Zeitschrift für Datenrecht und Informationssicherheit

digma

www.digma.info 11. Jahrgang, Heft 2, Juni 2011

Schwerpunkt:

Location Based Services

fokus: Datenschutz in ortsbasierten Diensten
fokus: Location Privacy in RFID-Systemen
report: Offene Deklaration von Web Analytics

Herausgegeben von
Bruno Baeriswyl
Beat Rudin
Bernhard M. Hämmerli
Rainer J. Schweizer
Günter Karjoth

Schulthess §

inhalt

fokus

Schwerpunkt:
Location Based Services

Datenschutz in ortsbasierten Diensten

Ortsbasierte Dienste ermöglichen eine Nutzung von Mobiltelefonen als persönliche Informationsquelle und helfen dabei, die für eine Person relevante Information aus der Datenflut des Internets herauszufiltern. Der Autor erklärt die Probleme von ortsbasierten Diensten und erläutert mögliche Lösungsansätze.

Datenschutzgerechte ortsbasierte Dienste

Bei vielen ortsbasierten Diensten besteht die Gefahr, dass die Diensteanbieter exzessiven Zugang zu den personenbezogenen Daten über die Nutzer erhalten. Wie können ortsbasierte Dienste rechts- und datenschutzkonform gestaltet werden?

Location Privacy in RFID-Systemen

RFID-Systeme ermöglichen die automatische drahtlose Identifikation von Objekten und stellen eine allgegenwärtige Technologie mit zahlreichen Anwendungsmöglichkeiten dar. Welches sind die Sicherheits- und Datenschutzanforderungen an solche Anwendungen?

Schutz von Lieferketten mit RFID-Tags

Das Einschleusen von Fälschungen stellt heute eine grosse Gefahr für Warenlieferketten dar. Das System «Tracker» setzt einfache RFID-Tags als Ersatz für herkömmliche Barcodes ein, um Lieferketten gegen eingeschleuste Fälschungen abzusichern und ausserdem neugierige Mitbewerber davon abzuhalten, die eigene Warenlieferkette auszuspähen.

impressum

digma: Zeitschrift für Datenrecht und Informationssicherheit, ISSN: 1424-9944, 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. Günter Karjoth

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

Zustelladresse: Redaktion digma, per Adr. Datenschutzbeauftragter des Kantons Basel-Stadt, Postfach 205, CH-4010 Basel
Tel. +41 (0)61 201 16 42, Fax +41 (0)61 201 16 41, redaktion@digma.info

Erscheinungsplan: jeweils im März, Juni, September und Dezember

Abonnementspreise: Jahresabo Schweiz: CHF 158.00, Jahresabo Ausland: Euro 131.00 (inkl. Versandspesen), Einzelheft: CHF 42.00

Anzeigenmarketing: Publicitas Publimag AG, Mürtschenstrasse 39, Postfach, CH-8010 Zürich
Tel. +41 (0)44 250 31 31, Fax +41 (0)44 250 31 32, www.publimag.ch, service.zh@publimag.ch

Herstellung: Schulthess Juristische Medien AG, Arbenzstrasse 20, Postfach, CH-8034 Zürich

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

Offene Deklaration von Web Analytics

Website-Betreiber sammeln und analysieren eine Fülle an Daten, ohne dies offen zu deklarieren. Datenschutz-Gütesiegel wie EuroPriSe erhöhen die Transparenz beim Einsatz von Web Analytics.

Häusliche Gewalt

StPO und OHG regelten die Mitteilung von Name und Adresse von Opfern an eine Beratungsstelle abschliessend und damit bleibe für kantonales Recht kein Raum, kritisieren Kettiger/Schwander einen in digma 2010.4 erschienenen Artikel von Glockengiesser/Stämpfli. Stimmt nicht ganz, wenden die beiden Autorinnen des ersten Beitrages ein, und weisen darauf hin, dass in Fällen von häuslicher Gewalt ausserhalb des Geltungsbereichs der StPO durchaus kantonaler Regelungsspielraum und -bedarf besteht.

