Zeitschrift für Datenrecht und Informationssicherheit

digma

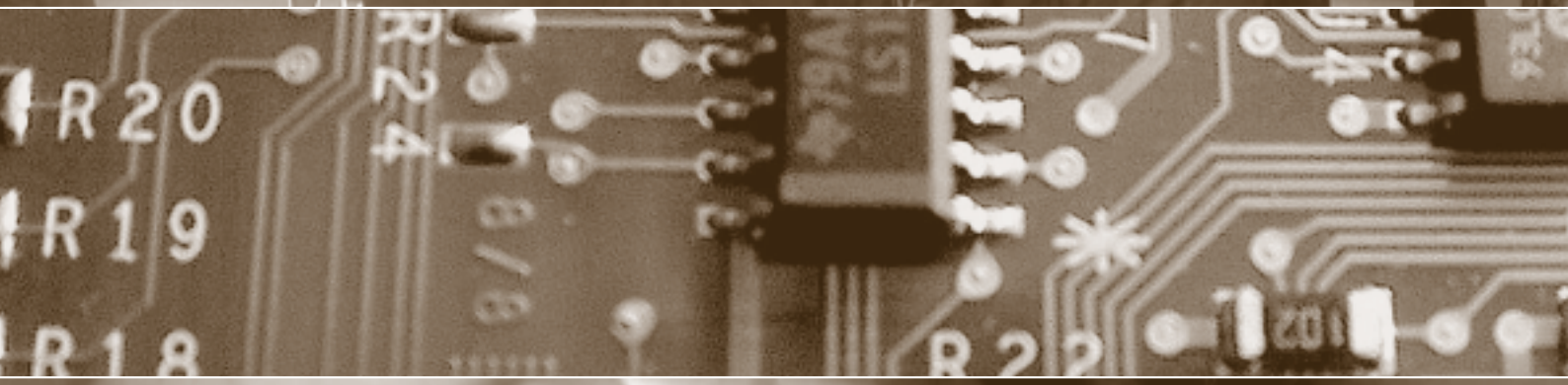
www.digma.info 6. Jahrgang, Heft 3, September 2006

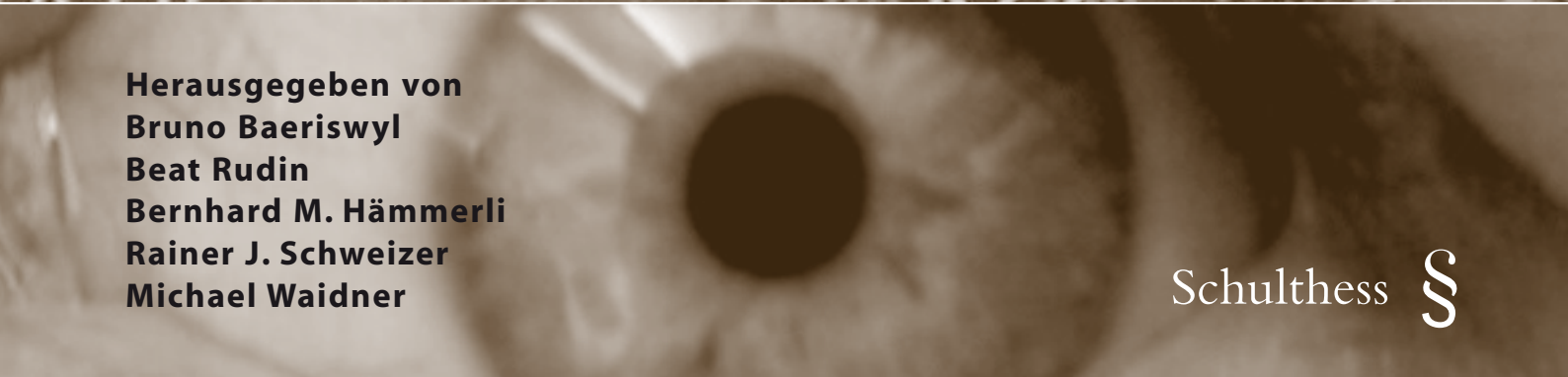
Spezialausgabe zum elften Symposium on Privacy and Security

Schwerpunkt:

Pervasive Computing

fokus: Risiko-Dialog zu Pervasive Computing
report: Ein Grundrecht auf Sicherheit?
report: Sichere Internet-Telefonie (VoIP)?





Herausgegeben von
Bruno Baeriswyl
Beat Rudin
Bernhard M. Hämmerli
Rainer J. Schweizer
Michael Waidner

Schulthess §

inhalt

fokus

Schwerpunkt:
Pervasive Computing

Wer macht was mit meinen Daten?

