erschienen in der FIfF-Kommunikation,
herausgegeben von FIfF e.V. - ISSN 0938-3476
www.fiff.de

FIfF-Studienpreis 2013
2. Preis

Agata Królikowski

‚Due To Legal Issues' – Packet Inspection

Packet Inspection (PI) ist die Vereinigung verschiedener Technologien, um über ein Netz versendete Informationen zu analysieren und zu verwalten. Zum einen gibt es die Deep Packet Inspection *(DPI), bei der Pakete über Steuerdaten hinaus bitweise analysiert werden, zum anderen gibt es die* Statistical Packet Inspection *(SPI), die auch bei verschlüsselten Daten erfolgreiche Analysen durchführen kann. PI wird auf vielfältige Weise von Staaten, Internet Service Providern oder Netzwerkadministratoren eingesetzt.*

Doch wie funktionieren Paketanalysemethoden und wie effizient sind sie? Und gibt es aus Sicht eines Nutzers des Netzes einen technischen oder rechtlichen Schutz gegen diese Analysen?

Diese beiden Fragen wurden in der Diplomarbeit aufgegriffen und ausgehend von den Begriffen der Schutzziele untersucht. Da Schutzziele sowohl in der Datensicherheit als auch im Datenschutz verwendet werden, eignen sie sich, eine Brücke zwischen der Technik und den juristischen Aspekten zu schlagen. Im Wesentlichen wurden Integrität, Vertraulichkeit, Verfügbarkeit und Unverkettbarkeit als Metrik bei der Bewertung von Paketanalysesystemen herangezogen, um auch den Umfang dieser Arbeit etwas einzugrenzen [1].

Packet Inspection: The Medium is the Message

DPI ist zunächst ein Oberbegriff für verschiedene Technologien, die über ein Netzwerk verschickte Pakete bitgenau untersuchen können. Pakete sind Informationseinheiten, die aus Steuerdaten (engl. header) und Nutz- bzw. Inhaltsdaten (engl. payload) bestehen. „Deep" bezieht sich auf das TCP/IP[1]-Referenzmodell, welches die einzelnen Funktionen einer Kommunikation und damit auch die Paketinformationen logisch in sieben Schichten unterteilt.

Das Ziel einer DPI-Analyse ist, die Pakete anhand der vorgefundenen Muster (Signaturen) möglichst genau und ohne Fehler zu klassifizieren und dann anhand der zu der Signatur gespeicherten Regeln entweder weiterzuleiten, zu verlangsamen oder zu verwerfen.

Da es sich bei DPI um die Analyse von Zeichenketten handelt, erschweren alle Mechanismen DPI, die diese Zeichenketten verändern. Auf den ersten Blick scheinen Verschlüsselung oder das Verwenden von Verschleierungsmechanismen (z. B. Ändern des Ports oder Tunnelprotokolle) als gute Instrumente, um DPI zu erschweren bzw. sogar unmöglich zu machen und damit die Vertraulichkeit und Unverkettbarkeit von Daten zu schützen.

Allerdings kommt es für den Schutz auch auf die Ebene der Verschlüsselung oder der Verschleierung an. Verschlüsselt man die eigentlich übertragenen Protokolle auf der Anwendungsebene, sind die vom Nutzer übertragenen Daten nicht mehr sichtbar. Im unverschlüsselten Text bleiben jedoch genug Informationen übrig, aus denen Signaturen und damit Klassifikatoren erstellt werden können. Verschlüsselung schützt also nicht automatisch vor Paketanalysen. Bei der Analyse verschlüsselter Daten geht es auch nicht darum, die darunter liegenden kryptografischen Verfahren zu brechen, sondern darum, die Informationen gerade trotz verwendeter Verschlüsselungs- und Verschleierungsmechanismen auswerten zu können. Die Form der Nachricht verrät häufig schon den Inhalt der Nachricht.