Raserei auf der Strasse

Wer mit seinem Auto auf der Strasse zu schnell unterwegs ist, riskiert, geblitzt zu werden. Höchste Zeit, dass das Strassenverkehrsgesetz geändert und die Höchstgeschwindigkeit abgeschafft werden. Eine abwegige Argumentation? Mitnichten, wenn man die Reaktion auf ein Bundesverwaltungsgerichtsurteil zu einer anderen «Raserei auf der Strasse» hört …

Schutz von Lieferketten mit RFID-Tags

«Tracker» sichert RFID-basierte Supply Chains gegen Fälschungen und neugierige Mitbewerber.

Erik-Oliver Blass, Dr., EURECOM, Networking and Security, Sophia Antipolis, Frankreich
blass@eurecom.fr

Refik Molva, Prof. Dr., EURECOM, Networking and Security, Sophia Antipolis, Frankreich
molva@eurecom.fr

Grosse Warenlieferketten sind heute durch das Einschleusen gefälschter Waren bedroht. RFID-Tags können mithilfe des Systems «Tracker» Lieferketten dagegen absichern.

Das Einschleusen gefälschter Ware stellt heute eine grosse Gefahr für Warenlieferketten (Supply Chains) dar. Die World Health Organization (WHO) schätzt, dass es sich bei 10% aller in den USA verkauften Medikamente im Jahr 2005 um Fälschungen gehandelt hat[1]. Betreiber von Lieferketten benötigen demnach Lösungen, wie Lieferketten gegen das Einschleusen von Fälschungen geschützt werden können. Inzwischen suchen spezielle Einsatzgruppen von WHO («IMPACT»), der internationalen Handelskammer («ICC Crime Services») und sogar EU-weite Forschungsprojekte wie «SToP» nach Lösungen gegen Fälschungen.

In vielen Lieferketten ersetzen heute sogenannte «RFID-Tags» die bekannten, herkömmlichen «Barcodes». Bei solchen Tags handelt es sich um billige Kleinstcomputer von nur wenigen Zentimetern Grösse, die drahtlos gespeicherte Informationen mit RFID-Lesegeräten austauschen können. Damit kann beispielsweise auf günstige Weise bei Wareneingang und -ausgang die eindeutige Warennummer «ausgelesen» werden. Tags können, genau wie Barcodes, an den Waren der Lieferkette befestigt werden – so zum Beispiel durch einfaches Aufkleben der Tags auf die Ware. Die Tag-Hardware ist aus Kostengründen sehr einfach gehalten. Ein Tag verfügt über keinerlei eigene Stromversorgung, sondern wird allein über das vom RFID-Lesegerät generierte elektromagnetische Feld betrieben. Um Informationen mit dem Leser auszutauschen, modifiziert das Tag das elektromagnetische Feld des Lesers, was wiederum vom Leser bemerkt werden kann. Neben dem Speichern und Auslesen von Daten bieten die in diesem Artikel betrachteten «billigsten» Tags keinerlei weitere Funktionalität an. Diese Tags sind völlig passiv. Zukünftig sollen aber andere, wesentlich teurere Tags auch kryptografische Protokolle ausführen können[2].

Neben vielen unmittelbaren Vorteilen von Tags gegenüber Barcodes (grösserer, wieder beschreibbarer Datenspeicher, effizienteres drahtloses Auslesen usw.) können Tags allerdings auch dabei helfen, Lieferketten gegen Warenfälschungen abzusichern.

Das im Folgenden beschriebene System «Tracker» ermöglicht dem Betreiber einer Lieferkette, präzise zu ermitteln, welchen Pfad eine bestimmte Ware durch die Warenlieferkette genommen hat. Damit lässt sich die Echtheit einer Ware überprüfen. Einer böswilligen dritten Instanz («Angreifer») ist es nicht möglich, eine gefälschte Ware in die Lieferkette einzuschleusen, ohne dass dies vom Betreiber der Lieferkette erkannt wird.

Ein zweiter, von Warenechtheit unabhängiger Beitrag Trackers betrifft den Schutz der «Privatsphäre» von Lieferketten. Üblicherweise möchten Betreiber von Lieferketten keinerlei sensitive Informationen über Details und interne Abläufe der Lieferkette an Mitbewerber preisgeben. So sollen Mitbewerber beispielsweise nicht erkennen können, welche Pfade Waren innerhalb der Lieferkette nehmen.

