquet-Chiffelle de la HES bernoise qui propose une approche globale susceptible d'élargir encore le débat en proposant une plate-forme sur laquelle un réseau de partenaires peut confronter les points de vue et ainsi dégager des pistes de réflexions communes qui débouchent sur des projets de recherche en adéquation avec les besoins de la société en matière de sécurité.

Conclusion

De nouvelles occasions offertes aux malfaiteurs impliquent nécessairement l'existence de nouvelles formes de délinquance et l'extension des formes existantes. Les astuces utilisées par les truands restent souvent simples, exploitent certainement davantage les lacunes des utilisateurs que des faiblesses techniques et ne nécessitent pas forcément de connaissance approfondie; nous sommes tous des victimes potentielles et les auteurs ne sont pas à rechercher uniquement parmi les techniciens confirmés.

Afin que le système judiciaire puisse conserver son rôle, il poursuit ses efforts de compréhension, d'intégration et de contrôle de l'évolution des technologies. Les écoles qui étudient et développent les nouvelles technologies, si elles s'associent aux praticiens et aux chercheurs provenant des sciences criminelles, peuvent contribuer à maintenir la veille technologique, à diffuser des connaissances indispensables au maintien de la sécurité publique et à concevoir leurs innovations en intégrant dans leurs concepts de base la sécurité nécessaire à maîtriser les effets néfastes liés à l'utilisation de leurs produits.

Si le système judiciaire et les usagers de systèmes informatisés sont parfois désemparés face à ces évolutions, les auteurs de crimes et délits se laissent eux-mêmes souvent piéger par la complexité des nouvelles technologies et abandonnent des traces susceptibles de les confondre. Le célèbre criminaliste français Locard disait bien à propos de l'élément matériel que "nul ne peut agir avec l'intensité que suppose l'action criminelle sans laisser des marques multiples de son passage…". Ce principe s'adapte certainement aux traces électroniques: les affaires récentes en matière de pédophilie l'ont clairement démontré. Il existe donc encore un potentiel de développement de méthodes d'investigation qui exploitent davantage les faiblesses des auteurs. •|

L'anonymat et Internet

Gilberto Girardello

Gilberto Girardello

Dans le monde réel, l'anonymat est largement utilisé: acheter son journal, faire ses courses, aller au théâtre, vous pouvez acheter une carte téléphonique à prépaiement et téléphoner où bon vous semble et sans pour autant donner votre identité lors de l'achat de la carte. De même dans un pays démocratique le vote s'effectue de manière anonyme.

Ingénieur ETS en Electrotechnique.

15 ans dans une société basée dans la région lausannoise spécialisée dans l'analyse fondamentale (spectrométrie X, OE, ICP).

Ingénieur de Service, puis Responsable support technique de deux lignes de produits.

Depuis plus de 3 ans, expert en informatique dans une entreprise publique.

Un nouveau venu à Internet ne réalise pas que chaque message posté dans les groupes de discussion, chaque message électronique envoyé, chaque page du ouaibe visitée, chaque banner visionné ainsi que chaque achat effectué laisse une trace de son passage sur Internet et que celle-ci est enregistrée.

Certains logiciels appelés "adware" sont pourvus de modules appelés "spyware" qui, à l'insu de l'utilisateur, collectent des informations sur ses habitudes (pages visitées, banner téléchargés, etc..) et qui les envoient sur des sites définis par les auteurs du "spyware". Ces traces ou enregistrements de données personnelles, peuvent être ensuite collectés par des personnes tierces et intégrées dans des bases de données qui sont ensuite revendues à des fins commerciales et également à d'autres fins.

Il est facile d'enregistrer et de préserver pour "l'éternité" les traces qui sont laissées sur Internet. Pour s'en convaincre et si l'on est un utilisateur d'Internet des premières heures, il suffit d'effectuer une requête avec son adresse e-mail ou son nom sur un site gratuit comme Google... Le résultat est sidérant.

Il se peut que même en prenant des précautions pour ne pas être "immortalisé" sur le net, une tierce personne, par exemple la société des amis boulistes dont vous faites partie ait publié la liste de ses membres, ainsi, votre nom, adresse et numéro de téléphone sont à disposition sur Internet à votre insu.

Il y a un autre aspect, par effet d'accumulation des traces laissées sur Internet, un "dossier virtuel" de chaque internaute peut être constitué. Pour autant que l'on dispose des bonnes

bases de données, en effectuant une requête, il devient possible de connaître le profil de chaque internaute. Des personnes malveillantes pourraient être tentées de tirer des avantages financiers ou tout autre avantage souvent illégaux, de données aussi sensibles.

L'anonymat est une des réponses à la protection de la vie privée. Par exemple un achat avec une carte de crédit d'une marchandise sur Internet peut être rendu anonyme par l'emploi d'un agent tiers (paypal). Ainsi, la société émettrice de la carte de crédit ne verra pas quelle est la société qui est la bénéficiaire de la transaction.

L'anonymat peut être utilisé de deux façons distinctes. L'anonymat peut être persistant, par l'emploi d'un ou de plusieurs pseudonymes, c'est-à-dire d'une ou plusieurs identités qui ne peuvent pas être liées de façon directe avec l'identité réelle de l'utilisateur. L'anonymat peut être momentané, par l'emploi d'une identité anonyme, c'est-à-dire l'emploi d'un site qui rend l'utilisateur anonyme seulement le temps nécessaire pour envoyer un e-mail ou pour obtenir une page du ouaibe.

Dans un cas comme dans l'autre, il s'agit d'une relation de confiance entre le site qui permet l'anonymat et l'internaute.

Idéalement, le site relais ne doit conserver aucun fichier de la relation avec l'internaute. Il existe plusieurs types de sites qui permettent l'anonymat, les plus efficaces étant ceux dont un relais existe entre plusieurs serveurs anonymes, ils sont également disposés géographiquement de manière opposée et les transmissions entre sites sont chiffrées, le but étant de rendre aussi difficile que possible l'identification de l'utilisateur réel. L'envoi de e-mails, qu'ils soient effectués avec un pseudonyme ou de manière anonyme devrait être chiffré avec PGP ou à l'aide d'un certificat X.509 afin de conserver la confidentialité et éviter qu'une personne tierce par interception du message puisse lire ou modifier le contenu.

Pour limiter l'usage de l'anonymat et aussi pour mieux contrôler les personnes qui utilisent Internet, des ébauches de "signatures numériques" ont vu le jour dans les années nonante. Ainsi Intel avait introduit le numéro de série pour la famille de processeur Pentium 3. Ce numéro de série devait permettre de "tracer" les ordinateurs dérobés. Microsoft avait également introduit dans sa suite Office 97, un "cookie" qui dès l'enregistrement d'un document sur un support magnétique ajoutait l'adresse MAC de la carte réseau à tous documents créés sur l'ordinateur, donc tous les documents avaient une "signature numérique" ce qui permettait d'identifier l'ordinateur sur lequel le document avait été écrit.

Le tollé engendré par ces mouchards a eu raison de l'utilisation de ces derniers. En effet, le numéro de série des Pentium 3 n'a pas été utilisé, de même, la génération du numéro de série des documents créés avec Office 97 a été supprimée avec l'application du service pack 1 d'Office 97.

Certaines sociétés industrielles dont Microsoft, Intel et AMD sont en train de développer tout un arsenal de mesures qui ont pour but de contrôler le contenu de l'ordinateur de monsieur tout le monde (TCPA = Trusted Computing Platform Alliance)

À l'aide de ces mesures, il sera pratiquement impossible de rester anonyme lors de l'utilisation d'un ordinateur (surf sur le ouaibe, envoi de e-mails, création de documents etc..)
Si ces mesures entrent en vigueur, il sera possible pour un éditeur de logiciels de vérifier la licence du logiciel à distance, la maison Warner pourra vous vendre des DVD qui ne peuvent être visionnés que trois fois, si vous désirez le visionner à nouveau, il faudra s'acquitter d'une nouvelle taxe. L'utilisation d'un logiciel sans licence pourra être détectée et ce dernier pourra être effacé. Le verrouillage de documents créés avec un logiciel

Microsoft pourra rendre l'ouverture de ce dernier impossible avec un autre traitement de texte, la location de logiciels deviendra effective et en cas de non-paiement, il sera possible de bloquer l'utilisation du logiciel, voire des documents qui ont été créés avec ce dernier. L'échange de musique ainsi que la copie de logiciels seront rendus impossibles, car le déverrouillage ne pourra se faire qu'après l'obtention d'une clé numérique payante appropriée. Il sera également possible de censurer des sites ouaibes et des documents jugés inappropriés.
Depuis plus d'une année déjà, certaines personnes voient dans Internet le grand méchant loup qu'il faut absolument maîtriser. Il faudrait donc d'après eux, verrouiller et contrôler tous les utilisateurs et censurer les sites inappropriés. Heureusement, des groupes de personnes se mobilisent afin d'éviter qu'Internet devienne un monde aseptisé où toutes personnes n'ayant pas les mêmes points de vue seraient mises au ban de la société.

Certes, il y a des groupes de personnes sans scrupules qui profitent de l'anonymat sur Internet pour commettre des actes délictueux comme la distribution de logiciels, musiques et autres films soumis à des droits d'auteurs. Les DoS (Denis de Service) et autres attaques ciblées sont effectuées à l'aide d'outils qui rendent la traçabilité de l'attaque impossible, il y a également l'emploi de Usenet et du E-mail pour l'envoi de courrier non sollicité (Spam). Ces types de problèmes peuvent être réglés par une plus grande surveillance des sites sensibles, une amélioration des logiciels de détection, des tests de validation de logiciels plus pointus et par une sensibilisation de l'utilisateur. Une collaboration plus rapide et une harmonisation des lois entre États permettraient d'enrayer la cyber-criminalité. •|

Adresse du site	Programme
• Pour surfer de manière anonyme:	
http://www.inetprivacy.com	a4proxy.exe
http://www.veins.org	proxyswitcher.exe
• Pour surfer et conserver son "intimité":	
http:/www.privoxy.org/	privoy_setup_3_0_0-3.exe
• Pour éradiquer les "spyware" de son ordinateur:	
http://www.lavasoft.de	aaw.exe
• Pour chiffrer ses e-mails:	
http://www.pgpi.com	pgp800-pf-w.exe
• Pour obtenir un certificat X.509:	
http://www.thawte.com	
• Anti-virus:	
http://www.kaspersky.com http://www.symantec.com/nav/nav_9xn http://www.free-av.com	
• Pare-feu:	
http://www.zonealarm.com http://www.portslock.com	

Références:
http://www.anu.edu.au/people/Roger.Clarke/DV/AnonLegal.html
http://www.cl.cam.ac.uk/~rja14/tcpa-faq.html

Avantages	Inconvénients
Utilisation d'un nouveau PROXY à chaque requête Fake IP Utilisation simple	Ne fonctionne pas derrière un FIREWALL Prix
Gratuit Utilisation d'un nouveau PROXY à chaque requête (manuel)	Ne fonctionne pas derrière un FIREWALL Pas de liste de PROXY prédéfinie
Gratuit Multi platforme Windows, Linux, etc.. Détection des pixels invisibles	Dans certains cas, la page demandée ne peut pas être affichée (utilisation par le site demandé d'un anti-privacy)
Gratuit Simple à utiliser Possibilité d'utiliser un logiciel de mise à jour de la définition des spywares	Mise à jour sporadique de définition des spyware
Gratuit	Pas d'intégration pour la messagerie électronique Pas de PGP disk
Gratuit Simple à utiliser Possibilité de devenir notaire thawte	Pour obtenir la certification (relation de confiance), il faut donner son identité
Le plus efficace Le plus connu Gratuit	Prix + Souscription annuelle Souscription annuelle -
Le plus efficace Le plus complet	- Prix + Complexité

Nota bene:
Peur de Windows et des rumeurs concernant les chevaux de Troie qu'il pourrait éventuellement contenir ?
Alors essayez LINUX ! … C'est gratuit !

Privacy-enabled Services for Enterprises

Günter Karjoth, Matthias Schunter and Michael Waidner

IBM Research Zurich Research Laboratory
http://www.research.ibm.com/privacy

Dr. Guenter Karjoth is a research staff member at the IBM Zurich Research Laboratory where he is currently working on privacy technologies. Since he joined IBM in 1986, he has been working on various projects in access control in distributed and object systems, mobile code security, and protocol engineering. Dr. Karjoth is author of about 40 international publications. He received his Diplom in Computer Science and his PhD from the University of Stuttgart, Germany. He is a member of the ACM and GI.

Dr. Matthias Schunter has been researcher in computer science at the Universities of Hildesheim and Dortmund since 1994. His research interests include formal modeling in privacy and the design of protocols providing multi-party security. He has participated in the projects CAFÉ on off-line electronic payments, and in SEMPER aiming at an open integrated solution for global electronic commerce. He was also group leader of the MAFTIA project which combines fault-tolerance and cryptography. All three projects were supported by the European Union. He received a diploma in Computer Science at University Hildesheim and he holds a PhD (Dr.-Ing.) in Computer Science from Saarland University.
Since April 2001, he is a member of the research group "Network Security and Cryptography" at the IBM Research Lab Zurich. This group is a leading contributor to the Privacy Research Institute of IBM. Dr. Schunter is author and co-author of more than thirty technical papers on security and privacy.

Dr. Michael Waidner. Manager of the Network Security and Cryptography Research Group at the IBM Zurich Research Lab and institute executive of the IBM Privacy Research Institute.
For my current projects see the project pages of my research group at IBM and of the IBM Privacy Research Institute. For my publications see the list of Sirene (which contains all my publications until mid 2002), or the list of my research group at IBM or the general paper search engine of IBM Research.