Diese Art der Analysen erfolgt mit Hilfe der sogenannten Statistical Packet Inspection (SPI). SPI bezeichnet Analysemethoden, die statistische Eigenschaften sowie Wahrscheinlichkeitsverteilungen der Pakete und Paketströme berechnen und so auf bestimmte Eigenschaften hin untersuchen. Die Eigenschaften können sich auch auf alle Daten eines Pakets – also auch Nutzdaten – beziehen.

Um die prinzipiellen Möglichkeiten von SPI zu beleuchten, wurden exemplarisch Verfahren untersucht, die Paketklassifikation vornehmen können, obwohl auf den unterschiedlichen Schichten Verschlüsselung oder Verschleierung eingesetzt werden. Entlang des Schichtenmodells wurde systematisch gezeigt, welche Paketinformationen bei Analysen sichtbar werden. Die in der Arbeit vorgestellten Untersuchungen zeigen dabei nur einen kleinen Ausschnitt der vorhandenen Forschung. Auch wenn die Forschungsergebnisse nur mit Vorsicht auf kommerzielle Systeme übertragbar sind, lassen sich prinzipielle Lösungen und Tendenzen aufzeigen. Die Analysemöglichkeiten reichten dabei von der Rekonstruktion verschlüsselter Sprachpakete bei variablen Bitra-

ten [2] oder verschlüsselten MPEG4 -Videodaten [3], Analysemethoden der Secure Shell (SSH) [4] hin zu Website Fingerprinting [5]. Aber auch Kommunikation über SSL/TLS sowie IPSec bieten genügend Anhaltspunkte für erfolgreiche Analysen [6].

So wird beispielsweise zur Identifizierung einer bestimmten Anwendung, die über SSL übertragen wird, die Tatsache ausgenutzt, dass verschiedene Verschlüsselungsmechanismen verschiedene Paketgrößen verursachen. Zwar sind bei SSL über 50 verschiedene Verschlüsselungsarten möglich, allerdings gibt es besonders häufig implementierte Algorithmen wie AES, RC4, so dass sich die Herstellung eines Zusammenhangs zwischen Paketgröße und ursprünglicher Paketgröße auf diese Algorithmen konzentrieren kann [7].

Um aus den über das Netz verschickten Paketen Strukturen abzuleiten, werden Algorithmen aus dem Bereich des maschinellen Lernens angewendet. Im Gegensatz zu DPI, bei der Signaturen aus Zeichenfolgen oder Hashwerten der Zeichenfolgen bestehen, werden Muster unabhängig von konkreten Zeichenfolgen gewonnen. Durch die genaue Analyse bestimmter Protokolle und verwendeter Verschlüsselungs- bzw. Verschleierungsmechanismen gibt es inzwischen umfassende Kataloge mit Parametern, die analysiert werden müssen, um wiederum Rückschlüsse auf Protokolle und Inhalte zu schließen. Analysiert werden z. B. Paketlängen, Reihenfolge der Pakete, Entropie, Abstand zwischen den Paketen, bestimmte gesetzte Bits usw. [8]. Es werden dann alle möglichen Varianten, wie ein Protokoll aussehen müsste, wenn es durch eine bestimmte Art und Weise verschlüsselt oder verschleiert wird, in einer Bibliothek gespeichert. Hinweise darauf, wie wirkungsvoll ein solcher Brute-Force-Ansatz ist, liefert beispielsweise das Datenblatt von PACE der Firma Ipoque [9]. Dort sind mehrere Hundert Protokolle ausgewiesen, die nach eigener Aussage erkannt werden können.

