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

Schulthess §

inhalt

fokus

Schwerpunkt:
Location Based Services

auftakt
Menschliches Versagen
von Michael Waidner Seite 49

Wo war wer wann? Ihr Smartphone weiss es
von Günter Karjoth Seite 52

Datenschutz in ortsbasierten Diensten
von Martin Werner Seite 54

Datenschutzgerechte ortsbasierte Dienste
von Jan Zibuschka und Eleny Kosta Seite 60

zwischentakt
Um Dimensionen brisanter: Facebooks Gesichtserkennung
von Beat Rudin Seite 65

Datenschutz durch Selbstregulierung?
von Kurt Pärli Seite 66

Location Privacy in RFID-Systemen
von Christian Wachsmann und Ahmad-Reza Sadeghi Seite 70

Schutz von Lieferketten mit RFID-Tags
von Erik-Oliver Blass und Refik Molva Seite 76

agenda Seite 79

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 …

report

Transparenz im Internet
Offene Deklaration von Web Analytics
von Darius Zumstein, Aleksandar Drobnjak und Andreas Meier — Seite 80

Follow-up: Häusliche Gewalt
Häusliche Gewalt: Vom Bund geregelt
von Daniel Kettiger und Marianne Schwander — Seite 86

Follow-up: Häusliche Gewalt
Häusliche Gewalt: Es darf diskutiert werden
von Iris Glockengiesser und Sandra Stämpfli — Seite 90

Transfer
Smartphones als Virenschleuder?
von Roland Portmann — Seite 92

forum

privatim
Aus den Datenschutzbehörden
von Sandra Stämpfli — Seite 94

schlusstakt
Raserei auf der Strasse
von Bruno Baeriswyl — Seite 96

cartoon
von Reto Fontana

Transfer

Smartphones als Virenschleuder?

Prof. Roland Portmann, Dozent für IT-Security, Hochschule Luzern – Technik & Architektur, roland.portmann@hslu.ch

Malware-Entwickler konzentrieren sich heute primär auf Rechner mit Microsoftbetriebssystemen. Nicht dass diese Betriebssysteme unsicherer wären als andere; ausschlaggebend ist die Marktdominanz dieses Betriebssystems. Bereits heute werden weltweit mehr Smartphones betrieben als Arbeitsplatzrechner. Wird sich der Fokus der Malware-Entwickler zu den Smartphones-Betriebssystemen verschieben?

Die Betriebssysteme von modernen Smartphones und Arbeitsplatzrechnern sind durchaus vergleichbar. So setzen Apple beim iPhone wie auch Google bei Android unix-ähnliche Betriebssysteme ein. Im Gegensatz zu Arbeitsplatzrechnern, wo ein Benutzer die volle Kontrolle über das Betriebssystem hat, besitzt ein Benutzer auf Smartphones nur eingeschränkte Berechtigungen. So können beispielsweise auf einem iPhone nur Applikationen gestartet werden, die von Apple signiert wurden.

Viele Benutzer von Smartphones umgehen diese Schutzmechanismen, indem sie mit einem Jailbreak das iPhone freischalten oder sich Root-Berechtigungen auf Android-Geräten verschaffen. Entsprechende Anleitungen sind auf dem Internet einfach zu finden. Damit lassen sich auch die ungeliebten Restriktionen der Hersteller umgehen. Mit einem offenen iPhone kann man dann Musik von «Gratis»-Seiten herunterladen und andere von Apple nicht vorgesehene Funktionen ausführen. Gemäss Jay Freeman, dem Entwickler eines Jailbraking-Programms[1], sollen auf etwa 10% aller 50 Millionen iPhones weltweit Jailbreaks angewendet worden sein.

Freiheit auch für Malware

Neben den neuen Freiheiten, die man mit einem gehackten Smartphone bekommt, handelt man sich grosse Sicherheitsprobleme ein. Ein wichtiger Schutzmechanismus gegen Malware wird damit lahmgelegt.

Im letzten Jahr wurden neue Angriffsmechanismen entwickelt, die verschiedene Schwachstellen der Smartphone-Betriebssysteme ausnützen und ein Smartphone auch ohne Benutzerinteraktion freischalten (rooten, jailbreaken) können. So reicht es aus, auf dem iPhone ein manipuliertes Bild im Tiff-Format zu öffnen (libtiff vulnerability). Auch mit fehlerhaften Schriften, die in PDF-Files eingebettet sind, kann ein Jailbreak auf das iPhone kommen. Ein Aufruf von verseuchten Web-Seiten im iPhone-Browser reicht also aus, um sein Gerät freigeschaltet zu bekommen. Verseuchte Webseiten können auch gleich eine Malware installieren.

Viele Jailbreaking-Applikationen installieren zusätzlich einen SSH-Server auf dem iPhone. Viele Benutzer vergessen aber, das initiale Passwort («alpine») zu ändern. Damit kann man über WLAN, das bei den meisten Smartphones ständig eingeschaltet ist, sehr einfach mit vollen Berechtigungen in das Smartphone eindringen.