I'm co-organizing the ETH Colloquium on Information Security at the Swiss Federal Institute of Technology (ETH) in Zurich. For organizational questions regarding this colloquium please contact Prof. Jürg Nievergelt.

The IBM Enterprise Privacy Architecture (EPA) is a methodology for enterprises to provide an enhanced and well-defined level of privacy to their customers. EPA is structured in four building blocks. The privacy regulation analysis identifies and structures the applicable regulations. The management reference model enables an enterprise to define and enforce an enterprise privacy strategy and the resulting privacy practices. The privacy agreement framework is a methodology for privacy-enabling business process re-engineering. It outputs a detailed model of the privacy-relevant players and activities as well as the privacy policies that govern these activities. The technical reference architecture defines the technology needed for implementing the identified practices.

Consumer privacy is a growing concern in the market place. While privacy concerns are most prominent for e-commerce (see for example [1, 7]), the concerns for traditional transactions are increasing as well. Some enterprises are aware of these problems and of the market share they might loose if they do not implement proper privacy practices. As a consequence enterprises publish privacy statements that promise fair information practices. Written in natural language or formalized using the World Wide Web Consortium's "Platform for Privacy Preferences Project (P3P)" [8], they only constitute privacy promises and are not necessarily backed-up by technological means. In addition, laws increasingly impose baseline privacy regulations. Enterprises willing to implement fair privacy practices usually face the following problems:

- Business processes are designed without considering privacy requirements. Thus, enterprises are forced to create stockpiles of personally identifiable information (PII or short personal data) instead of collecting personal data when needed for the business at hand.
- Existing services often identify users even though their identity is not needed for the business at hand. Privacy-enhancing security technology that provides security with less data is rarely used.
- Enterprises store a variety of personal data. Larger enterprises may not know what types of PII are collected and where it is stored.
- Enterprises may neither know the consent a customer has given nor the legal regulations that apply to a specific customer record.

Enterprises that want to respect the privacy of consumers need three main technologies.

Privacy-enabling design includes techniques that make services more privacy friendly. A core building block is data minimization. The goal of data minimization is to minimize the amount of personal data than needs to be collected to achieve the objectives of an enterprise. This includes privacy-enabling applications that are designed to provide services while minimizing the data needed. Tools for such applications are pseudonymity systems and anonymous authentication schemes [3].

Even with privacy-enabled design, an enterprise still stores a certain amount of personal data. The customers are required to trust the enterprise to use this data as promised in a privacy policy. Privacy management services help enterprises to enforce the promised practices in an auditable way.

Without computer security, a company cannot guarantee privacy. Privacy-enabled security services are needed to secure the infrastructure running the enterprise privacy man-

agement services. Nevertheless, existing security technology often provides security without privacy. Examples are non-anonymous identification and authentication schemes, data collected by intrusion detection systems, and coarse access control. In order to enable privacy, these technologies need to be transformed into privacy-enabling security services. Analogously to privacy-enabled applications, the goal is to provide security without collecting personal data about honest users. The goal of the IBM Enterprise Privacy Architecture (EPA) is to solve these problems while concentrating on the enterprise-related aspects. Essentially, EPA is a methodology for enterprises to provide a welldefined and enhanced level of privacy to its customers. It provides the foundation for the privacy part of IBM's Security and Privacy Services.

1 The IBM Enterprise Privacy Architecture

The IBM Enterprise Privacy Architecture is a methodology that allows enterprises to maximize the business use of personal information while respecting privacy concerns and regulations. It provides a sustainable privacy management system, which can be customized to the total set of privacy regulations and privacy choices facing an enterprise.

EPA introduces privacy-awareness and privacy services into enterprises in a systematic and complete way. Figure 1 illustrates its components, outlined in form of a pyramid. As a prerequisite, the EPA privacy regulation analysis identifies and structures the applicable regulations. The Management Reference Model (top 3 layers in Figure 1) constitutes the tip of the EPA pyramid, defining the privacy strategy and practices of the enterprise. The

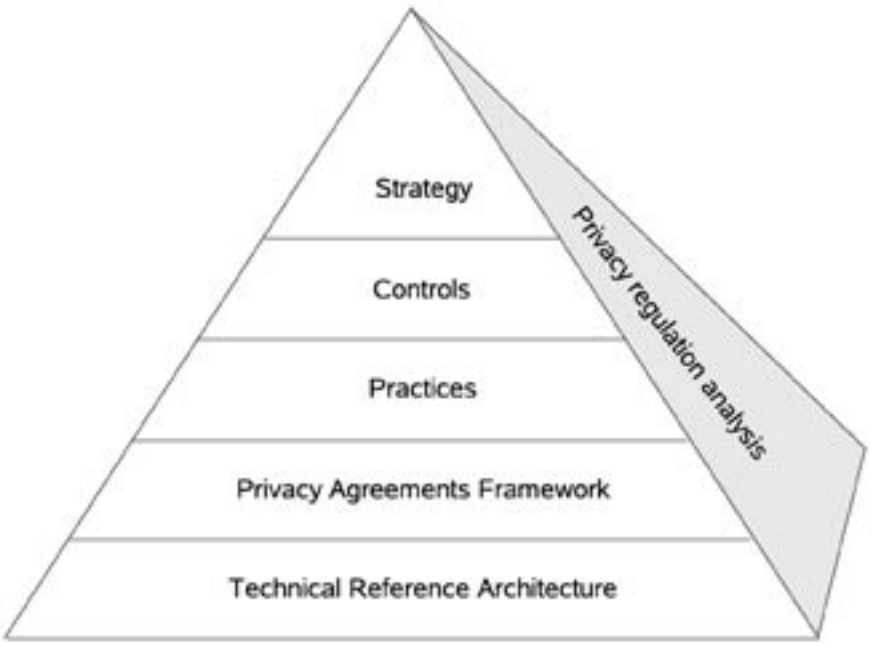


Figure 1. Building Blocks of the IBM Enterprise Privacy Architecture

Privacy Agreements Framework provides a privacy-enabled model for privacy-enhanced business process re-engineering. The lowest layer is the Technical Reference Architecture that defines the technology for implementing the required privacy services.

1.1 Privacy Regulation Analysis

Regulatory compliance is a primary driver of privacy-related activity in the marketplace. Thus, it is clear that a useful picture of the regulatory landscape is a pre-requisite to developing any kind of privacy architecture. The challenge is that regulations are typically written in dense legal style with formats and terminology that tend to differ depending on their origin and purpose.

EPA addresses this challenge by regulatory summary tables and regulation rules tables. Regulatory summary tables summarize the applicable regulations using a unified terminology. The regulation rules tables identify data that is in the enterprise as well as the legal restrictions on using such data. The regulation rules tables are enterprise-specific and more formal than the regulation summary table. An entry describes which party can perform which action on which type of data, the resulting privacy obligations, and a reference to the legal regulation. In addition, the four businessuse phases Collection, Retention, Processing and Use ("CRPU") are used to categorize the scope of privacy regulations.

1.2 Management Reference Model

The EPA Management Reference Model addresses the enterprise-wide processes necessary for a comprehensive privacy management program. These processes are structured and linked to drive the program starting from a strategic view down through the implementation of privacy practices (see Figure 1).

Strategy defines the privacy philosophy, the highlevel policies and identifies the applicable regulations. This represents the highest level of an enterprise's privacy program and embodies its philosophy, its policies and the regulations it will adhere to. The outputs are a privacy strategy as well as a security strategy. Both define what an enterprise will do for protecting privacy and security.

Control defines the general controls necessary to enforce policy. Its components are a Privacy Requirements Process, the Information Asset Classification and Control, a Compliance Enforcement Process, a definition of the Organizational Roles and Responsibilities as well as an Employee Education Program.

Practices defines the incorporation of policy into business processes.

This represents the level of an enterprise's privacy program that translates privacy policy obligations into the general processes, programs and activities that will implement them. Its components are a Privacy Statement declaring the enterprise policy, a Customer Preference Program for defining optin and opt-out choices, an Individual Participation Process that enables customers to access their data, a Dispute Process, an External Communication Program that advertises the privacy efforts of an enterprise, and Information Access Controls that protect the enterprises' data and resources.

1.3 Privacy Agreements Framework

The Privacy Agreements Framework models the transaction level management of privacy at the points where enterprises use personal information within business processes. This includes processes that connect the individual to the enterprise, processes linking people and departments within the enterprise, and processes linking the enterprise with third parties. This model can then be used to identify privacy agreements that are required between the players involved. The main parts of the model are players, data, and rules:

Players The players are the entities that interact while processing collected data. Basic players are data subjects (persons about whom data is collected) and different data users (enterprises or employees using the data). The player model uses an object-oriented modeling technique to identify the players, their operations on the data, as well as the interactions among the players. The result is documented using UML [2] class and collaboration diagrams.

Data The data model identifies the data needed for the processes. Besides identifying the fields collected in forms, it classifies data into at least three categories:

- Personally identifiable information is the most sensitive kind of information that can be linked to a real-world identity. Examples include a tuple name/surname or a U.S. social security number.

- Depersonalized Information is PII where the identifying information has been replaced by a pseudonym. Even though this data is less sensitive, some parties are able to repersonalize it by replacing the pseudonym with the identifying information. Examples include the age with a customer number.

- Anonymized Information contains no identifying information or pseudonyms. It is the least sensitive kind of information that can be obtained by removing all personal data from a set of data. For anonymized data, it is required that identifying the data subject given the data is virtually impossible. Examples include the town of residence or an age in years on its own (i.e., without any other information that may enable identification of the data subject).

Rules The rules model identifies the rules that govern the usage of data by players and their operations. It defines what player may perform which operation for what purpose. In addition, rules may impose conditions and may define obligations that result from performing an operation.

1.4 Technical Reference Architecture

To guarantee that an enterprise provides sufficient privacy to its customers, privacy-enforcement needs to be deployed on an enterprise-wide scale. All applications that handle personal data need to make sure that the handling adheres to the promised policies. An enterprise-wide privacy-management system uses at least three types of systems (see Figure 2):

The Policy Management System enables the administrators of the system to define, change and update privacy policies. It distributes the privacy policies to the privacy enforcement systems.

The Privacy Enforcement System enforces the privacy protection for each individual resource that stores privacy-relevant data. It obtains policies from the policy management system and offers auditing data to the audit console. The privacy enforcement system is usually split into two parts: A resource-specific resource monitor shields the resource and a resource-independent authorization director evaluates the policies and decides whether requests are granted or not.

The authorization director authorizes operations on the collected data. After evaluating the policy, the authorization director returns whether the request is authorized or not and whether an authorized request implies any privacy obligations. Each kind of protected resource (database, CRM system,…) uses a corresponding resource monitor. This monitor shields the resource from direct access. Each incoming request is translated into a call to the authorization director. Only if the authorization director authorizes the request, the request is forwarded to the resource. The resource monitor records audit data and tracks pending privacy obligations.

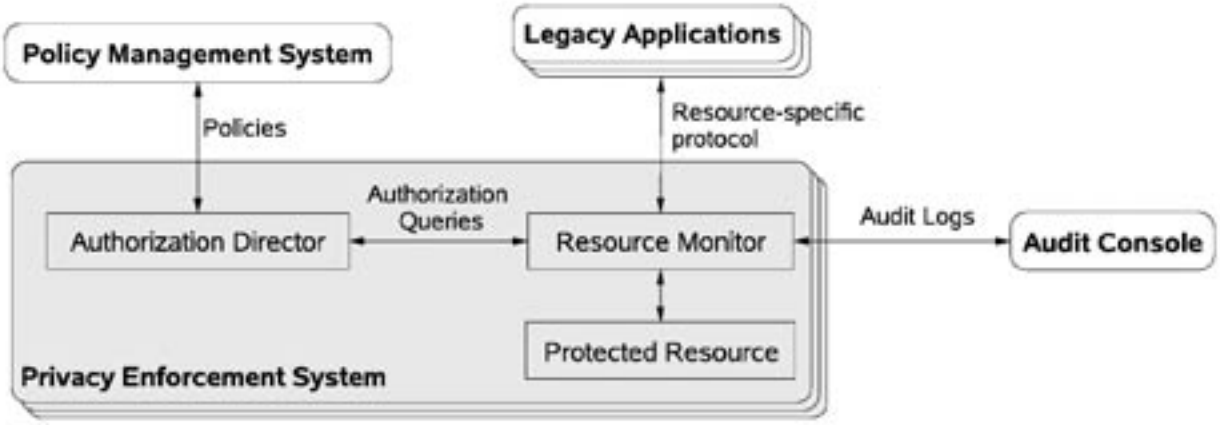


Figure 2. Components of a Enterprise Privacy Enforcement System

Audit Console This system enables the Privacy Officer to review the audit information stored in the enforcement nodes and the policies distributed by the policy management systems. The Platform for Enterprise Privacy Practices (EP3P) is a refinement of the EPA Technical Reference Architecture [5, 6]. It enables enterprises to formalize and enforce privacy practices and to manage the consent of their customers.

2 Benefits for the Enterprise

EPA helps enterprises leverage personal data while protecting privacy. It recognizes the issues and investment relating to existing personal data in legacy systems as well as those generated by e-business initiatives. As such, EPA's value revolves around the following:

Enhance and preserve the value of data assets. The data model of the Technical Reference Model provides for the identification and categorization of personal data within the organization and thereby allows the establishment of appropriate protection measures.

Operate consistently with multiple privacy regulations and standards. The privacy regulation analysis helps to identify compliance obligations across different jurisdictions and express these in common terms. The applicable regulations are formalized by an enterprise privacy policy that is associated with any collected data. This so-called "sticky policy paradigm" supports identifying the applicable regulations and privacy promises for all personal data in an enterprise.