Um Übertragungsverzögerungen zu vermeiden, werden Packet-Inspection-Lösungen immer auch mit dem Ziel entwickelt, die Analyse und Klassifikation in Echtzeit durchzuführen [10]. Dies ist allerdings bei bei Datenübertragungsraten von beispielsweise 10 Gbit/s in Rechnernetzen mit einem hohen Rechen-, Speicher- und Strombedarf verbunden. Um dies zu erreichen, und auch Fehlerraten, die bei der Klassifikation entstehen niedrig zu halten, werden Pakete und Paketströme DPI und SPI sowie weitere verschiedene Arten von port-, inhalts-, verhaltens- und statistikbasierter Methoden ergänzend mit eingesetzt. Pakete werden in hybriden Mehrkernarchitekturen vorgefiltert, indem sie in einzelne Bestandteile zerlegt und mit jeweils spezialisierten Architekturen getrennt nach den verschiedenen Paketschichten analysiert werden. PI-Systeme wie beispielsweise *Procera PakketLogic PL20000 Series* können auf diese Weise Durchsatzraten bis zu 320 Gbit/s erzielen [11]. Zum Vergleich: Der größte Internetknoten der Welt – Deutscher Commercial Internet Exchange Frankfurt (DE-CIX) – hatte 2011 einen durchschnittlichen Durchsatz von etwa 1,5 Tbit/s [12].

Welchen technischen Schutz gibt es noch?

Um sich also vor dieser Art von Analysen zu schützen, muss das Aussehen schon verschlüsselter Nachrichten derart verändert werden, dass daraus keine Informationen gezogen werden können. Ebenfalls sollte im Idealfall verborgen werden, dass Nutzer überhaupt Schutzmechanismen verwenden, da auch dies verdächtig sein könnte [13].

Die Idee, Nachrichten derart zu verschleiern, ist schon relativ alt und wurde bereits 1964 von *Paul Baran* vorgeschlagen. Sogenannte „Dummy"-Paketströme sollten Parameter von Paketen und Paketströmen direkt manipulieren. 1981 hat *David Chaum* das Konzept der Mixnetzwerke eingeführt, um E-Mails unverfolgbar zu machen. Eine Weiterentwicklung dieses Konzepts ist das Projekt *The Onion Routing* (TOR), welches Mixing, Rerouting und Verschlüsselung kombiniert. Doch gibt es prinzipielle Grenzen, wenn der Angreifer beispielsweise den Eingangs- und Ausgangsrouter kontrolliert. Auch ist die Verkettung von Inhalten und Umständen der Nachrichten durch den Einsatz statistischer Verfahren in Verbindung mit Wasserzeichen möglich [14].

In weiteren Projekten wie z. B. *Traffic Morphing* [15], werden verschiedene Ansätze zur Verschleierung erprobt und weiterentwickelt. Ein Problem dieser (und doch recht exotischen) Ansätze ist allerdings, dass ein großer Overhead entsteht und die Kommunikation merklich verlangsamt wird. Zudem werden in den Forschungsprojekten häufig nur einzelne Protokolle mit einzelnen Webseiten untersucht, so dass noch keine generellen Ergebnisse zur Verfügung stehen. Das größte Problem dieser Lösungsansätze ist allerdings, dass sie sich immer an technisch versierte Nutzer richten.

Daneben wurden in der Arbeit Maßnahmen untersucht, die streng genommen nicht unter Schutzmaßnahmen fallen, jedoch in der Lage sind, Paketdiskriminierung auf Seite von ISPs sichtbar zu machen. Die Aufdeckung von Paketdiskriminierung ist aber dennoch interessant und ein erster Schritt, die dahinter liegenden Überwachungsmechanismen zu identifizieren. Zu den untersuchten Projekten gehören *Network Neutrality Bot* [16],

Agata Królikowski

Agata Królikowski hat an der Humboldt-Universität zu Berlin zunächst Jura und dann Informatik studiert. Bis 2012 war sie wissenschaftliche Mitarbeiterin am Lehrstuhl Informatik in Bildung und Gesellschaft von Prof. Dr. Wolfgang Coy, wo sie ihre beiden Fachrichtungen miteinander verbinden konnte. Zur Zeit ist sie wissenschaftliche Mitarbeiterin am Innovations-Inkubator der Leuphana Universität Lüneburg und arbeitet dort in den Projekten Hybrid Publishing und Grundversorgung 2.0. Sie ist Präsidiumsmitglied sowie Mitglied des erweiterten Vorstands der GI und außerdem Sprecherin der Fachgruppe *Internet und Gesellschaft*.