Tracker im Überblick

Grob vereinfacht kann eine Lieferkette allgemein als gerichteter Graph dargestellt werden. Waren fliessen gemäss bestimmter Kanten (Vorschriften) vom Wurzelknoten (Hersteller) bis hin zu Blattknoten (Verbraucher). Auf ihrem Weg passieren Waren weitere Knoten (z.B. Zulieferer, Qualitätskontrolle), bis sie schliesslich einen Blattknoten erreichen. Bestimmte, ausgewählte Knoten innerhalb der Graphen heissen in Tracker «Checkpoints». Bei einem Checkpoint möchte der Betreiber der Lieferkette jederzeit überprüfen können, ob eine Ware, die diesen Checkpoint passiert, echt ist oder ob es sich um eine Fälschung handelt.

Ein einfaches Beispiel zeigt die Abbildung auf der nächsten Seite. Alle Waren werden zunächst

bei Hersteller ‹H› in die Lieferkette eingesetzt. Bei den Knoten ‹a›, ‹b›, ‹c›, ‹d› in der Abbildung handelt es sich um Zulieferer. Knoten ‹e› kann als Verbraucher oder Endkunde betrachtet werden. Die Kanten in der Abbildung geben erlaubte Pfade durch die Lieferkette an. So ist z.B. der Pfad ‹H, a, d, e› laut Betreiber der Lieferkette genauso erlaubt wie der Pfad ‹H, a, c, c, e›. Nicht erlaubt wäre beispielsweise der Pfad ‹H, c, e› oder der Pfad ‹d, e, b›. Falls eine Ware einen solchen Pfad nimmt oder generell einen unvollständigen Pfad, dann wäre das ein Hinweis auf eine Fälschung, d.h., ein Angreifer hat eine gefälschte Ware unbefugt in die Lieferkette eingeschleust.

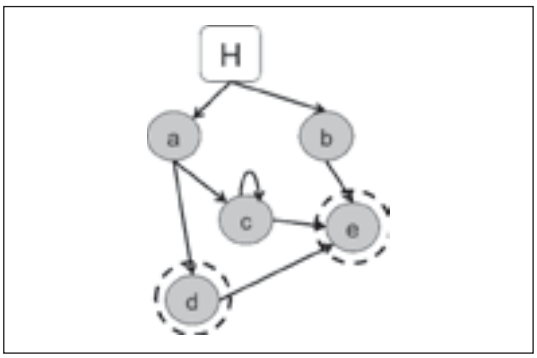

Abbildung: Lieferkette mit Checkpoints

Tracker bietet zwei komplementäre Formen von Sicherheit:

- *Schutz gegen Fälschungen:* Tracker ermöglicht dem Betreiber der Lieferkette, an einem Checkpoint (im Beispiel ‹d› oder ‹e›) genau zu verifizieren, welchen Pfad eine Ware genommen hat. Damit können Fälschungen identifiziert werden – ein Angreifer kann keine gefälschten Waren in die Lieferkette einschleusen. Dies ist selbst dann der Fall, wenn der Angreifer in der Lage ist, die drahtlose Kommunikation zwischen Tags und Lesegeräten innerhalb der Lieferkette abzuhören oder gar auf Tags gespeicherte Daten durch eigene ersetzen kann (Stichwort: «Cloning»).
- *Schutz der Privatsphäre:* Ausschliesslich der Betreiber der Lieferkette kann überprüfen, welchen Pfad Waren genommen haben. Keine dritte Instanz, z.B. Mitbewerber (ebenso als «Angreifer» zu bezeichnen), ist in der Lage, Informationen über die Historie einer Ware in der Lieferkette zu erlangen. Dies gilt auch im Falle eines Angreifers, der die drahtlose Kommunikation zwischen Tags und Lesegeräten abhört und Daten auf Tags durch eigene Informationen austauscht.

Tracker-Protokollbeschreibung

Überblick

Tracker geht zunächst davon aus, dass Waren mit RFID-Tags ausgestattet werden. Diese Tags verfügen über einen wiederbeschreibbaren Speicher. Jede Station in der Lieferkette, äquivalent zu einem Knoten in einem Graph, verfügt über einen RFID-Leser. Damit können die im Tag gespeicherten Daten ausgelesen und Tags danach neu beschrieben werden.