Build and promote trust in the marketplace. EPA enables customers to retain control over their data.

The Management Reference Model enables and promotes responsiveness and privacy awareness of the enterprise. Together with external auditing, these measures promote trust of the customers.

Realize substantial privacy management choices. The regulatory analysis reveals compliance choices. This analysis highlights choices for uses of less sensitive data types and shows high risk and redundant privacy relationships.

Operate a sound platform for persistent privacy management. The Requirements Process within the Management Reference Model ensures ongoing environmental input on privacy.

3 Conclusions

The IBM Enterprise Privacy Architecture enables enterprises to provide an increased and well-defined level of privacy to their customers. It enables enterprises to act as the custodians of their customer's personal data that protect against privacy violations by themselves or others. Note that the Enterprise Privacy Architecture assumes that the customers trust the privacy administrators and privacy enforcement systems of the enterprise to some extent (Of course, this trust can be reduced by external audits and on-line auditing systems that are maintained by independent parties). The systems then protect the customer's data against privacy violations by regular employees or systems.

An important aspect of EPA's privacy enforcement system is the management of the data subject's consent on a per-person basis. Consent management includes the management of the consented policy as well as the management of the users opt-in and opt-out choices. The core of EPA's notion of consent management is the sticky policy paradigm: When submitting data to an enterprise, the user implicitly consents to the applicable policy and to the selected opt-in and opt-out choices. Opt-in and opt-out choices as well as the consented policy are associated with the collected data.

This holds even if the data is sent to another enterprise. Note that policy management on a per-user-basis is useful once consent and different sources need to be considered [4]. Examples are managing data of different policy versions (e.g., due to different collection times), different user roles (e.g., premium and users funded by advertising), or users from different legislation (e.g., Europe and US). •|

Acknowledgments

We would like to thank Kathy Bohrer, Nigel Brown, Jan Camenisch, Calvin Powers, and Els Van Herreweghen for valuable comments. In addition, we would like to thank all members of the EPA team for the productive cooperation.

References

[1] Mark S. Ackerman, Lorrie Faith Cranor, and Joseph Reagle. Privacy in e-commerce: examining user scenarios and privacy preferences. In 1st ACM Conference on Electronic Commerce, pages 1-8. ACM Press, 1999.

[2] Grady Booch. Object Oriented Analysis and Design. Benjamin Cummings, 1994.

[3] Jan Camenisch and Anna Lysyanskaya. An efficient system for non-transferable anonymous credentials with optional anonymity revocation. In Advances in Cryptology - EUROCRYPT '2001, Lecture Notes in Computer Science 2045, pp.93-117. Springer, 2001.

[4] Rüdiger Grimm and Alexander Roßnagel. Can P3P help to protect privacy worldwide? In ACM Multimedia Workshop, pages 157-160. ACM Press, 2000.

[5] Günter Karjoth, Matthias Schunter, and Michael Waidner. The Platform for Enterprise Privacy Practices – Privacy-enabled Management of Customer Data. To appear in 2nd Workshop on Privacy Enhancing Technologies (PET2002). April 2002.

[6] Günter Karjoth, Matthias Schunter, and Michael Waidner. A Privacy Model for Enterprises. To appear in Computer Security Foundations Workshop (CSFW2002). IEEE Press, 2002.

[7] Sarah Spiekermann, Jens Grossklags, and Bettina Berendt. E-privacy in 2nd Generation ECommerce: Privacy Preferences versus actual Behavior. In Electronic Commerce (EC'01), pages 38-47. ACM Press, 2001.

[8] The Platform for Privacy Preferences (P3P), W3C Candidate Recommendation, http://www.w3.org/TR/2000/CR-P3P- 20001215, 2000.

Convenience versus Security und Privacy in d stationären und elektronischen Verkaufsplatt

Rolf Gasenzer

Rolf Gasenzer

Überlegungen zu den "Economics" von Datenschutzmechanismen für den Endanwender: Wo liegen die Bedürfnisse im Rahmen seines alltäglichen Kaufverhaltens?

1979 - 1984 Wirtschaftswissenschaftliches Studium Universität St. Gallen (HSG, Studienrichtung Betriebswirtschaft, Vertiefungsrichtung Marketing)
1982 – 1986 IBM (Schweiz) AG, Systems Engineering und Industry Marketing
1986 – 1999 Furrer & Partner AG, Bereichsleiter Telecommunications und Electronic Publishing, Mitglied der Geschäftsleitung
ab 1999 Pixelpark (Schweiz) AG, Senior Consultant
ab 1995 Hochschule für Technik und Informatik, Berner Fachhochschule, Lehrbeauftragter und anschliessend Professor für Wirtschaftsinformatik sowie Leiter des CCEC (Competence Center Electronic Commerce)

Datenschutz ist Persönlichkeitsschutz. Der 45-jährige Schweizer setzt seit über 20 Jahren regelmässig seine Bancomat-Karte für den Geldbezug am Automaten ein, namentlich wenn er aus Sicht der Diffusionstheorie zur Gruppe der Early Adopters gehört. Im Laufe der Zeit kam wie eine Selbstverständlichkeit das Bezahlen im Laden mit dem EFT/POS-System dazu, indem die vertraute und bereits im breiten Einsatz stehende Bancomat-Karte unter der Bezeichung EC-Direct mit der entsprechenden Funktionalität ergänzt wurde. Je nach beruflicher Ausrichtung folgte bereits in den frühen achtziger Jahren sicher aber zu Beginn der neunziger Jahre in weiten Kreisen in der Schweiz der regelmässige Einsatz einer Kreditkarte. Alle diese Transaktionen sind grundsätzlich in einem IT-System abgebildet. Das heisst: Wir blicken auf eine bereits zwei Dekaden umfassende Geschichte hinsichtlich einer relativ dichten und individualisierbaren elektronischen Datenspur jedes Einzelnen zurück. Wenn wir uns noch vor Augen führen, dass die angesprochenen Zahlungsmittel in der Schweiz unter dem Konzerndach der Telekurs AG (einer Gesellschaft im Mehrheitsbesitz der Schweizer Banken) in verschiedenen Tochterfirmen (Europay, der damaligen Payserv und weiteren mehr) zusammenliefen, dann müsste doch eigentlich einige Brisanz in der Fragestellung liegen, ob hier einem allfälligen Missbrauch dieser – auch im Sinne des Datenschutzgesetzes – sicher schutzwürdigen Daten nicht bereits Tür und Tor geöffnet ist?

Das marktpsychologische Phänomen "Vertrauen"

Trotzdem scheint der Normalbür-

len Konsumentenmärkten der Schweiz auf tformen

ger ohne viel Federlesens von diesen Geldversorgungs- und Zahlungsmöglichkeiten Gebrauch zu machen, da sie infolge ihres bequemen Einsatzes das Nutzenniveau des Anwenders – nicht zuletzt auch hinsichtlich der Orts- und Zeitsouveränität – markant steigern. Neben diesen Satisfaktoren im Herzberg'schen Sinne scheinen auch mögliche Dissatisfaktoren aus dem Wege geräumt. Während der gesamten oben angesprochenen informatikgeschichtlichen Periode konnte kein nennenswerter Fall von Missbrauch irgendwelcher Art festgestellt werden. Dies, obwohl es für einen Konzern wie Telekurs naheliegend wäre, aus der Verknüpfung der unterschiedlichen Datenbestände in den Konzerntöchtern weiter Kapital zu schlagen, indem beispielsweise Kaufverhaltensmerkmale zu spezifischen Kundendsegmenten zusammengezogen und dann auf dem Address-Broking Markt als direkt adressierbare Prospectslisten für Direct-Mail Kampagnen angeboten würden. Es ist also festzuhalten, dass diese Payment Service Provider sich einer – natürlich auch durch die Schweizer Gesetzgebung mitbeeinflussten – Selbstbescheidung unterziehen, was auf Anwenderseite wiederum ein Vertrauenspotential über lange Jahre fehlerfreien Betriebs aufbaut, das nicht so leicht zu erschüttern ist. Diesem Umstand ist es bis zu einem gewissen Masse auch zuzuschreiben, dass die Schweizer Konsumentenschaft auch den Lockrufen der Grossverteiler gefolgt ist und sich in der breiten Mehrheit ohne grosses Zögern eine Cumulus- (MIGROS) bzw. Super-Card (COOP) hat ausstellen lassen; und zwar im Bewusstsein, dass gerade diese Kundenbindungsinstrumente dazu dienen sollten, über Kaufverhaltensanalysen das Angebot der Grossverteiler noch kundengerichteter gestalten zu können. Die Kundschaft liess sich dies mit einem nachschüssigen Rabatt von rund einem Prozent auf grössere Sortimentsbezüge abgelten.

(Marken-)Bekanntheit der Marktteilnehmer als entscheidener Faktor…

Es ist ersichtlich, dass in jenen Bereichen, in denen die Marktteilnehmer auf Anbieterseite gut bekannt sind und demzufolge über eine vertrauenserweckende Marke ("Brand") verfügen, auf Seiten der Kundschaft auch ein grosses Mass an Vertrauen in ein die üblichen Standards an ethischem Verhalten ansetzendes und die Schweizer Gesetzgebung berücksichtigendes Geschäftsgebahren vorhanden ist; auch und nicht zuletzt was die Verwendung von sensitiven Daten anbetrifft. Dies, obwohl die technologischen Möglichkeiten in den

letzten Jahren auch unter dem Stichwort Geomarketing, welches Adress-, Haushalt- und personenbezogene Daten mit geographischen Visualisierungstechniken in der Weise verbindet, dass auf marketingstrategische und marketingoperative Fragestellungen in äussserst produktiver und auf Optimierungstechniken beruhender Weise direkt für den geschäftlichen Alltag Antworten gewonnen werden können, deutlich erweitert worden sind.

… auch auf elektronischen Plattformen

Heikler wird die Ausgangslage in all denjenigen Fällen, wo der Leistungsanbieter zunächst nicht näher bekannt ist, sei es, dass er aus dem Ausland oder erst seit jüngster Zeit im jeweiligen Zielmarkt operiert. Hinzu kommt nun ein vermehrtes Aufsetzen von Markttransaktionen jeglicher Art auf elektronische Plattformen, die wir unter den Stichworten E-Commerce (bei stationären Anwenderterminals) beziehungsweise M-Commerce (bei mobilen Anwenderterminals) subsumieren können. Beim Agieren auf elektronischen Plattformen sind vom Standpunkt des Konsumenten aus gesehen verschiedene Punkte zu bedenken: Im Gegensatz zum stationären Präsenzverkauf sind die gesamten Aktivitäten des Anwenders in den virtuellen "Shops" zeitgenau und mit allen Interaktionsdetails in den Log-Files für den Anbieter nachvollziehbar. Im weiteren wird durch die Repräsentanz der individuellen Identifikationsmerkmale mittels Codierungselementen eine Entpersonalisierung der Markttransaktion vorgenommen. Es gilt nun, aus Sicht der Anwender und der Anbieter wieder eine Authentifizierung des jeweiligen Marktpartners sowie die Integrität der zugrundeliegenden Markttransaktion zu gewährleisten. Diese Virtualisierung der individuellen Identifikationsmerkmale hat in einer möglichst einfachen und sicheren Weise zu erfolgen.

Bestehende und bewährte Mechanismen…

Dabei sind auch – lediglich auf den ersten Blick – rudimentäre und archaisch anmutende Verfahren durchaus zielführend. Ein Beispiel hierfür liegt im Telebanking, das nun in der Schweiz hinsichtlich des Zugriffs auf die persönlichen Konten und den Zahlungsverkehr für das breite Publikum auf eine über fünfzehnjährige Periode einwandfreien Betriebes ohne Sicherheitsprobleme zurückblickt. Telebanking wurde zuerst auf proprietären nationalen Plattformen wie Videotex angeboten und im Zuge der Migration verschiedener Applikationen auf das World Wide Web (WWW) auch ins Internet integriert. Was gleich blieb, war der Indentifikationsvorgang, der sessionspezifisch bei einer durchschnittlichen Häufigkeit von rund einer Session pro Woche genügend einfach handhabbar war. Neben den Indentifikationsmerkmalen der Vertragsnummer und des persönlichen Passwortes (bzw. PIN, Personal Identification Number) wird ein nur für eine Session gültiges Zusatzmerkmal eingesetzt. Auf der sogenannten Streichliste mit typischerweise einigen Dutzend mehrstelligen Zahlenkombinationen, die dem Anwender vor Aufbrauchen jeweils über einen automatisierten Mail-Order Prozess wieder zugeht, wird in vorgegebener Reihenfolge jeweils eine Zahl "verbraucht", also "abgestrichen". Das Papier mit den Streichnummern, das auf Wunsch auch durch einen elektronischen Zahlengenerator im Kreditkartenformat ersetzt werden kann, ist einfach mitzuführen und bietet damit den standortunabhängigen Zugriff auf die eigene Kontobasis, wo immer auch ein geeignetes WWW-Terminal vorhanden ist.