Agata Królikowski und Stefan Hügel bei der Preisverleihung
Foto: Benhamin Kees

DiffProbe [17] und *Glasnost* [18]. Die Diskriminierung wird aufgedeckt, indem die Verzögerungszeiten zweier Paketströme miteinander verglichen werden.

Auch wenn diese Forschungsansätze ein klein wenig Anlass zur Hoffnung geben, verbergen sich dahinter im Moment noch einige Probleme. Da Schutzmechanismen nicht standardmäßig zur Verfügung stehen, müssen Nutzer sich selbst auf ihren Endgeräten darum kümmern. Gleichzeitig können Analysen großflächig an wenigen Knoten implementiert werden. Des Weiteren bieten über das Netz versendete Pakete eine Fülle von Parametern, die untersucht und ausgewertet werden können. Es ist kaum möglich, alle Parameter von vornherein zu verschleiern, so dass eine kleine Änderung in einem Analysealgorithmus einen Schutzmechanismus gänzlich aushebeln kann. Die entwickelten Werkzeuge sind von einem Standard weit entfernt.

Es gibt zur Zeit keinen wirklich wirksamen technischen Schutz gegen die eingesetzten Systeme und man muss bei der Kommunikation über das Internet mit der ständigen Verletzung von Vertraulichkeit, Integrität, Verfügbarkeit und Unverkettbarkeit rechnen. Aus technischer Sicht bleibt höchstens, dass man möglichst viele seiner Daten verschlüsselt und ab und zu testet, wie weit die ISPs in eine Kommunikation beispielsweise durch QoS[2]-Maßnahmen eingreifen. Letztendlich sind Schutzziele auf technischer Ebene aber nicht durchsetzbar.

Rechtliche Probleme

Betrachtet man Kommunikation mittels Post, Funk oder Telefon, die sehr leicht überwindbare oder keine technischen Schutzmaßnahmen aufweisen, stellt sich aber zunächst die Frage, weshalb Analysen von Internetverkehr überhaupt in der rechtlichen Grauzone liegen und damit problematisch sein könnten. Privater Funkverkehr ist in Deutschland von jedem mithörbar, Briefe können unbemerkt geöffnet und Telefonate zumindest von technisch Versierten abgehört werden. Aus diesem Gedanken heraus hat der Gesetzgeber das Brief-, Post- und Fernmeldegeheimnis in Art. 10 GG[3] geschaffen.

Grundgedanke bei diesem Grundrecht ist, dass der Austausch von Information so geschützt sein muss, als ob er von Angesicht zu Angesicht stattfinden würde, d. h. die Nachrichten dürfen von Unbefugten nicht zur Kenntnis genommen werden. Da Grundrechte im Allgemeinen zunächst nur den Staat binden, das TK-Geheimnis jedoch einen hohen Stellenwert genießt, wurde im Zuge der Privatisierung der Post und TK-Anbieter der Wesensgehalt des Art. 10 GG auf §88 TKG[4] übertragen, der nun auch private Stellen bindet. Telekommunikation (TK) ist der „technische Vorgang des Aussendens, Übermittelns und Empfangens von Signalen mittels TK-Anlagen“ [19]. Die Vertraulichkeit der Kommunikation wird durch das TK-Geheimnis in Art. 10 GG geschützt und umfasst deren Inhalt und Umstände, unabhängig davon, welche Technik verwendet wird. Inhaltliche Daten sind E-Mails, Chatnachrichten, Bilder usw. – Umstände umfassen Verkehrsdaten und Daten, die es ermöglichen, die Kommunikation von anderen zu unterscheiden. Darunter fallen Identifizierungsmerkmale und Kennungen.

Der Schutz über das Grundrecht des Art. 10 GG bzw. §88 TKG bietet jedoch nur auf den ersten Blick Sicherheit. Denn es kann durchaus auch erforderlich werden, das TK-Grundrecht einzuschränken.