Der Direktor des IBM-Forschungslabors in Rüschlikon fordert, dass wir uns als Gesellschaft sehr viel stärker damit auseinandersetzen, was mit unserer Privatheit passiert, wenn wirtschaftliche Umschichtungen stattfinden oder die Technologie rasante Fortschritte erzielt.

Pervasive Computing im Alltag

Mit welchen konkreten Anwendungen ist in Zukunft zu rechnen? Viele Anwendungen, die heute noch im Ideen- oder Prototypenstadium sind, lassen erahnen, wie Pervasive Computing unseren Alltag verändern wird. Der Autor, der selber an der ETH an Prototypen arbeitet, gibt einen Überblick.

PvC und Informationssicherheit

Pervasive Sicherheit unterscheidet sich in manchen Aspekten von der IT-Sicherheitsproblematik in Computernetzen. Deshalb sind viele Lösungen nur beschränkt übertragbar. Verlangt sind Lösungen, welche die besonderen Rahmenbedingungen berücksichtigen.

Risiko-Dialog zu Pervasive Computing

Wie können künftige Informations- und Kommunikationstechnologien verantwortungsvoll eingesetzt werden? Darüber haben in einem schweizerischen Dialog rund 45 Personen aus Wirtschaft, Wissenschaft, Behörden, Patienten-, Konsumenten-, Datenschutz- sowie Umweltorganisationen diskutiert.

impressum

digma: Zeitschrift für Datenrecht und Informationssicherheit, ISSN: 13239944, Website: www.digma.info

Herausgeber: Dr. iur. Bruno Baeriswyl, Dr. iur. Beat Rudin, Prof. Dr. Bernhard M. Hämmerli, Prof. Dr. iur. Rainer, J. Schweizer, Dr. Michael Waidner

Redaktion: Dr. iur. Bruno Baeriswyl und Dr. iur. Beat Rudin

Rubrikenredaktor: Dr. iur. Amédéo Wermelinger

Zustelladresse: Redaktion digma, c/o Stiftung für Datenschutz und Informationssicherheit, Kirschgartenstrasse 7, CH-4010 Basel
Tel. +41 (0)61 270 17 70, redaktion@digma.info

Erscheinungsplan: jeweils im März, Juni, September und Dezember

Abonnementspreise: Jahresabo Schweiz: CHF 158.00, Jahresabo Ausland: Euro 123.00 (inkl. Versandspesen), Einzelheft: CHF 42.00

Anzeigenmarketing: Schulthess Druck AG, Doris Affolter, Arbenzstrasse 20, Postfach, CH-8034 Zürich
Tel. +41 (0)44 386 40 85, Fax +41 (0)44 383 79 45, doris.affolter@schulthess.com

Druck: Schulthess Druck AG, Arbenzstrasse 20, Postfach, CH-8034 Zürich, ISDN +41 (0)44 380 18 86

Verlag und Abonnementsverwaltung: Schulthess Juristische Medien AG, Zwingliplatz 2, Postfach, CH-8022 Zürich
Tel. +41 (0)44 200 29 99, Fax +41 (0)44 200 29 98, www.schulthess.com, zs.verlag@schulthess.com

Ein Grundrecht auf Sicherheit?

Politik und Teile der Rechtswissenschaft haben in jüngerer Vergangenheit ein Grundrecht auf Sicherheit postuliert. Die frühere deutsche Bundesjustizministerin sieht darin eine Verkehrung der Funktion der Grundrechte als Schutz vor einem überbordenden Staat in ihr Gegenteil.

Qui a volé le mascotte du gardien?

Im Nachgang zur digma-Nummer zu Hooliganismus liefert der Autor Erkenntnisse über den Hooliganismus aus einer Studie zu «Le stade de football: lieu de ralliement, de recrutement et de sociabilité de la droite extrême».

Keine Frist für den Anspruch auf Berichtigung

Das Bundesgericht hatte sich im März 2006 mit der Frage zu befassen, ob die betroffene Person ihren Anspruch auf Berichtigung oder Vernichtung unrichtiger Personendaten jederzeit – also ohne zeitliche Befristung – geltend machen kann.

Privatrechtlicher Datenschutz

Die Habilitation von Regine E. Aebi-Müller nimmt die theoretische Verankerung des privatrechtlichen Datenschutzes unter die wissenschaftliche Lupe.

Die Schengen/ Dublin-Anforderungen

Mit der Assoziierung der Schweiz an Schengen/Dublin werden für Bund und Kantone die EU-Datenschutz-Anforderungen verbindlich. Die Vereinigung der schweizerischen Datenschutzbeauftragten unterstützt aktiv die Umsetzung in den Kantonen.

report

forum

Brückenschlag

Sichere Internet-Telefonie (VoIP)?