…in ihrer Benutzerfreundlichkeit…

Diese Lösung ist hinsichtlich ihres tieffrequenten Einsatzes genügend benutzerfreundlich. Bei höherfrequentem Einsatz, der typischerweise in E-Commerce und Mobile-Commerce-Anwendungen vorherrscht, wo mehrere Transaktionen pro Tag getätigt werden (man denke insbe-

sondere an kleinpreisige Informationsprodukte für Informationsbezüger in ihrem geschäftlichen und privaten Alltag), sind hier aber anderer Lösungen gefragt, die dem Idealzustand eines "One-Stop Shoppping, Billing and Payment" nahekommen. Auf Seiten des Anwenders steht der einfache Bezug einer (Informations-)Leistung im Vordergrund und eine damit verknüpfte simple aber sichere Form der Bezahlung. Dazu ist es wichtig, kioskartige Lösungen zu entwickeln, die es dem Anwender erlauben, sich pro Session nur einmal identifizieren und allfällige Leistungsbezüge zur Verrechnung autorisieren zu müssen, um sich danach ungehindert im Informationsraum verschiedener Content Provider bewegen und nach Bedarf „auf Knopfdruck" (Informations-)Leistungen beziehen zu können. Aktuell finden wir in den unter den Stichworten "Electronic" und "Mobile" Payment in der Praxis figurierenden Ansätzen dieses "One-Click"-Protokoll nirgends. Dies hängt nicht zuletzt auch mit den eingesetzen "Token" für die Identifikation, Athentifizierung und Autorisierung zusammen, die von den Formfaktoren her oft in verschiedene Soft- und Hardwarekomponenten aufgeteilt sind.

…mit neusten Technologien kombinierbar

Es wird zuwenig nach Ansätzen gesucht, die auf alltagsgebräuchliche Gegenstände abzielen, welche ohnehin vom Anwender immer mitgeführt werden. Einer dieser Gegenstände ist das Mobiltelefon. Ein Handy neuerer Bauart bietet verschiedene Möglichkeiten der Funktionalitätserweiterung über Programmierungsschnittstellen. Uebergeführt in die Rolle als persönlicher, digitaler Assistent (PDA) mit Sprach- und Datenkommunikationsmöglichkeit sollte sich auch eine Hardware-Erweiterung realisieren lassen, welche mittels biometrischen Schnittstellen (wie beispielweise einem Fingerabdruck) dem Anwender erlaubt, sein Autorisierungs-Token auf einfachste Art zu "öffnen" und in der jeweiligen Session für die Leistungsbezüge auf elektronischen Plattformen einzusetzen. Damit wird vermieden, dass weitere Zugangscodes beim Anwender "memorisiert" werden müssen (was oft auch ein Aufschreiben und Mitführen dieser Zugangscodes mit den damit verbundenen Risiken bedeutet) und gewährleistet, dass die Autorisierung einer Transaktion intuitiv sowie ohne unnötige und damit mühselige Interaktionsschritte vollzogen werden kann. Gelingt es dann noch, die Schnittstelle zu der elektronischen Plattform möglichst berührungslos und von proprietären Zusatzkomponenten unabhängig zu machen, dann ergibt sich daraus auf der Mobiltelefonplattform ein geradezu ideales, weil multifunktionales und in die Tagesabläufe integriertes, Autorisierungs-Token. In diese Richtung sollten verstärkte Aktivitäten bei der Entwicklung auf Hard- und Softwareseite laufen. Insbesondere in den biometrischen Verfahren liegen einige Chancen für anwenderfreundliche Lösungen, die auch im breiten Publikum eingesetzt werden können. Dies gilt es konsequent zu nutzen, um den produktivitätsfördernden und nutzenstiftenden Applikationen im E- und M-Commerce weiter zum Durchbruch zu verhelfen. Denn damit verbindet sich neben der Steigerung des Nutzens auf Stufe der privaten Anwender und der Unternehmen eben auch eine gesamtwirtschaftlich verbesserte Wettbewerbsfähigkeit. •|

Biometrie – Bindeglied zwischen digitaler und physischer Identität

Dr. Lorenz Müller
V.I.P - Mitglieder

Lorenz Müller

Studies in mathematics, physics and philosophy at the University of Bern, Diploma (1979); PhD at the Laboratory for High Energy Physics, Bern, Promotion (1983); Postdoc at SLAC, research in high energy physics, Stanford; Assistant professor, Laboratory for High Energy Physics, University of Bern and CERN (1987-1989); Group leader, Neuro-informatics at the Institute for Informatics, University of Bern (1990-1997) 50%; Group leader technical training, Ascom Tech AG (1990-1995) 50%; Managing director of the postgraduate education program eduswiss (1996- 2002) 50%; Director aR&D, University of Applied Science Berne, HTA Biel; Professor for cryptography and neuronal networks; Managing director eduswiss (since 1992 until end of 2002); Project leader Cod-it (Oct. 2002)

"Jeden Morgen schlich die Alte zu dem Ställchen und rief: ‚Hänsel streck die Finger heraus, damit ich sehe, ob du bald fett bist.' Hänsel streckte ihr aber ein Knöchlein heraus, und die Alte, die trübe Augen hatte, konnte es nicht sehen und meinte es wären Hänsels Finger, und verwunderte sich, dass er gar nicht fett werden wollte."

Dieses kleine Zitat aus Grimms Märchen "Hänsel und Gretel" zeigt, dass die Messung von physischen Merkmalen zur Erkennung von persönlichen und individuellen Eigenschaften schon immer ein Thema war. Das Wissensgebiet, das heute mit fortgeschrittensten wissenschaftlichen Methoden betrieben wird, ist unter dem Namen Biometrie bekannt. Gleichzeitig illustriert das obige Zitat aber auch, dass die Fälschung biometrischer Daten durchaus möglich und das Resultat immer nur so gut wie die Messmethode ist. Der heutige Boom in der Sicherheitstechnologie als Folge der Terroranschläge in den USA hat der Biometrie enormen Auftrieb verschafft. Dies obschon das Gebiet nicht überall den besten Ruf geniesst. Gewisse Bedenken sind durchaus begründet, sind doch mit sehr ähnlichen Methoden unter dem Begriff Physiognomik noch bis weit ins letzte Jahrhundert hinein rassistische und diskriminierende Ideologien auf eine pseudo-wissenschaftliche Basis gestellt worden. Auch neueste, in das weite Gebiet der Biometrie fallende Methoden, wie zum Beispiel die DNA-Analyse verbunden mit der Suche nach problematischen Genen, können begründete und manchmal auch unbegründete Ängste schüren. Breit anerkannt ist die Methodik in der Kriminalistik. Schon seit über 100 Jahren nutzt die Polizei zum Beispiel Fingerabdrücke als Beweismittel bei der Suche und Überführung von Verbrechern[1].

Warum Biometrie

Was hat nun aber zum heutigen Interessenaufschwung für biometrische Methoden geführt. Auf der einen Seite ist da sicher der technologische Fortschritt, der rasche Messungen von Merkmalen und deren Auswertung mit vertretbarem Aufwand und hoher Qualität erlaubt. Auf der ande-

ren Seite steht aber das ungelöste Problem aller Sicherheitskonzepte: Wie verbindet man die digital definierten Identitäten mit den richtigen physischen Personen, die der Identität entsprechen (Fig 1)?

Bei allem Fortschritt, der in der Sicherheitstechnologie gemacht wurde, ist und bleibt die Authentifizierung von Personen der Schwachpunkt in vielen Sicherheitskonzepten. Pässe mit einer meist wenig aussagekräftigen Fotographie, Kreditkarten rudimentär durch eine nur oberflächlich verifizierbare Unterschrift gesichert oder meist leicht zu erratende Passwörter sollen diese Verbindung zwischen Person und digitaler Identität sicherstellen. Eine wahre Einladung für alle Übeltäter. Wieso sollten sich diese mit komplexen mathematischen Problemen auseinandersetzen, um zum Beispiel ein Kryptosystem anzugreifen, wenn es doch so einfach ist eine Identität zu stehlen. Das Problem ist bekannt und kann nicht allein durch Verbesserungen im digitalen Sicherheitssystem gelöst werden. Die Schwachstelle zwischen physischer Person und ihrer digitalen Identität ist mit konventionellen Methoden kaum zu eliminieren. Biometrische Methoden sind nun ein vielversprechender neuer Ansatz, wird doch ein direkter, nur schwierig zu manipulierender Bezug zwischen Daten und Person geschaffen.

Biometrische Methoden

Wie Biometrie funktionieren könnte, wurde kürzlich im Spielberg Film ‚Minority Report' ziemlich drastisch dargestellt. Obschon die Anwendung durch den totalen Überwachungsstaat Science Fiktion ist und hoffentlich auch bleibt, ist die gezeigte Technologie nicht weit von der Realität entfernt. Biometrische Authentifikation basiert auf der Tatsache, dass viele Eigenschaften eines Individuums einzigartig sind und sich lebenslang kaum verändern. In der Biometrie geht es darum, geeignete solche Merkmale zu identifizieren, diese messtechnisch zu erfassen, die Resultate zu parametrisieren und durch geeignete Eichung zu standardisieren. Die wichtigsten Technologien sollen kurz beleuchtet werden.

Fingerabdruck

Allgemein bekannt ist die Einzigartigkeit der Fingerabdrucke. Die Methodik Fingerabdrucke in standardisierter Form zu erfassen und abzulegen ist weltweit erprobt und in der Personenauthentifikation gebräuchlich[2]. Neuestes Beispiel ist die Datenbank Eurodac im Rahmen des Dubliner Abkommens[3]. Wie jedermann an sich

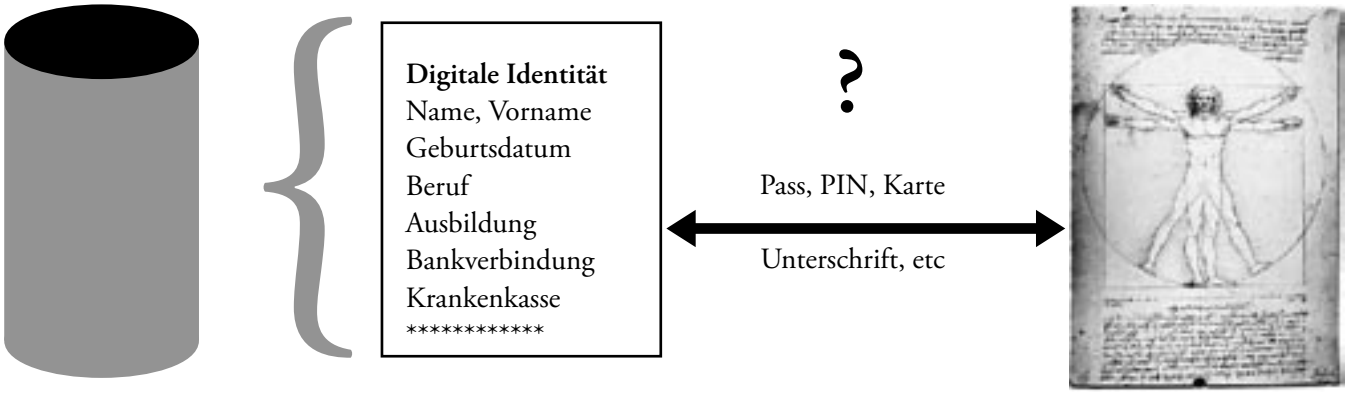


Fig 1 Die Verbindung zwischen physischer Person und ihrer digitalen Identität ist eine notorische Schwachstelle in vielen Sicherheitskonzepten

selbst leicht feststellen kann, bilden die Hautrillen ein Muster von parallel verlaufenden gekurvten Linien, die im äusseren Bereich der Fingerkuppen meist offene Schlaufen bilden. Im zentralen Bereich sind die Rillen zum Teil geschlossen, abrupt endend und können Wirbel bilden. Dieser zentrale Bereich ist besonders reich an charakteristischen Merkmalen. Das globale Muster wird nach bestimmten Kriterien zentriert, orientiert und in Klassen eingeteilt (globale Eigenschaften, siehe Fig. 2). Dazu kommen sogenannte lokale Merkmale, die man als Minutia Punkte bezeichnet. Diese charakterisieren und definieren die Lage und Art von Verzweigungen, Endungen, Einschlüssen, Divergenzen, lokale Rillendichte usw. Heutige Fingerabdruckerkennungssystem identifizieren rund 50-70 solche Minutia Punkte je mit bis zu 7 charakteristischen Merkmalen, so dass die Wahrscheinlichkeit, dass zwei Fingerabdrucke gleich klassiert werden auch unter Berücksichtigung von gewissen Messfehlern gegen Null geht.

Technisch besteht ein Fingerabdruckerkennungssystem aus einem Sensor, der das Rillenmuster erfasst, einem Bildverarbeitungsteil, der die relevanten Merkmale herausfiltert und einem Erkennungsalgorithmus, der die Minutia Punkte nach Lage und Eigenschaften identifiziert. Sensortechnologien basieren entwe-

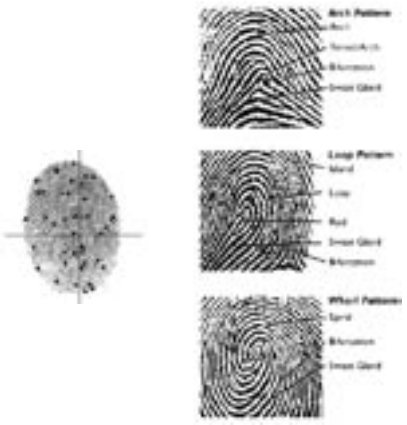


Fig. 2: Minutia Punkte auf einem Fingerabdruck, globale FP-Muster

der auf optischer oder kapazitativer Erkennung der Rillenmuster. Rein optische Systeme sind natürlich anfällig auf Replay-Angriffe (Präsentation von kopierten Fingerabdrucken) und müssen mit zusätzlichen Sensoren die Echtheit des präsentierten Bildes nachprüfen. Kapazitative Sensoren messen die unterschiedlichen elektrischen oder thermischen Eigenschaften zwischen den direkt am Sensor aufliegenden Rillenbergen und den Tälern mit etwas Luft dazwischen. Die Überlistung solcher Sensoren mit gefälschten Fingern ist zwar schwierig aber nicht unmöglich[4]. Nachteil der kapazitativen Sensoren ist ihre Empfindlichkeit gegenüber elektrostatischen Entladungen und ihr Preis (grossflächige Halbleiterchips). Beide Arten von Sensoren werden heute in Erkennungssystemen eingesetzt und können teilweise sogar in Smart-Cards implementiert werden.