Tracker bietet zwei komplementäre Formen von Sicherheit: Schutz gegen Fälschungen und Schutz der «Privatsphäre» von Lieferketten.

In einem Checkpoint liest der Betreiber der Lieferkette schliesslich die Daten eines an einer Ware befestigten Tags aus und kann dann entscheiden, welchen Pfad die Ware genommen hat.

Tracker-Details

Die Idee von Tracker besteht darin, die von einer Ware besuchten Stationen der Lieferkette als Polynom ‹Q(x)› zu codieren. Dieses Polynom wird auf das Tag der Ware gespeichert und jedes Mal, wenn eine neue Station besucht wird, verändert.

Sobald eine Ware eine neue Station in der Lieferkette erreicht, liest der RFID-Leser die auf dem Tag gespeicherten Daten aus und erhält somit das Polynom. Der Leser berechnet nun auf Basis dieses Polynoms ein neues Polynom. Genauer: Der RFID-Leser führt eine bestimmte Funktion ‹$f_1()$› auf das zuvor ausgelesene Polynom aus und schreibt das Resultat ‹$f_1(Q[x])$›, wiederum ein Polynom, als neues Datum in das Tag. Der nächste RFID-Leser würde dieses Polynom ‹$f_1(Q[x])$› auslesen, seine Funktion ‹$f_2()$› darauf ausführen und ‹$f_2(f_1(Q[x]))$› in das Tag schreiben. Dieses Schema wiederholt sich, bis die Ware bei einem Checkpoint oder beim Verbraucher ankommt.

Kurz&bündig

In grossen Warenlieferketten ersetzen RFID-Tags heute herkömmliche Barcodes. Tags haben gegenüber Barcodes einige Vorteile wie höhere Auslesegeschwindigkeit oder grössere Flexibilität durch wiederbeschreibbaren Speicher. Ausserdem können RFID-Tags helfen, Lieferketten gegen zwei grosse Gefahren abzusichern. Eine Gefahr geht davon aus, dass Angreifer versuchen, Fälschungen unbemerkt in die Lieferketten einzuschleusen. Ausserdem können Mitbewerber versuchen, interne Abläufe über die Warenkette in Erfahrung zu bringen. Das RFID-basierte System Tracker schützt gegen diese Gefahren. Die Idee von Tracker ist es, den durch die Lieferkette genommenen Pfad einer Ware als ein verschlüsseltes Polynom auf dem der Ware anhaftenden RFID-Tag abzuspeichern. RFID-Lesegeräte entschlüsseln diese Polynome nicht, sondern berechnen mithilfe effizienter «additiv homomorpher Verschlüsselung» ein neues Polynom und speichern dieses im Tag. Der Betreiber einer Lieferkette kann schliesslich das Polynom auf einem Tag entschlüsseln und die genaue Historie der Ware bestimmen.

Die von jedem Leser ausgeführte Funktion ‹f› hat die Eigenschaft, eindeutige Polynome zu erzeugen. Das bedeutet, dass die Reihenfolge von Stationen in der Lieferkette eindeutig in das Polynom mit eincodiert wird. In der Abbildung würden sich so zwei verschiedene Polynome für Tags ergeben, die die Pfade ‹H, b, e› oder ‹H, e, b› durchlaufen. Da der Betreiber der Lieferkette die möglichen erlaubten Pfade kennt, kann er auch die sich daraus ergebenen Polynome berechnen.

Erreicht eine Ware so schliesslich einen Checkpoint, so liest der Betreiber das auf dem Tag gespeicherte Polynom aus. Der Betreiber kann nun nur auf Basis des gespeicherten Polynoms eindeutig über den genommenen Pfad entscheiden. Er vergleicht dazu einfach das ausgelesene Polynom mit der Liste der vorab berechneten Polynome gültiger Pfade.

Die von einer Ware besuchten Stationen der Lieferkette werden als Polynom ‹Q(x)› codiert, auf das Tag der Ware gespeichert und bei jeder besuchten Station verändert.