Prof. Dr. Andreas Steffen, ITA-HSR, Rapperswil
andreas.steffen@hsr.ch

«Voice over IP» (VoIP), d. h. die digitale Übertragung von Sprache eingebettet in IP-Datenpakete, ersetzt zunehmend die herkömmliche Telefonie. Viele Firmen, bei denen der Ersatz der Haustelefonzentrale ansteht, entscheiden sich aus Kosten- und/oder Flexibilitätsgründen für eine VoIP-Lösung. Und Millionen von Privatpersonen und Kleinfirmen benützen Skype und Co., um zum Nulltarif weltweit über das Internet zu kommunizieren. Bei aller Begeisterung für die innovativen Möglichkeiten, die sich mit dieser neuen Technologie ergeben, sowie den Gesprächsgebühren, die gespart werden können, gehen die Sicherheitsaspekte meist völlig vergessen. Dieser Artikel soll aufzeigen, wie verletzlich die Übertragung via IP ist, will aber auch auf wirksame Schutzmassnahmen hinweisen, die ergriffen werden können.

Vertraulichkeit von VoIP-Gesprächen

Frage: Traditionell können Telefongespräche entweder mittels Krokodilklemmen am Hausverteilerkasten oder via Softwareschalter in der Telefonzentrale angezapft werden. Damit dies möglich wird, sind aber einige physische oder juristische Hürden zu überwinden. Wie steht es hier mit der Internet-Telefonie?

Antwort: Da im Netz Audio- und Video-Pakete gleich wie alle anderen IP-Pakete behandelt werden, können sämtliche Hilfsmittel, die zur Überwachung des Datenverkehrs zur Verfügung stehen, auch zum Abfangen von Multimediaströmen eingesetzt werden. Besonders einfach ist dies im lokalen Netz (LAN) einer Firma oder Schule möglich. Die Palette der frei verfügbaren Tools reicht vom professionellen Netzwerkanalyseprogramm Ethereal (www.ethereal.com) bis zur kinderleicht zu bedienenden Hackersoftware Cain & Abel (www.oxid.it), die automatisch jeden VoIP-Verbindungsaufbau erkennt und die Gespräche in direkt abspielbaren Audio-Dateien ablegt.

Einen gewissen Schutz vor dem unkontrollierten «Schnüffeln» im internen Netz bietet das Aufsetzen eines Virtuellen LANs (VLAN), in das alle IP-fähigen Telefonapparate eingebunden werden. Diese Abschottungsmassnahme wird aber aufgeweicht, sobald auch mit PC-basierten «Software Phones» telefoniert wird, da die PCs eben auch zum Surfen im Internet verwendet werden und damit im normalen Datennetz der Firma angesiedelt werden müssen, wo sie wieder einfach abgehört werden können.

Etwas anders ist die Situation beim globalen Telefonieren im Internet. Hier kann nur in den durch die Netzwerkbetreiber verwalteten Internetknoten (Router) auf die sich im Transit befindenden Sprachpakete zugriffen werden. Das Abhören ist damit normalerweise den Strafverfolgungsbehörden und den nationalen Geheimdiensten vorbehalten. In Ländern mit hoher Korruptionsrate könnten aber auch kriminelle Organisationen oder Privatpersonen mit genügend Finanzkraft Zugriff auf das Netz erhalten.

Frage: Können VoIP-Gespräche durch Verschlüsselung vor dem unberechtigten Mithören geschützt werden, um so z. B. Industriespionage wirkungsvoll verhindern zu können?

Antwort: Ja, eine Verschlüsselung der Multimediaströme ist prinzipiell möglich und mit dem Secure Realtime Transport Protocol (SRTP) existiert seit einigen Jahren ein internationaler Standard, der optimal auf die Echtzeitaspekte bei der Sprach- und Videoübertragung Rücksicht nimmt. Obwohl einige IP-Telefone von namhaften VoIP-Herstellern SRTP unterstützen, wird eine konsequente Verschlüsselung leider mangels genügender Sensibilisierung der Anwender intern noch selten eingesetzt.

Besser sieht es beim Gebrauch von «Softphones» aus. Da auf mobilen Rechnern häufig ein VPN-Client für den Fernzugriff installiert ist, kann die gesicherte Tunnelverbindung ins Firmen- oder Campusnetz für Gespräche mitbenutzt werden. Die am ITA-HSR entwickelte Linux strongSwan VPN-Lösung (www.strongswan.org) wird von mehreren Herstellern als eingebettete Software in ihren Telefonen oder VoIP-Gateways eingesetzt. Allerdings ist die Kapselung der relativ kompakten Sprachpakete durch das generische IPsec Sicherheitsprotokoll mit einem grossen

Overhead verbunden, der bis zu 50–100% der Nutzlast betragen kann und damit wertvolle Netzwerkbandbreite kostet.