Handabdruck

Eine weitere Erkennungstechnologie basiert auf den unterschiedlichen Formen von Handflächen. Handabdruckerkennung ist wohl die erste und einfachste automatisierte biometrische Technologie. Es ist relativ einfach die Grössenparameter einer Hand abzulesen, die Einzigartigkeit ist aber nicht im gleichem Mass gesichert, wie diejenige der anderen genannten Methoden. Für den Anwender ist sie relativ einfach, es muss lediglich die Hand auf eine Erkennungsfläche gelegt werden. Handerkennung wird deshalb noch oft in Hochsicherheitsumgebungen jedoch meist in Kombination mit einem Passwort oder PIN-Code angewandt.

Gesichtserkennung

Wohl die umstrittenste Technologie ist die Gesichtserkennung. Sie erlaubt es Personen ohne deren Einverständnis biometrisch zu erfassen, und dies sogar ohne dass der Erfasste überhaupt etwas davon bemerkt. Aus Sicht des Daten- und Persönlichkeitsschutzes sicher eine fragwürdige Sache. Die Erkennung erfolgt durch die Messung der relativen Positionen und Grössen von Augen, Nase, Mund und anderen

Charakteristika. Obschon Gesichtserkennung noch eine relativ unsichere und fehleranfällige Technologie ist, werden bereits heute solche Systeme in sicherheitskritischen öffentlichen Räumen wie zum Beispiel Flugplätzen, Stadien oder Schalterräumen aber auch für die Authentifikation von berechtigten Personen in Zugangskontrollsystemen eingesetzt.

Iris und Retina

Das Auge ist das auffälligste individuelle Merkmal und es ist wohl kein Zufall, dass sich Menschen, die einander begegnen zur Erkennung in die Augen schauen. Biometrisch interessant ist sowohl das Äussere der Augen (Iris) wie der Augenhintergrund (Retina).

Erst vor wenigen Jahren entdeckt und patentiert worden, ist die Individualität der Iris mit ihrer Struktur und Farbe[5]. Länger bekannt, aber auch erst in den letzten Jahren systematisch genutzt ist das individuelle Muster des Aderngeflechts der Retina im Augenhintergrund[6]. Die erstgenannte Technologie basiert auf der individuellen Struktur und dem Muster der Filamente in der Iris (siehe Figur), während bei der Retinaerkennung das Muster der Adern parametrisiert wird. Beide Methoden sind biometrisch ausserordentlich sicher, das heisst die False Acceptance Rate (FAR) und die False Rejection Rate (FRR) sind vernachlässigbar. Für beide Methoden braucht es aber aufwendige und teure Technologien für die Datenerfassung und insbesondere die Retinaerkennung wird von den erfassten Personen als invasiv und unangenehm empfunden. Ausserdem gelingt die Messung nur, wenn die Personen still halten und direkt in die Detektoren hineinschauen. Die Methoden werden deshalb hauptsächlich in speziellen Anwendungsnischen zum Einsatz kommen.

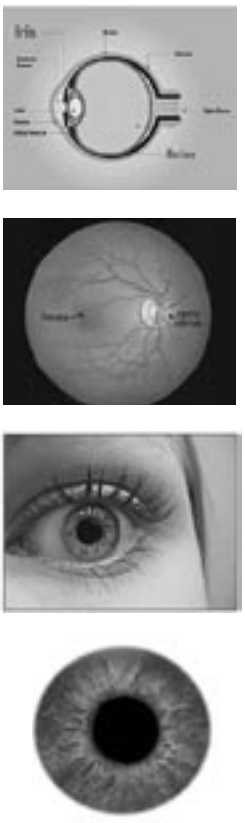


Fig. 3: Iris und Retina haben bei jedem Menschen eindeutig unterscheidbare Merkmale.

Stimmerkennung

Ein grösseres und breiteres Anwendungspotential hat die Stimmerkennung. Es handelt sich, wie bei der unten genannten Unterschriftserkennung um eine verhaltensbasierte biometrische Technologie. In einem Erkennungsprozess wird die Person aufgefordert eine bestimmte Passphrase zu sprechen, die vorher nicht bekannt ist. Dies soll die natürlich naheliegenden Replay-Angriffe durch aufgenommene Stimmen erschweren. Das Frequenzmuster der Stimme wird dann in einem Voice-Print in Funktion der Zeit aufgetragen und mit abgespeicherten Lautmustern der Person verglichen. Stimmerkennung ist eine komplementäre Technologie zur Spracherkennung. Im ersten Fall versucht man möglichst genau ein Stimmmuster zu erfassen, im zweiten Fall wird versucht gemeinsame Phonemmuster aus möglichst vielen unterschiedlichen Stimmen zu identifizieren. Für die beiden unterschiedlichen Probleme sind deshalb nicht die gleichen Erkennungstechnologien anwendbar. Wie alle verhaltensbasierten Methoden muss die Stimmerkennung situationsabhängige Variationen in der Stimmlage ausgleichen können. Das heisst natürlich, dass die Vergleichsmessungen mit grösseren Toleranzschwellen interpretiert werden und sich die Sicherheit der Authentifikation dadurch reduziert.

Unterschrift

Seit Jahrhunderten ist das Unterschreiben die Standardmethode, um zwischen einem Dokument und einer Person einen verpflichtenden Bezug zu schaffen. Die digitale Erfassung von Unterschriften gehört deshalb zu den Basistechniken der Biometrie. Unterschriftsdetektoren erfassen nicht nur das Schriftbild sondern auch die Dynamik der Schreibstiftführung. Trotzdem ist die Unterschriftserkennung, wie alle verhaltensbasierten Methoden nicht sehr sicher, da die natürlichen Schwankungen bei der Unterschriftsabgabe berücksichtigt und damit die Akzeptanzbandbreiten für die Merkmale zu gross gewählt werden müssen. Unterschriftserkennung ist trotz dieser Schwäche in fast allen Geldtransaktionen eine immer noch gebräuchliche Technik.

DNA und verwandte Methoden

Mit der rasanten Entwicklung in der Biotechnologie sind bereits heute völlig neue biochemisch basierte Identifikationssysteme absehbar. Vorläufer dieser Entwicklung ist die DNA-Analyse, die geringste Mengen von Zellmaterial eindeutige einem Individuum zuordnen kann. Es ist absehbar, dass bald weitere biochemische, individualisierende Markersysteme gefunden werden. Vorläufig sind diese Methoden für die unmittelbare Authentifikation noch nicht geeignet, da die Messung nur offline im Labor durchgeführt werden kann. Biochips haben jedoch das Potential diesen Mangel bald zu beheben. Die Entwicklung von biochemisch basierten, kaum mehr angreifbaren Authentifizierungssystemen ist wohl nur eine Frage der Zeit.

Anwendung und Trends in der Biometrie

Biometrie hat sich in den letzten Jahren zu einer wahren Boombranche entwickelt. Dutzende von Startups bieten biometrische Sicherheitstechnologien an. Es hat sich jedoch gezeigt, dass fast alle heute gebräuchlichen Systeme die hochgesteckten Erwartungen punkto Sicherheit nicht vollständig erfüllen können. Zwar ist die Hürde für biometrische Fälschungen deutlich höher, als für das Stehlen von Ausweisen oder digitalen Geheimnissen, wie PIN-Codes oder Passwörtern, trotzdem können die Erfassungssysteme mit etwas Insiderkenntnissen oft ohne grossen Aufwand überlistet werden. Ein biometrischer Angriff verlangt jedoch direkt eine physische Präsenz am Ort des Detektors. Obschon dies eine beträchtliche Hürde darstellt, ist das Risiko eines erfolgreichen Angriffs auf einen biometrischen Detektor kaum kalkulierbar. Ein Ausweg aus diesem Problem sind komplexere Sensorsysteme, die gleichzeitig mehrere Merkmale erfassen, wie zum Beispiel Fingerabdruckdetektoren, die gleichzeitig auch Puls, Hautimpedanz und weitere Eigenschaften messen. Dies führt jedoch zu teuren und störanfälligen Systemen. Einfacher und naheliegend ist der hybride Ansatz mit einer Kombination von biometrischer und passwortbasierter Authentifikation. Ein doppelt erfolgreicher Angriff wird dann sehr unwahrscheinlich.

Eine grundlegende Schwäche der meisten biometrischen Sicherheitssysteme ist das Erfassungskonzept. Die biometrischen Daten der zu identifizierenden Personen werden zentral erfasst. Bei jeder Zugangskontrolle muss das System nun nicht nur entscheiden, ob die zu authentifizierende Person einer der vielen abgespeicherten biometrischen Identitäten entspricht, sondern auch noch welcher. Die Messung muss deshalb extrem präzis sein und ist natürlich anfällig auf FAR und FRR Fehler. Die geeigneten Detektoren stehen nur noch an wenigen Stellen im kontrollierten Umfeld zur Verfügung. Damit behindert das Authentifizierungssystem die heute unabdingbare Mobilität. Ausserdem schätzen es die Leute gar nicht, ihre biometrischen Daten an irgendwelche Datenbanken abzugeben.

Biometrie in einem Projekt der HTI

An der HTI wurde unter dem Namen Cod-it ein neuartiges Authentifizierungssystem entwickelt, das die obge-

nannten Probleme sehr elegant löst. Kernstück ist eine Smart-Card mit einer biometrischen Schnittstelle zum Besitzer und einer kryptographisch gesicherten optischen Schnittstelle zur digitalen Welt (Fig 4). Dank einem einfachen Challenge-Response Protokoll, das direkt über den Bildschirm auf die Karte übertragen wird, kann sich der Kartenbesitzer sofort und überall sicher ausweisen. Die biometrischen Daten sind nur noch auf der einzelnen Karte gespeichert, die beim Besitzer bleibt. Simple und robuste Authentifizierung, der Schutz sensibler persönlicher Daten und uneingeschränkte Mobilität sind dadurch gewährleistet. Das Grundkonzept hat im letzten Jahr den Venture 2002 Preis als bester Geschäftsplan gewonnen und wird nun an der HTI weiterentwickelt. Die erste auf dem Cod-it Konzept aufbauende Produktlinie ist ein universelles Zugangskontrollsystem, das mit einer einzigen Karte Eintritt in gesicherte Gebäude und Lokalitäten, Zutritt zum Intranet und insbesondere auch sicheren Remote Access zum Computer System ermöglicht. Das Produkt soll von einer Spinoff Firma auf den Markt gebracht werden. Die im Rahmen des Cod-it Projektes eingesetzten Techniken eröffnen gleich mehreren Forschungsgruppen an der HTI die Gelegenheit in das zukunftsträchtige Gebiet der Biometrie einzusteigen. •|

---

[1] *Scotland Yard nutzt Fingerabdrucke nach dem Galton Klassifikationssystem offiziell schon seit 1901*

[2] *Bereits im 19. Jahrhundert wurden die grundlegenden Fingerabdruckmuster beschrieben und klassifiziert. Das von Sir Francis Galton (Britischer Anthropologe) 1892 eingeführte Klassifizierungssystem mit ‚Minutia Punkten' ist immer noch die Basis der Fingerabdruckerkennung.*

[3] *http://europa.eu.int/scadplus/leg/de/lvb/33081.htm*

[4] *Ein japanischer Professor konnte kürzlich zeigen, dass ein Grossteil der Fingerprint-Sensoren gefälschte Finger nicht zurückweisen (False acceptance). Im Rahmen einer Diplomarbeit an der SWS werden diese Experimente verifiziert und Gegenmassnahmen für die Verbesserung der Erkennungsalgorithmen gesucht.*

[5] *Based on Dr. John Daughman's work, Cambrifge University and patented by Leonard Flom, Aran Safir, 1987*

[6] *Nebenprodukt der Augenlaserchirurgie, Dr. John Marshall, Augenarzt in London, hat Nutzung der Einzigartigkeit patentiert, das Grundpatent ist inzwischen aber abgelaufen*

Sind biometrische Daten anonym?

Dr. Thomas Probst

Thomas Probst

Dr. Thomas Probst studierte Mathematik und Physik und arbeitet beim Unabhängigen Landeszentrum für Datenschutz Schleswig-Holstein (ULD) in Kiel. Er beschäftigt sich schwerpunktmäßig mit Systemdatenschutz, der Konzeption des Datenschutz-Gütesiegels des ULD, der Erstellung von IT-Datenschutzkriterien sowie mit der sicheren und datenschutzfreundlichen Gestaltung biometrischer Verfahren. Für das ULD betreute er das Arbeitspaket Datenschutz des Projektes BioTrusT, das im Auftrag des deutschen Bundeswirtschaftsministeriums biometrische Verfahren im Bankbereich untersucht hat.

Nachdem die Biometrie in der Vergangenheit in der Forschung oder in Hochsicherheitsbereichen eher ein Schattendasein geführt hat und einem breiten Publikum allenfalls aus Spionagefilmen geläufig war, hat sie sich in den letzten Jahren durch Presse- und Filmberichte erheblich an Bekanntheit gewonnen. Der wissenschaftliche Begriff Biometrie wurde ursprünglich im Zusammenhang mit der zahlenmäßigen Beschreibung und Vermessung in der Biologie und der medizinischen Statistik verwendet. Erst in letzter Zeit wird er häufiger mit einer automatisierten Vermessung des menschlichen Körpers und einer damit möglichen automatisierten Erkennung benutzt. Solche Verfahren sind gemeint, wenn im folgenden von biometrischen Verfahren die Rede ist.