Schutz gegen Fälschungen

Um sich gegen Angreifer und gefälschte Waren zu schützen, sind die auf den Tags gespeicherten Polynome in Tracker verschlüsselt. Die von den RFID-Lesern ausgeführten Funktionen ‹f› sind derart, dass sie auf verschlüsselten Polynomen operieren können. Man spricht hier von sogenannter «additiv homomorpher Verschlüsselung». Der Leser führt seine ‹f›-Funktion direkt auf dem ausgelesenen, verschlüsselten Polynom aus. Das Ergebnis einer solchen Operation ist dann die Verschlüsselung des Resultats der ‹f›-Funktion. Ein Angreifer ist nicht in der Lage, ein gültiges, verschlüsseltes Polynom zu erzeugen und auf einem Tag abzuspeichern. Der Angreifer kann auch kein verschlüsseltes Polynom von einem anderen Tag einer (gültigen) Ware auslesen, verändern und auf sein eigenes Tag kopieren. Der Betreiber der Lieferkette kann solches «Cloning» unmittelbar am Checkpoint feststellen. Tracker ermöglicht dies, indem das (verschlüsselte) Polynom mit einer ebenso verschlüsselten, eindeutigen ID verbunden ist. Genauer gesagt berechnet Tracker den sogenannten «HMAC» der ID. Tracker speichert die verschlüsselte ID und den HMAC auch auf dem Tag ab. Der Betreiber kann, nachdem er die ID entschlüsselt hat, genau nachprüfen, ob das vorliegende Tag mit dieser ID einen bestimmten Pfad genommen hat. Ein «Clone»-Tag, das die gleiche ID speichert wie ein originales Tag, wird daher sofort erkannt.

Sogar RFID-Leser von einzelnen Stationen können nicht die ‹f›-Funktion anderer Leser von anderen Stationen in der Lieferkette fälschen.

Lediglich der Betreiber der Lieferkette ist in der Lage, an einem Checkpoint die im Tag gespeicherte Verschlüsselung eines Polynoms zu entschlüsseln und damit das Polynom zu erhalten.

Schutz der «Privatsphäre» der Lieferkette

Angreifer sollen nicht in der Lage sein, irgendwelche Informationen über die Herkunft einer Ware zu treffen. Zum Beispiel soll es Angreifern unmöglich sein, den Pfad, den eine Ware genommen hat, aus dem im Tag gespeicherten Datum zu rekonstruieren. Zudem soll ein Angreifer, der die Daten aus zwei Tags ausliest, nicht entscheiden können, ob die Waren der Tags über eine oder mehrere gleiche Stationen in der Lieferkette das Ziel erreicht haben. Wenn z.B. eine Ware über Pfad ‹H, a, c, e› und eine andere über ‹H, b, e› den Verbraucher erreicht, so soll der Angreifer nicht erkennen können, dass die beiden Waren über verschiedene Pfade den Verbraucher erreicht haben. Selbst wenn zwei Waren den Verbraucher über zwei exakt gleiche Pfade erreichen, so soll diese Information für den Angreifer nicht erkenntlich sein.

Tracker löst dieses Problem mithilfe von sogenannter «probabilistischer Verschlüsselung». Diese Technik ermöglicht, dass Chiffrate, die Ergebnisse von Verschlüsselungsoperationen, für einen Angreifer immer völlig «zufällig» aussehen. Ein Angreifer kann ein Chiffrat nicht von einer Menge Zufallszahlen unterscheiden. Selbst zwei Chiffrate von ein und demselben Klartext sehen unterschiedlich voneinander aus.

Literatur

- Erik-Oliver Blass/Kaoutar Elkhiyaoui/Refik Molva, «Tracker: Security and Privacy for RFID-based Supply Chains», Proceedings of 18th Annual Network & Distributed System Security Symposium (NDSS '11), 455–472, San Diego, USA, 2011 (ISBN 1-891562-32-0).
- G. Avoine, RFID Security & Privacy Lounge, 2011, <http://www.avoine.net/rfid/>.
- EU project SToP, Stop Tampering of Products, 2010, <http://www.stop-project.eu/>.
- ICC Commercial Crime Services. Counterfeiting Intelligence Bureau, 2010, <http://www.icc-ccs.org/>.
- International Medical Products Anti-Counterfeiting Taskforce. International Medical Products Anti-Counterfeiting Taskforce – IMPACT, 2010. <http://www.who.int/impact/>.