Malware aus dem App-Store

Die App-Store von Apple und Google bieten mehrere 100 000 Applikationen an. Obwohl die Anbieter versuchen, nur sichere Applikationen über ihre Stores anzubieten, kann nicht ausgeschlossen werden, dass Applikationen angeboten werden, die auch unerwünschte Funktionen implementiert haben, von denen der Benutzer nichts weiss. Es gab im letzten Sommer Gerüchte über ein Wallpaper für Android-Phones, das im Hintergrund verschiedene Informationen wie SMS-Nachrichten, SIM-Kartennummern und Passwörter an eine chinesische Webseite weiterleitet[2]. Dies führte dazu, dass Google die App nach millionenfachem Download aus dem Market sperrte. Auch wenn sich schlussendlich dieses Gerücht nicht bewahrheitete, zeigt dieses Vorkommnis die mit den Stores verbundenen Risiken eindrücklich auf.

Neue Welten für Malware

Für Malware auf Smartphones öffnen sich neue Welten. Eine Malware kann im Hintergrund beliebige SMS an alle gespeicherten Kontakte verschicken. Diese SMS können beispielsweise einen Link auf Webseiten enthalten, die manipulierte TIFF-Bilder oder PDF-

Files enthalten. Da das SMS ja von einer bekannten Person kommt, wird der Empfänger diesen Link vermutlich anklicken, insbesondere wenn im SMS-Text beispielsweise steht «Geniale Webseite für dich entdeckt!». Mittels MMS können allfällige Multimediaschwachstellen ausgenützt werden. Eine Verbreitung von Malware mit Bluetooth war bereits vor Jahren erfolgreich.

Mindestens im Labor gibt es bereits Implementationen von Botnets für Smartphones. Ein mit einer Botnet-Software verseuchtes Smartphone lässt sich von einer verteilten Server-Infrastruktur fernsteuern und verschickt beispielsweise Spam-Mails oder wird für «Distributed Denial of Service»-Angriffe verwendet. Während ein privater Computer nur wenige Stunden pro Tag läuft, ist ein Smartphones 24 Stunden mit dem Internet verbunden. DDoS-Angriffe von Smartphones könnten daher sehr effektiv sein.

Malware over the Air

Alle Smartphones kommunizieren über viele Wege mit der Welt, sei es über die ständige Internetverbindung über den Telefonprovider oder per SMS (MMS). Smartphones können mit WLAN-Access Points verbunden werden und unterstützen das Bluetooth-Protokoll.

Mit der nächsten Protokoll-Generation (LTE) der Telefonie-Provider wird die Bandbreite von Smartphones vervielfacht. Die Rechnerleistung der Smartphones steigt ständig an. Dies wird in Zukunft sehr gefährliche Angriffe ermöglichen.

Während heute die meisten Arbeitsplatzrechner über eine Firewall an das Internet angeschlossen werden, sind die Smartphones ungeschützt im Internet.

Interessante Informationen auf Smartphones

Auf Smartphones werden heute sehr viele persönliche Informationen gespeichert. Das Adressbuch vieler Anwender umfasst mehr als 1000 Kontakte, alle E-Mail-Accounts werden synchronisiert, Informationen aus den Social-Network-Applikationen enthalten viele persönliche Informationen; Passwörter werden mit SMS an Kollegen scheinbar sicher übertragen; ein Smartphone weiss mittels der Lokalisierungsfunktionalitäten ständig, wo sich der Eigentümer aufhält; die Zugangsinformationen zu E-Mail-Accounts und zu VPN-Eingängen liefern Zugangsinformationen für Firmennetzwerke; man hat Live-Videobilder und Fotos; man findet Bank-Codes und vermutlich in Zukunft auch Kreditkarten-Informationen. Man braucht nicht viel Fantasie, um illegale «Anwendungsmöglichkeiten» für diese Fülle von Informationen zu finden.

Haben Sie einen Virenscanner?

Es gibt auf dem Markt Virenscanner für Smartphones. Es muss aber bezweifelt werden, dass diese Virenscanner bei massiven Angriffen einen ausreichenden Schutz bieten können, da selbst auf leistungsfähigen Arbeitsplatzrechnern der Schutz durch die Virenscanner eher abnimmt.

Aussicht

Warum soll sich die immer professioneller werdende Malware-Szene mit gut geschützten Microsoftbetriebssystemen abmühen, wenn die Benutzer ihr Smartphone selber öffnen (jailbreak, rooten)? Zudem werden auf Smartphones viele Informationen verwaltet, die für kriminelle Organisationen von grossem Wert sein können. Es wäre daher nicht überraschend, wenn die Malware-Szene ein zunehmendes Interesse für iPhones, Androids & Co. entwickeln würde. ■

Lucerne University of
Applied Sciences and Arts

HOCHSCHULE
LUZERN

Technik & Architektur
CC Informations- & Softwaresicherheit

Fussnoten

1 <http://www.saurik.com/id/12>.
2 <http://www.areamobile.de/news/16046-spyware-fuer-android-wallpaper-apps-stehlen-passwoerter>.

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 §