Biometrische Verfahren

Das Grundprinzip biometrischer Verfahren ist - unabhängig von den verwendeten Körpermerkmalen wie Fingerabdruck, Unterschrift, Gesicht oder Irismuster - stets gleich: Zunächst werden durch Sensoren (z.B. Kameras, Mikrofonen, Spezialsensoren zur Aufnahmen von Gerüchen oder Fingerabdrücken) die menschliche Körpercharakteristika als Referenzmuster elektronisch erfasst und gespeichert. Auf diese Weise wird die Person in das System “eingelernt”, was auch ohne deren Kenntnis geschehen kann (etwa beim “Einlernen” von latenten Fingerabdrücken, Fotos oder Videoaufnahmen als Datenquelle). Für eine Wiedererkennung werden erneut biometrische Merkmale einer Person erfasst und mit den gespeicherten

Referenzwerten verglichen. Im Falle einer Übereinstimmung ist die Erkennung erfolgreich.

Der Vergleich zwischen aktuellem und gespeichertem Merkmal erfolgt nicht anhand der Rohdaten (z.B. Ton- oder Videoaufnahme oder elektrische Impulse der Sensoren), sondern nach einem Vorverarbeitungsschritt anhand sog. Templates: Dies sind relativ kleine Datensätze, die Parameter eines mathematischen Modells der Rohdaten enthalten, beispielsweise Koordinaten von Minutien (Endpunkte und Verzweigunen) bei Fingerabdruckverfahren oder Parameter einer modellhaften Beschreibung eines Gesichts. Üblicherweise werden aus Effizienzgründen beim Einlernen nicht die Rohdaten, sondern die (bereits vorverarbeiteten) Templates gespeichert. Diese erlauben aber - im Gegensatz zu manchen Rohdaten wie etwa Gesichts- oder Stimmaufnahmen - keine unmittelbaren Rückschlüsse auf die beschriebene Person; hierzu ist vielmehr der Vergleichsalgorithmus als Hilfsmittel notwendig.

Biometrische Systeme können in zwei Betriebsarten eingesetzt werden: Verifikation und Identifikation: Bei der Verifikation wird in einem 1:1-Vergleich die behauptete Identität eines Benutzers nachgewiesen, indem die aktuell präsentierten Daten mit einem eingelernten Referenzwert verglichen werden. Die Identifikation hingegen vergleicht die aktuellen Daten mit allen gespeicherten Referenzwerten (1:n-Vergleich) und liefert als Ergebnis den "besten Treffer" oder eine Auswahl davon zurück. Identifikationsverfahren werden beispielsweise bei der Tätersuche verwendet.

Fehlentscheidungen

Bei einer mehrfachen Aufnahme biometrischer Daten einer Person sind diese nicht 100%-tig identisch. Für die Varianz sind Messfehler (etwa ein schräg aufgelegter Finger) oder Veränderungen (wie Stimmbruch, Frisuränderung, Verletzung am Finger etc.) verantwortlich. Die entsprechenden Templates sind ebenfalls nicht identisch. Beim Vergleichsprozess wird dies berücksichtigt, indem spezielle Vergleichsalgorithmen nicht auf eine absolute Übereinstimmung, sondern nur auf eine hinreichende Übereinstimmung testen. Dabei kommt es zu Fehlentscheidungen des Systems. Dies können falsche Positivmeldungen wie auch falsche Negativmeldungen sein. Mittels eines Parameters (Toleranzschwelle) wird bestimmt, ab welchem Übereinstimmungsgrad ein positives Ergebnis gemeldet wird. Die Wahl der Toleranzschwelle beeinflusst entscheidend die Qualität der biometrischen Erkennung, d.h. Art und Anteil von Falschmeldungen. Dabei lässt sich nur eine Fehlerart zu(un)gunsten der anderen optimieren; bei einer Sicherheitsanwendung (z.B. Zutrittskontrolle) muss zwischen Sicherheit (wenige falsche Positivmeldungen, dafür mehr falsche Negativmeldungen) und Bequemlichkeit (wenige falsche Negativmeldungen und mehr falsche Positivmeldungen) abgewogen werden.

Die statistische Bestimmung der Fehlerraten ist nicht einfach und hängt stark von den zugrundeliegenden Testdaten und ihrem Umfang ab, aber auch von der Testmethodik (Labortest bzw. Feldtest); je nach Wert der Toleranzschwelle liegen die Fehlerraten durchaus im einstelligen Prozentbereich.

Einsatzgebiete

Biometrische Verfahren lassen sich in ganz unterschiedliche Zusammenhängen einsetzen. In erster Linie sind es klassische Sicherheitsmechanismen wie Zugangs- oder Zutrittskontrollen, wo ein biometrischer Vergleich die Konzepte von Besitz (z.B. Chipkarte, Schlüssel) und Wissen (z.B. Passwörter oder PIN) ersetzt oder ergänzt. Ebenfalls in diesen Bereich fallen die biometrische Sicherung elektronischer Signaturen, die Anmeldung an Computersystemen oder die Aktivierung von Mobiltelefonen. Auch die Ergänzung von Ausweispapieren um biometrische Merkmale gehört dazu,

solange diese nur bei einer konkreten Kontrolle (z.B. Einreise etc.) zum Vergleich verwendet werden.

Eine andere Kategorie bilden biometrische Verfahren, die zur Identifikation eingesetzt werden, etwa bei der Zuordnung von Fingerabdrücken aus Tatortspuren zu einem bisher unbekannten Verdächtigen mit Hilfe eines zentralen Registers. Ähnliche Verfahren kommen auch bei der Registrierung von Asylbewerbern zum Einsatz und soll dazu dienen, die mehrfache Stellung eines Asylantrags unter Angabe falscher Identitätsdaten erkennbar zu machen. Dazu werden die Fingerabdrücke aller Asylbewerber in einer Datenbank gespeichert und bei einem neu gestellten Asylantrag die Fingerabdrücke des Antragstellers mit dem gesamten Bestand verglichen, um ggf. einen bereits zuvor gestellten Antrag aufzudecken. Welche Auswirkungen Fehlentscheidungen biometrischer Verfahren haben, hängt vom Einsatzumfeld, aber auch vom Umgang mit der biometrischen Entscheidung (dem "Glauben an die Technik") ab: Sie können von verspätetem Zutritt vom Arbeitsplatz, Verzögerungen bei der Flugabfertigung bis hin zur Abschiebung von Asylbewerbern reichen. Hier gilt es, verantwortungsvoll mit der neuen Technik umzugehen.

Während sich die Verfahren der ersten Kategorie sowohl als Verifikations- als auch als Identifikationsverfahren gestalten lassen, können Anwendungen der zweiten Kategorie nur als Identifikationsverfahren betrieben werden. Die Gestaltung als Verifikationsverfahren erlaubt es, die biometrischen Referenzdaten unter der Hoheit des Nutzers (etwa auf einer Chipkarte, Mobiltelefonen o.ä.) zu speichern. Dies lässt ein zusätzliches Sicherheitselement ("Besitz der Chipkarte") neben die biometrischen Daten treten und schützt diese vor unbefugter und unbemerkter Auswertung, da sie im Einflussbereich des Nutzers gespeichert werden. Weiterhin entbindet den Betreiber von der Speicherung der Daten an einer (sicherheitskritischen) zentralen Stellen. Eine Gestaltung als Verifikationsverfahren und eine Datenspeicherung unter Nutzerhoheit ist daher zu favorisieren.

Personenbezug, Anonymität und Pseudonymität

Personenbezug im datenschutzrechtlichen Sinne ist ein relativer Begriff, der vom Kontextwissen (und dem Grad der Verfügbarkeit) des Datenverarbeiters abhängt. So können Daten für einen Verarbeiter personenbezogen sein, für einen anderen nicht. Dieser Zustand kann sich im Laufe der Zeit ändern.

Unter biometrischen Rohdaten gibt es solche, die für Menschen leicht und ohne Hilfsmittel zu vergleichen sind (z.B. Stimmen oder Gesichter), und andere, bei denen dies nur mit Mühe oder gar nicht gelingt (z.B. Aufnahmen von Ohren oder Handrücken). Biometrischen Rohdaten der ersten Gruppe sind für den Menschen geeignet, ohne weitere Kenntnisse Personen wiederzuerkennen und direkt zu adressieren; sie sind daher personenbezogen. Anders ist dies bei Daten der zweiten Gruppe, denn hier müssen weitere Informationen hinzugezogen werden, um die Rohdaten einer bestimmten Person zuordnen zu können. Fehlen einem Betreiber eines biometrischen Verfahrens diese Kontextinformationen, so liegt (für ihn) kein Personenbezug vor.

Aus Templates lassen sich im Allgemeinen die Rohdaten nicht zurückgewinnen; sie sind einem Hashwert vergleichbar. Um zu ihnen einen Personenbezug herzustellen, müssen sie maschinell mit anderen Templates verglichen werden, die ihrerseits mit Hinweisen auf die Person verknüpft sind. Dazu müssen sowohl der Vergleichsalgorithmus als auch eine Sammlung von Templates mit weiteren Adressierungsinformationen (Name, Kennummer etc.) vorliegen. Das Verfahren ist mit der oben beschriebenen Identifikation zu vergleichen, die einem "unbekannten" Template diejenigen Adressie-

rungsinformationen zuweist, die mit dem besten passenden Template der Sammlung verknüpft sind. Da solche Algorithmen und Vergleichsinformationen derzeit nur sehr eingeschränkt und nicht allgemein verfügbar sind, kann man bei reinen Templates (ohne zusätzliche Daten) einen Personenbezug verneinen.

Anonymität lässt sich aus technischer Sicht als Zustand definieren, innerhalb einer Menge von Subjekten (z.B. Personen oder Kommunikationsvorgänge) nicht identifizierbar zu sein. Aus Sicht des Datenschutzes sind solche Daten anonym, die zwar Einzelangaben über eine Person sind, aber von niemandem (außer von ihr selbst) und unter keinen Umständen – mit welchem verfügbaren Kontextwissen auch immer – einer Person zugeordnet werden können ("De-anonymisierung"). Da dies nicht mit absoluter Sicherheit ausgeschlossen werden kann, muss das Risiko einer Aufdeckung betrachtet werden, das in vorhandenem oder erwerbbaren Zusatzwissen, möglichem Zeit- und Aufwandseinsatz oder neuen technischen Möglichkeiten besteht. Pragmatisch sprechen die Datenschutzgesetze von anonymen Daten, wenn die Zuordnung "nicht mehr oder nur mit einem unverhältnismäßig großen Aufwand an Zeit, Kosten und Arbeitskraft" möglich ist. Dies ist bei biometrische Daten gerade nicht der Fall: Rohdaten können personenbezogen sein, oder ein Bezug kann mehr oder weniger leicht mit Kontextwissen hergestellt werden kann; sie sind nicht anonym.

Pseudonymität lässt Personen agieren, ohne dass sie ihre Identität offen legen müssen. Sie erlaubt aber gleichzeitig eine Zurechenbarkeit. Häufig werden für die Zuordnung zwischen Person und Aktion Pseudonyme (Decknamen oder Kennummern) verwendet. Das Wissen über die Zuordnung zwischen Pseudonym und Inhaber entscheidet, ob Aktionen anonym oder identifizierbar erfolgen.

Man kann die drei folgenden Arten von Pseudonymen unterscheiden: öffentliche Pseudonyme, anfänglich nicht-öffentliche Pseudonyme, anfänglich nicht-zugeordnete Pseudonyme. Ist die Zuordnung von Inhaber und Pseudonym allgemein bekannt, so spricht man von öffentlichen Pseudonymen (z.B. Telefonnummern); der Personenbezug lässt sich sehr leicht herstellen. Bei (anfänglich) nicht-öffentlichen Pseudonymen ist die Zuordnungsregel nur (zunächst) wenigen Stellen oder Personen bekannt (z.B. Personalnummer, Kontonummer, Sozialversicherungsnummer); vom Schutz der Zuordnungsregel hängt ab, ob und wie leicht ein Personenbezug hergestellt werden kann. Eine Änderung des Pseudonyms ist häufig prinzipiell möglich, liegt aber nicht immer im Einflussbereich des Inhabers (etwa bei der Sozialversicherungsnummer). Schließlich spricht man von anfänglich nicht-zugeordneten Pseudonymen (manchmal auch von anonymen Pseudonymen), wenn die Zuordnung anfänglich allen Parteien (ggf. mit Ausnahme des Inhabers) unbekannt ist (z.B. bei selbstgewählten Pseudonymen oder automatisch generierten Pseudonymen).

Pseudonyme Daten sind solche personenbeziehbaren Daten, die mit Hilfe eines Pseudonyms oder Zuordnungsregel einer bestimmten Person zugeordnet werden können. Je nachdem, ob dem Datenverarbeiter diese Regel bekannt ist oder nicht, handelt es sich für ihn um personenbezogenen Daten oder nicht. Mit der Verfügbarkeit dieser Regel lässt sich also der Personenbezug steuern. Pseudonyme können im Laufe der Zeit ihren Charakter ändern. Ein Beispiel ist die Telefonnummer einer Person: Während es vor etwa 20 Jahren für eine Privatperson nahezu unmöglich gewesen sein dürfte, zu einer gegebenen Anschlussnummer den Teilnehmernamen zu ermitteln (ohne einen Anruf bei der entsprechenden Nummer zu tätigen), ist dies im Zeitalter von PC, Telefonnummersammlungen auf CD-ROM und der Möglichkeit zur Inverssuche kein Problem mehr. Aus einem

anfänglich nicht-öffentlichen Pseudonym ist ein öffentliches Pseudonym geworden.