Fussnoten

1 K. Brooks, Anti-Counterfeiting Initiatives and RFID Practices. Contract Pharma, Feb 2006, <http://tinyurl.com/yj5pxct>.

2 Siehe die Übersicht über aktuelle Forschungsarbeiten bei Avoine 2011.

3 Blass/Molva 2011.

Evaluierung

Tracker ist extrem effizient und leichtgewichtig, sowohl für die RFID-Tags als auch für RFID-Lesegeräte. Ein Tag benötigt insgesamt nur 80 Byte Speicher, damit der Betreiber es eindeutig identifizieren und gleichzeitig den genommenen Pfad durch die Lieferkette verifizieren kann. Bis auf diese 80 Byte werden keine Anforderungen an das Tag gestellt. Diese Effizienz macht Tracker besonders für billigste, serienmässig und in Massen produzierte RFID-Tags der Standardkategorie «EPC Class 1 Gen 2» interessant. EURECOM erarbeitet gerade einen Prototypen, um die einfache Umsetzbarkeit von Tracker in die Praxis zu demonstrieren. Auch aufseiten der Lesegeräte ist Tracker äusserst effizient: Ein Leser muss nur eine sogenannte «elliptische Kurven-Elgamal-Verschlüsselung» ausführen können. Da diese Operation selbst sehr leichtgewichtig ist, können günstige RFID-Leser auf Mikrocontroller-Basis in Tracker eingesetzt werden.

Neben diesen praktischen Aspekten ist Tracker auch auf theoretischer Ebene evaluiert worden[3]. Die Sicherheit in Bezug auf Schutz gegen Fälschungen und Schutz der Privatsphäre sind mathematisch formal bewiesen worden. Genauer gesagt ist es gelungen zu zeigen, dass Trackers Eigenschaften mindestens so sicher sind wie zwei lang etablierte Eigenschaften, auf denen heute viele Sicherheitsprotokolle im alltäglichen Gebrauch basieren: die sogenannten «Computational» und «Decisional Diffie Hellman»-Eigenschaft sowie die «Existential Forgery»- und «Indistinguishability»-Eigenschaft von HMAC.

Die Sicherheit in Bezug auf Schutz gegen Fälschungen und Schutz der «Privatsphäre» von Lieferketten sind mathematisch formal bewiesen worden.

Ein solch formaler Beweis von Sicherheit erhöht den Wert von und das Vertrauen in Tracker gegenüber sonst nur oberflächlichen Sicherheitsanalysen stark.

Fazit

Das Einschleusen von Fälschungen stellt heute eine grosse Gefahr für Warenlieferketten dar. Das System «Tracker» setzt einfache RFID-Tags als Ersatz für herkömmliche Barcodes ein, um Lieferketten gegen eingeschleuste Fälschungen abzusichern. Mithilfe von Tracker lassen sich ausserdem neugierige Mitbewerber davon abhalten, die eigene Warenlieferkette auszuspähen und Informationen über Abläufe und Zusammenhänge innerhalb der Lieferkette zu erlangen. ■

agenda

The 11th Privacy Enhancing Technologies Symposium (PETS 2011)
University of Waterloo, Canada
27.–29. Juli 2011
<http://petsymposium.org/2011>

CRYPTO 2011
UC Santa Barbara, California, USA
14.–18. August 2011
<http://www.iacr.org/conferences/crypto2011>

Datenschutz Sommerakademie
Unabhängiges Landeszentrum für Datenschutz Schleswig-Holstein
29. August 2011, Kiel
<www.datenschutzzentrum.de>

16. Symposium on Privacy and Security
Stiftung für Datenschutz und Informationssicherheit
6. September 2011, ETH Zürich
<http://www.privacy-security.ch>

35. Datenschutzfachtagung (DAFTA)
Gesellschaft für Datenschutz und Datensicherheit (GDD) e.V.
17.–18. November 2011, Maternushaus, Köln
<https://www.gdd.de/veranstaltungen>

14. Berner Tagung für Informationssicherheit
Information Security Society Switzerland (ISSS)
24. November 2011, Bern
<http://www.isss.ch>

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

Meine Bestellung

❑ 1 Jahresabonnement digma (4 Hefte des laufenden Jahrgangs)
à **CHF 158.00** bzw. bei Zustellung ins Ausland **EUR 131.00** (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 §