Austausch von Session-Schlüsseln

Frage: Wie können zwei Gesprächspartner, die zum ersten Mal miteinander kommunizieren wollen, unkompliziert und sicher einen gemeinsamen geheimen Session-Schlüssel austauschen?

Antwort: Seit gut dreissig Jahren existiert mit dem Diffie-Hellman Key Exchange-Algorithmus ein Verfahren, das einen Schlüsselaustausch über ein unsicheres Medium ermöglicht, ohne dass Dritte, die den Austausch aufzeichnen, irgendwelche Rückschlüsse auf den geheimen Schlüssel ziehen können. Mit dem Multimedia Internet Keying Protokoll (MIKEY) wurde vor kurzen ein entsprechender Standard speziell für den Aufbau von Multimediaverbindungen definiert.

Authentisierung der Gesprächspartner

Frage: Wie kann ich sicherstellen, dass ich direkt mit dem richtigen Gesprächspartner verbunden werde, ohne die Gefahr eines «Man-in-the-Middle», der sich dazwischengeschaltet hat? Und wie kann ich mich vor unerwünschten Anrufen schützen?

Antwort: Die zuverlässige Authentisierung der Kommunikationspartner ist ein zentrales Thema bei der Internet-Telefonie. Solange nur im eigenen Firmennetz telefoniert wird, stellt sich das Problem meist nicht, da alle Teilnehmer über lokale Mechanismen authentisiert werden können. Sobald aber ein VoIP-Gespräch über Domänengrenzen hinweg aufgebaut werden soll, stellt die fehlende globale Public Key Infrastruktur, die zur Authentisierung benötigt würde, zurzeit eine grosse Hürde dar.

Getrieben durch die Angst vor SPIT (SPAM over Internet Telephony), d. h. millionenfach versendete unerwünschte Werbeclips, wird darüber nachgedacht, ob sog. DomainKeys, die im Rahmen der SPAM-Bekämpfung zur Authentisierung von E-Mail-Servern im globalen Domain-Name-System (DNS) hinterlegt werden, nicht auch für eine skalierbare, domänenübergreifende Authentisierung von VoIP-Teilnehmern genutzt werden könnten. Unser Institut hat die Machbarkeit dieses Ansatzes kürzlich praktisch nachgewiesen.

Sicherheit von Skype?

Frage: Welche Sicherheitsrisiken gehe ich beim Telefonieren mit Skype ein?

Antwort: Der proprietäre Skype Client, dessen Software bisher nur bruchstückhaft analysiert werden konnte, hat zwar vorbildlich eine Peer-to-Peer Verschlüsselung, sowie eine zentralisierte Benutzerauthentisierung realisiert, die so stark ist, dass selbst die dazu berechtigten Strafverfolgungsbehörden keine Möglichkeit sehen, Skype-Gespräche abzuhören. Aber wer weiss, ob die Skype-Besitzerin eBay gewisse Masterschlüssel nicht schon an den Meistbietenden versteigert hat? ■

HSR
HOCHSCHULE FÜR TECHNIK
RAPPERSWIL

ITA
INSTITUT FÜR INTERNET-TECHNOLOGIEN
UND -ANWENDUNGEN

Literatur und Links

- Andreas Steffen, Secure Internet Telephony, LinuxTag 2006 Wiesbaden, <http://www.strongswan.org/LinuxTag2006-VoIP.pdf> (11.7.2006).
- Philippe Biondi/Fabrice Desclaux, Silver Needle in the Skype, BlackHat Europe 2006, <http://www.blackhat.com/presentations/bh-europe-06/bh-eu-06-biondi/bh-eu-06-biondi-up.pdf> (11.7.2006).

Zeitschrift für Datenrecht und Informationssicherheit
digma
www.digma.info
erscheint vierteljährlich

Meine Bestellung

❑ 1 Jahresabonnement digma (4 Hefte des laufenden Jahrgangs)
à **CHF 155.00** bzw. bei Zustellung ins Ausland **EUR 126.00** (inkl. Versandkosten)

Name Vorname

Firma

Strasse

PLZ Ort Land

Datum Unterschrift

Bitte senden Sie Ihre Bestellung an:
Schulthess Juristische Medien AG, Zwingliplatz 2, CH-8022 Zürich
Telefon +41 44 200 29 19
Telefax +41 44 200 29 18
E-Mail: zs.verlag@schulthess.com
Homepage: www.schulthess.com

Schulthess §