Mit Verkettung wird die Zusammenführung von Daten oder Informationen bezeichnet, die häufig mittels identifizierender Merkmale oder Pseudonyme geschieht. Ein Beispiel ist der Abgleich verschiedener Erkrankungen eines Patienten mit Hilfe eines Pseudonyms zu Forschungszwecken oder die Erstellung von Nutzungsprofilen von Internet-Surfern anhand der IP-Nummern.

Biometrische Daten als Pseudonyme

Biometrische Rohdaten können personenbezogen sein und sind nicht anonym im Sinne der Datenschutzgesetze. Die berechneten Templates weisen selbst keinen Personenbezug auf, solange sie nicht mit anderen Daten verknüpft sind. Sie können aber eine solche Verknüpfung leisten und daher als (anfänglich nicht-öffentliche) Pseudonyme wirken.

Biometrische Verfahren können in vielen Zusammenhängen eingesetzt werden. Derzeit gibt es viele unterschiedliche Verfahren am Markt. Die zu einem biometrischen Rohdatum erzeugten Templates verschiedener Verfahren sind im allgemeinen nicht untereinander vergleichbar; die unterschiedlichen Verfahren generieren derzeit für einen Benutzer verschiedene Pseudonyme. Kommen hingegen – etwa aufgrund von künftigen Standardisierungen – immer dieselben technischen Verfahren zum Einsatz, so werden für eine Person stets Templates gleicher Struktur erzeugt und gespeichert. Das biometrische Pseudonym und häufig auch die Zuordnung zur Personen werden mit der Zeit einem immer größer werdenden Kreis bekannt, weil sie in immer mehr Systemen gespeichert werden. Auch ein Austausch von Rohdaten oder Templates (incl. der zugehörigen Personenidentität) zwischen verschiedenen Betreibern biometrischer Verfahren wird um so interessanter, je universeller die Daten verarbeitet werden können. Die Templates werden auf diese Weise – gewollt oder ungewollt – zu öffentlichen Pseudonymen.

Wenn aber praktisch jedermann über das Pseudonym und seine Zuordnung zur Person verfügt oder verfügen kann, wirken diese als universelles Personenkennzeichen, machen Daten personenbeziehbar und erlauben eine Verkettung von personenbezogenen Daten. Daher liegt in der unkontrollierten Anwendung biometrischer Verfahren eine besondere Brisanz, insbesondere in einer unbemerkten Nutzung wie etwa der Anbindung an Videoüberwachungssysteme, gegen die man sich de facto nicht wehren kann und die auch unbemerkt erfolgen kann. Denn während sich übliche Pseudonyme ändern lassen und daher eine Verkettung erschweren oder unmöglich machen, sind biometrische Rohdaten dauerhaft personengebunden und daher bei einer Kompromittierung "verbraucht". Eine Änderung der Pseudonyme könnte allenfalls durch Verwendung anderer biometrischer Verfahren mit anderen Templatestrukturen vorgenommen werden.

Auswege aus dem Dilemma?

Daher ist es sinnvoll, biometrische Pseudonyme nicht unmittelbar einzusetzen, sondern mittels kryptographischer Techniken abzusichern und nur indirekt zu verwenden. Die Idee bei sogenannten "templatefreien Verfahren" ist, in einem zweistufigen Prozess zur Pseudonymisierung unkritische (Transaktions-)Pseudonyme zu verwenden und die Zuordnung dieser zum Inhaber durch ein "biometrisches Pseudonym" vorzunehmen. Bei Verwendung geeigneter kryptographischer Verfahren kann man dann zwei Transaktionspseudonymen nicht ansehen, ob sie einer oder zwei verschiedenen Personen zugeordnet sind; eine unbefugte Verkettung ist mit ihnen nicht möglich.
Solche templatefreien Verfahren stehen aber erst am Anfang der technischen Entwicklung, denn die Proble-

matik der Varianz biometrischer Rohdaten, der man in den üblichen Verfahren durch Konstruktion des Vergleichsalgorithmus und der Festlegung der Toleranzschwelle begegnet, muss hier in die Konstruktion eines eindeutigen kryptographischen Schlüssels verlagert werden. So müssen die unterschiedlichen Rohdaten, die bei Aufnahmen desselben biometrischen Merkmals gemessen werden, stets zu demselben biometrischen Schlüssel führen; Merkmale unterschiedlicher Personen müssen hingegen verschiedene Schlüssel ergeben. Mit dem Schlüssel wird dann eine Zufallszahl verschlüsselt. Das Klartext-Chiffrat-Paar (bestehend aus Zufallszahl und Verschlüsselungsergebnis) bildet ein Transaktionspseudonym und ist an den Inhaber gebunden, denn nur sein biometrischer Schlüssel "passt". Es erlaubt aber bei Verwendung geeigneter kryptographischer Techniken keine Rückschlüsse auf diesen Schlüssel und daher auch nicht auf die biometrischen Merkmalen.

Fazit

Biometrische Daten sind dauerhaft personengebunden und daher besonders schützenswert. Wenn immer möglich, sollten sie im Einflussbereich der Nutzer gespeichert werden. Bei der Gestaltung biometrischer Verfahren ist auf eine hohe Systemsicherheit zu achten, um die biometrische Daten zu schützen. Umgekehrt können biometrischen Verfahren dazu beitragen, Werte und Daten effektiv zu schützen - dies macht . Templatefreie Verfahren sind aus Sicht des Datenschutzes zu bevorzugen, da mit ihnen die Gebote der Datensparsamkeit und Datenvermeidung erfüllt werden können. •|

Literatur:

Behrens, Michael/Roth, Richard (Hrsg.): Biometrische Identifikation, Braunschweig/Wiesbaden 2001.

Hansen, Marit: Privacy Enhancing Technologies, in: Roßnagel (Hrsg): Handbuch Datenschutzrecht, München 2003.

Probst, Thomas: Anonymität und Pseudonymität bei biometrischen Identifikationsverfahren, in: Bäumler/von Mutius (Hrsg.): Anonymität im Internet. Grundlagen, Methoden und Tools zur Realisierung eines Grundrechts. Braunschweig/Wiesbaden 2003.

DRIVE- Drug In Virtual Enterprise

Alberto Sanna
with Daniela Cipriano, Sandro Buso, Marc Wilikens

Alberto Sanna was born on May 10, 1962.

Alberto Sanna got his Nuclear Engineering degree at Politecnico di Milano in 1991.
He is involved in healthcare process re-engineering projects at Scientific Institute H San Raffaele (HSR) since 1989, when he joined for completing his degree thesis on automation in production of radiopharmaceuticals in the Nuclear Medicine department.

In 1991, after the degree thesis, he was in charge of automation projects in the Nuclear Chemistry and Laboratory Medicine departments. The projects included designing and realizing robotic workcells that would be used in Patient/Operator safety and/or high throughput critical processes.

From 1992 to 1996, he was assigned to the Information Technology department, where his robotics experience was merged with process analysis and Information System analysis, design and implementation.

From 1996 to present, he has been in charge of Laboratory Information System and Process Technologies and in charge of The Healtech Group. The Healtech group is a team of engineers aimed at developing and engineering safe, secure and effective health process models and systems within the more general framework of a Patient-centric hospital re-engineering process. In particular, he is presently in charge of inter-service (Laboratory and Pharmacy) process integration projects, inter-hospital (Laboratory/Pharmacy and Clinical Ward) process integration projects, hospital-territory integration projects (laboratory report delivery in territory, on top of public internet infrastructures) and disease management decision support system.

Since June 2000, he holds the position as project manager of the European R&D project DRIVE: Drug in virtual enterprises, that is dedicated to the realization of a vertical integration in the pharmaceutical supply chain from manufacturers to bedside, on top of the e-commerce infrastructures.

Since 1996 he is an active expert in the European Standardization Body CEN TC 251 Health Informatics WGIII - Safety Security and Quality, in which he is the project leader of the SAFE-ID work item “Safety procedures of identification of Patients and related objects”, approved September 19, 2000. He is active in other international scientific associations and in ISO TC 215 Health Informatics WGIV on Security.

He is active in publishing/presenting activities in more than 50 national and international congresses on automation, information technology and e-commerce topics in healthcare and he is co-inventor in two patents aimed at healthcare process innovations.

He has recently been appointed as a Professor of Dependability of Information Systems by the University of Milan, Department of Information Science.

In the dynamic healthcare environment, laboratory diagnostics and pharmaceutical therapy are the medical events with the highest occurrence rate, for both in-Patients and out-Patients. The convergence of these disciplines in a unique info-knowledge infrastructure is the unique intervention point with the highest impact potential in the healthcare domain, particularly within the hospital environment in which the highest frequency of such events occurs. The DRIVE project aims at providing a fully integrated info-knowledge environment on top of an integrated product supply chain (based on the concepts and business models of the e-Commerce) infrastructure and a safe and secure data infrastructure (based on the concepts of trust and dependability) among stakeholders to drive the laboratory diagnostics and the pharmaceutical therapy (and further medical disciplines) convergence within the hospital environment.

Introduction

The healthcare sector is the largest single service sector, accounting for approximately 650 billion Euro in the European Union (approximately 9% of the GDP). A remarkable and unique feature of this market is represented by the relevant social and political attention it arouses, which is an obvious consequence of their mission to protect the health of millions of Citizens.

The health sector has scope for major reforms of its working practices through the adoption of distributed IT products and services. Notwithstanding local differences in Health Care organization and management in the EU, the technological challenges and approaches are becoming increasingly homogeneous due to:

- The universality of health care delivery and its knowledge intensive nature, which require global interoperable technological solutions;
- Increased mobility of Citizens and increased need for universal accessibility of electronic patient data;
- EU-wide legal and regulatory frameworks such as those related to Privacy protection;
- Globalization of business services and supply chains

Healthcare enterprises (HCE) are facing strong economical and social pressures. Particularly in the EU, cost containment pressure and the need to balance social impacts forces healthcare systems within a context of finite resources and quality improvement. This evolution in turn, drives healthcare enterprises towards optimization of their use of resources, in their internal business processes and in their business partnerships. Information infrastructures now offer opportunities for this optimization and for the integration on a wider scale of other business processes involved in healthcare delivery (e.g. pharmaceutical and medical device industries,

healthcare service suppliers, insurance and government administrations, etc.) giving place to virtual enterprises.

From recent studies[1], Adverse Drug Events are clinical events suffered by patients as a result of inappropriate drug therapy management and have been identified as the single major cause (19%) of medication errors in hospitals. Examples of medication errors are, among the others, wrong drug (administration of a drug which was not that prescribed), wrong dose (administration of an amount of drug greater or less than that prescribed) and expired drug (administration of a drug that has deteriorated due to incorrect ward storage or has exceeded its expiration date). Other medication errors can originate from logistic inefficiencies of the drug distribution system: delays on ordering medication from the pharmacy department, failures to locate medication that was in the ward, etc. Statistics collected on real cases have demonstrated that Adverse Drug Events can double the death risk for patients[2].

The drug delivery system in large HCE's such as hospitals is by far the single intervention point with the highest potential for cost savings and quality improvement, affecting Patient quality of life and safety. Therefore, the ***Drug in Virtual Enterprise (DRIVE)*** project will be applied and piloted on the drug processes of an integrated clinical and logistic drug supply chain.

The DRIVE project is set to apply Trust services from a well-suited Trust Infrastructure, through the use of strong authentication and identification techniques, to business processes in order to allow them to exhibit important features in the dimensions of safety, security, protection, integrity. These processes can be referred as Electronic-enable processes, or, shortly, E-processes. To this aim, the DRIVE project, has been approved within the 5th Framework Program – Information Society Technologies programme. The participants to this project are the following:

- Istituto Scientifico Università San Raffaele, Milano
- Aurion Produktions und Handels, Austria
- Karolinska Institutet, Sweden
- AtosOrigin Integration, France
- AstraZeneca, Italy
- GlaxoSmithKline, Italy
- Joint Research Centre , EU
- Politecnico di Milano, Italy

E-processes will be then applied to integrate work and business practices among different enterprises, by means of innovative processes that extend traditional enterprise boundaries and that embrace consumers and suppliers in a tight relationship.

Given that safety and supply chain integration are worth significant values in the healthcare drug market, the objective of the DRIVE project is to deliver dedicated information services among key value-makers, i.e. drug manufacturers, drug distributors, and hospitals (including drug related hospital sub-processes from pharmacy to bedside). Such innovative and added value services will be traded and delivered on top of e-commerce infrastructures on a "pay per use" basis. In the European public healthcare system, such added value services will produce significant advantages to the European Citizen, both the Patient and Taxpayer.

Technology description

General

In order to produce safety and supply chain integration values in the drug process from drug manufacturer to bedside, the DRIVE information management infrastructure will deliver end-to-end services aimed at:

- Real time knowledge and information sharing
- Dependability in information flow

- Accountability tracking in knowledge and information flow
- Performance evaluation in quality enhanced business processes
- Patient information privacy protection

The DRIVE information system automates the continuous cycle of supply procurement and usage throughout the Virtual Enterprise (VE) covering, with the following functionalities, the whole drug process (see figure 1):

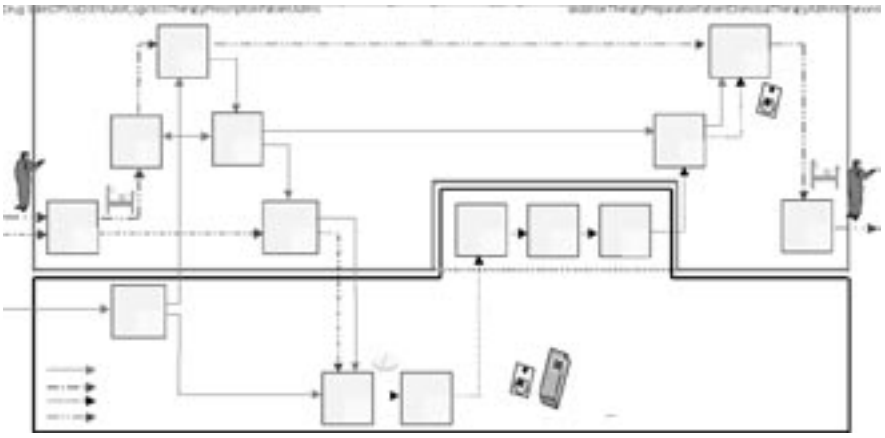


Figure 1 - Printing area illustration

- ***Patient Identification***: the patient is the most important business actor within the VE. For this reason, he/she must always be identifiable by the system. The patient is equipped with a wristband, containing a 2D code, from the time of admission into the Hospital until he/she is dismissed. All business processes that involve the Patient (i.e. Therapy administration) include Patient 2D code reading.
- ***Therapy management***: online therapy prescription, preparation, and administration.
- ***Supply Request***: including online requisition generation and validation.
- ***Ordering***: generating a purchase order and Web-based transmission to vendor.
- ***Receiving***: generating a receipt and tracking.
- ***Distribution***: tracking where and when supplies are dispersed throughout the organization.
- ***Usage***: including usage tracking and eventually charging of supplies to patient accounts.
- ***Invoice***: invoice tracking and Web transmission of invoice.
- ***Inventory management***: support for par-level inventory and automatic replenishment suggestions when supplies drop to user-defined levels.
- ***Vendor database***: online vendor supply catalogs with price list update.
- ***Management reporting***

The DRIVE information systems are strongly based on Internet/Intranet connectivity that is essential to the implementation of a distributed supply chain solution.

The aims of DRIVE is not to substitute Enterprise Resource Planning (ERP) already present in Hospital, but integrate them with DRIVE information systems in order to provide a full function SCM system strongly integrated with Clinical Management system.

DRIVE Information Systems

Collaborative Logistics mainly consists of three main modules. The connectivity module enables the computer system in one organization (i.e. Drug Supplier) to communicate with another (i.e. Hospital) organization's system directly. By means of Internet connection, the most important electronic transaction can be exchanged: Purchase Order, Advanced Shipping Note, and Invoice. Moreover the connectivity allows each business partner to share information such as, stock levels, price list, etc. The replenishment module gives the up-to-date replenishment suggestions to the manager of the Pharmacy in order to refill the Warehouse in the most efficient way including forecasting of required drugs, based on recorded usage. The Collaborative Logistics can be integrated with Hospital and Supplier ERP Systems in order to exchange electronic transactions and get stock levels for replenishment. The Collaborative Logistics System is able to act as a broker in a many (Supplier) to many (Hospital) model. The Intelligence module provides a flexible reporting tool.

Hospital Logistics include all the Material Management functionality that covers the drug process inside the Hospital. The Hospital Logistics is based on the drug bar code label that, at the moment, is not enough to satisfy all the tracking requirements; for this reason, DRIVE includes the possibility to re-label drugs with a new bar code label that also include expiration date and lot code. Hospital Logistics include the usage of Hand-held PCs, as well as bar code scanners, to provide the means for tracking the drugs movement inside the Hospital and check that the operator handles the correct drug.

Hospital Logistics provides three main modules. A complete Warehouse Management for the Pharmacy Warehouse and Wards Warehouse including the interface with Smart Cabinets that, by means of indicators, actuators and controllers guide the operator during the picking process. The Warehouse Management is integrated with the ERP System in order to align it to the stock consumption. Supply Request management gives to the Hospital Ward an instrument to activate a fast replenishment of ward warehouse based on therapy requisitioning, and inventory. The Intelligence module provides a flexible reporting tool. Hospital Logistics System is based on Internet technology in order to be able to support future scenarios where there can be more that one Centralized Pharmacy that supplies more than one Hospital Wards.

Clinical Management is based on the Smart Cart (see figure 2)/Smart Bed systems that provide operators a mobile workstation (mounted on the cart) or a fixed workstation to the bed side that allow access to information at the point of use. Smart Cart/Smart Bed systems are equipped with bar code scanners, to provide the means for tracking the drugs preparation/administration and check the Patient identity. The Therapy Prescription, Therapy Preparation, Therapy Administration and Clinical Record management functions give to the operator a support for all the Clinical process phases.

Trust Infrastructure provides a safe

Fig. 2 - A possible Smart Cart design

infrastructure that guarantees: the certified access to the system, by means of smart cards; protection of the private data; the encryption/decryption of the data exchanged on the public Internet; the electronic signature of the most important transaction (i.e. Therapy prescription/preparation/administration).

Performance Evaluation provides

an electronic control panel of the VE based on data collected by Collaborative Logistics, Hospital Logistics and Clinical Management DRIVE modules. The control panel provides a hierarchy of indicators for monitoring the system performance. The set of indicators at the same level of the hierarchy represents exhaustively the status of the system at a certain time period. In such a way it is possible for the managers executing the control to have a complete vision of the system at different levels of detail. The set of indicators measures the system performance by considering different aspects such as costs, safety of patients, service level and efficiency of the process. High detailed indicators measure the performance of a particular activity along the process of the drug distribution in healthcare systems; detailed indicators are obviously very focused and restricted. Low detailed indicators are more aggregate than the previous and less focused on the activities.

Conclusion

In conclusion, the objective of the DRIVE project is to provide the information infrastructure to allow enterprises to run E-processes, i.e. processes made safe and secure through the use of an appropriate IT Infrastructure. In particular the project applies the E-process concept in the establishment of a virtual enterprise among main value makers in the drug market (drug manufacturers, distributors and hospitals). Such a virtual enterprise will jointly produce value in a safe and secure framework by means of real time information and knowledge sharing in the overall process, within a quality business process on top of a trust infrastructure. Value produced in such an E-process will be shared in a business-to-business context on top of E-commerce infrastructures. The achievements the DRIVE Pilot will be able to demonstrate can be easily applied Europe-wide and the whole European Healthcare sector can immediately benefit from the results of the project. Finally, it should be noted that the DRIVE Project has the potential to give rise to standardization recommendations at European and International level in the field of "Safety & Security in Healthcare". •|

Alberto Sanna	sanna.alberto@hsr.it	Istituto ScientificoUniversità San Raffaele
Daniela Cipriano	cipriano.daniela@hsr.it	Istituto ScientificoUniversità San Raffaele
Sandro Buso	sbuso@atos-group.com	AtosOrigin Integration
Marc Wilikens	marc.wilikens@jrc.it	The Joint Research Centre, EU

1. *Leape Ll, Brennan Ta, Cullen Dj: The Nature Of Adverse Events In Hospitalized Patients. Results Of The Harvard Medical Practice Study Ii – N Engl J Med 1991; 324:377-84.*

2. *Classen C. et al.: JAMA, Jan 22/29, 1997 – Vol. 277, No. 4: 301-306.*

C'est ça (aussi) la télévision

Tania Chytil

Tania Chytil est née à Porrentruy le 3 janvier 1970. Elle a fait ses classes dans cette ville. Après avoir obtenu sa maturité fédérale en 1988, elle a quitté la Suisse pour Londres et New York.

De retour au pays, elle a réussi en 1994 sa licence en droit à l'Université de Lausanne où elle a occupé ensuite un poste d'assistante.

Tania Chytil est devenue présentatrice à l'émission « Magellan » en janvier 1995. En août de la même année, elle a présenté l'émission de la grille d'été « Fous de pub » avant de collaborer, dès novembre 1995, à l'émission « Vérité, Vérités ».

Elle termine sa formation de JRI en avril 2000 et travaille à Vaud-Régions. Puis elle présente le 19 h : 00 des Régions d'août 2001 à août 2002. Depuis août 2002, journaliste et co-présentatrice, avec Phil Mundwiller, de Territoires 21, la nouvelle émission scientifique de la TSR.

C'est l'histoire d'un reportage. "Au doigt et à l'œil". Un reportage réalisé pour "Territoires 21", l'émission scientifique de la télévision suisse romande. Il a été imaginé en août, réalisé en septembre et diffusé en octobre. De la même année, rassurez-vous. 2002. Le sujet était dans l'air du temps. Des articles paraissant par-ci par-là sur ces nouvelles technologies. Et puis Steven Spielberg sortait "Minority Report". Il fallait aller voir de plus près.

C'est ce que nous avons fait.

Première et indispensable étape en ces temps avancés : surfer sur le net. Les sites étaient abondants. Parfois intéressants. Puis, appel à la documentation écrite de la TSR, le service qui, auparavant, découpait et classait les articles de journaux. Aujourd'hui, avouons-le, ils découpent un peu moins, informatique oblige. De lectures en coups de fil, de spécialistes en experts, j'ai peu à peu fait connaissance avec dame "biométrie", compris ce que cela regroupait, à quoi cela servait, ce qu'on pouvait en faire et où cela nous menait.

De son côté, le réalisateur du reportage avait fait beaucoup de recherches aussi (dans les reportages "magazines" de la TSR, journaliste et réalisateur travaillent ensemble ; l'un s'occupe un peu plus du fond, l'autre de la forme. En bout de course, chacun met son grain de sel dans la partie de l'autre, forcément. Heureusement.) Il avait trouvé plusieurs entreprises qui utilisent la biométrie, qui fabriquent des appareils de mesures.

Nous avions deux semaines pour préparer ce reportage. Deux semaines pour trouver les contacts, voir les gens, prendre rendez-vous. Plus le temps avançait, plus nous nous rendions compte que les personnes incontournables se trouvaient… aux Etats-Unis. Une société fabrique des scanners à main dans la Silicone Valley. L'aéroport de San Francisco utilise justement ces scanners, depuis des années, pour sécuriser l'accès au tarmac. Les dates de tournage étaient fixées d'avance. Du 9 au 13 septembre 2002. Entre les deux, il y a quoi ? Je vous le donne en mille: le 11. Et que croyez-vous que le service de presse d'un aéroport américain vous répond quand vous lui demandez s'il serait par hasard possible de venir filmer ses installations de sécurité un 11 septembre ? Juste. Il n'est pas enchanté-enchanté. Mais par contre, pas de problème pour trouver des vols de libre. Personne ne veut voyager à une telle date. Résultat des courses : on modifie les dates de tournages et du coup celle de montage (ce qui n'est pas évident lorsqu'on connaît le merveilleux monde fantastique de la télévision).

A l'entreprise précitée et à l'aéroport (tout autant précité) venaient s'ajouter le 1er supermarché des Etats-Unis qui utilise les empreintes digitales comme moyen de paiement et l'aéroport d'Amsterdam qui a misé, lui, sur l'iris pour faire passer la douane sans passeport aux "frequent flyers". Plus un expert qui prenait de la distance par rapport à tout cela et qui parlait des avantages, des inconvénients et des dérives de la biométrie.

Mais que faire de la reconnaissance faciale ? De "l'Affaire du Super Bowl" (où les spectateurs avaient été examinés à la loupe puisque les autorités policières de Floride avaient un système de vidéo surveillance capable de reconnaître les délinquants et criminels) ? De "l'essai" de l'aéroport de Kloten (l'office des réfugiés et la police zurichoise se sont offerts un système de caméra vidéo qui "photographie" les visages des passagers "suspects" lors de leur arrivée sur sol helvétique) ? Et que faire des prélèvements ADN ?

Par manque d'image (eh oui, la télévision a vraiment ses limites…), nous n'avons pu qu'évoquer ces problèmes. Mais pas les montrer.

Nous avions 5 jours de tournage prévus, pas un de plus, voyage compris, pour boucler le tout. C'est court (pour ceux qui ne s'en seraient pas rendu compte). Le spécialiste se trouvait en Suisse. Le supermarché à Seattle. L'entreprise dans la Silicone Valley. Le premier aéroport à San Francisco. L'autre à Amsterdam. Nous avons volé, couru, dormi dans l'avion, tourné quelques minutes après en être descendus (de l'avion), loué des voitures ENORMES (plus hautes et grandes encore que ce qu'on pouvait imaginer), ri, mangé merveilleusement bien entre Seattle et San Francisco (ce genre de détail est important et véridique). Et surtout eu beaucoup de plaisir entre caméraman, preneur de son, réalisateur et journaliste.

Au retour, huit jours de montage, à Genève. Des jours angoissants pour une jeune journaliste dont c'était le premier "long" reportage.

Je vous vois venir avec vos âmes de scientifiques. Vous faites le calcul. Vous comptez le nombre de personnes qui ont travaillé sur ce reportage de 15 misérables minutes pour expliquer aux téléspectateurs les tenants et aboutissants de la biométrie. Il y a l'équipe de base (dont je viens de vous parler). Ça fait quatre. Ajoutez un monteur, une illustratrice sonore, une personne qui a fait tous les traitements d'images, quatre personnes qui ont doublé les intervenants parlant anglais, deux producteurs (qui n'ont que regardé le reportage et soutenu le moral des troupes, je vous l'accorde), un directeur de la TSR (qui l'a financé, ce reportage). Ca fait 14. Et j'en oublie. Mais ça fait déjà beaucoup.
C'est quand-même un sport de riches, la télévision. •|