So sind gem. §109 Abs. 2 S. 1 TKG TK-Anlagebetreiber verpflichtet, technischen Maßnahmen zum Schutz ihrer Anlagen zu ergreifen. Ein weiterer Anwendungsfall von PI ist die effektive Nutzung der Bandbreite. So dürfen z. B. Verkehrsdaten zweckgebunden erhoben und verarbeitet werden (§96 Abs. 1 TKG), um TK-Dienste zu erbringen. TK-Dienste sind dabei Transportdienstleistungen, die zur Übertragung von Signalen dienen. Nun wird z. B. die Übertragung von VoIP[5]-Paketen in Anschluss an die Tradition des Telefons als TK-Dienst betrachtet, die Übertragung von Daten (z. B. FTP)[6] hingegen nicht:

> *„Während die Bereitstellung eines Internet-Zugangs [...] eine besondere Dienstleistung darstellt, weist das bloße Telefonieren über das Internet keinen äußerlich erkennbaren Unterschied zur herkömmlichen leitungsgebundenen Telefonie auf. Insoweit handelt es sich um einen einheitlichen Lebensvorgang, der keiner anderen rechtlichen Bewertung als die herkömmliche Sprachtelefonie unterliegt und damit als eine reine TK-Dienstleistung anzusehen ist, die ganz in der Übertragung von Signalen über Kommunikationsnetze besteht und daher ausschließlich dem TKG zuzuordnen ist“.*[7]

Diese Unterscheidung zwischen Datenübertragung und VoIP ist willkürlich, die Kenntnis des Anwendungsprotokolls ist für die Übermittlung der richtigen Signale und damit für die Erbringung eines TK-Dienstes nicht notwendig. An dieser Stelle wird den ISPs Tür und Tor geöffnet, Analysemethoden anzuwenden.

Ein weiteres berechtigtes Interesse liegt in der sogenannten *Lawful Interception*. Die TK-Unternehmen sind gesetzlich verpflichtet, dem Staat eine Überwachungsinfrastruktur zur Verfügung zu stellen. In Deutschland besteht eine Mitwirkungspflicht gem. §110 TKG in Verbindung mit der Telekommunikations-Überwachungsverordnung. TKG-Überwachungen können beispielsweise im Rahmen der Verfolgung von Straftaten gem. §100 a StPO,[8] zur Überwachung durch den Nachrichtendienst (vgl. G10-Gesetz) oder aufgrund anderer Polizeigesetze erfolgen. Diese Mitwirkungspflicht hat zur Folge, dass eine Infrastruktur vorhanden ist, sich in den Händen dieser Firmen befindet und gleichzeitig aber

auch dieselbe Technologie umfasst, die man zur Bandbreitenmanagement, Traffic Shaping oder Netzwerksicherheit verwendet.

Neue Dimension: Statistische Analysen

Das Problem ergibt sich jedoch nicht nur aus der Überwachung als solcher, sondern vor allem aus dem Ausmaß. PI-Systeme sind leistungsfähig genug, um an zentralen Internetknoten wie dem DE-CIX Echtzeitanalysen des gesamten Internetverkehrs in Deutschland durchzuführen. Das TK-Verhalten jedes einzelnen Nutzers kann detailliert aufgenommen, analysiert und gespeichert sowie mit anderen Daten verknüpft und rückwirkend auch in anderen Zusammenhängen betrachtet werden. Da das Internet aber nicht nur der Kommunikation, sondern darüber hinaus auch als Plattform für virtuelle Versammlungen, Beschaffen künstlerischer Werke jeglicher Art, Presse, Rundfunk usw. dient, werden dadurch viel mehr Facetten eines Nutzers erfasst als nur die Tatsache, wer mit wem wann worüber kommuniziert hat. Es ist möglich, ein „Meinungsbild der Nation" aufzunehmen und dieses auch zu steuern. Bereits statistische Analysen wären dazu in der Lage. Zu bedenken ist jedoch, dass nur wenige Nutzer Schutzmaßnahmen ergreifen und somit sogar Klartextanalysen in großem Ausmaß möglich sind. Es zeigt sich, dass mit dem Internet nicht nur Grenzen der Kommunikation verschoben, sondern mit der Digitalisierung auch die Hemmschwelle zur Überwachung deutlich gesenkt wurde.

Diese großflächige Überwachungsmöglichkeit führt die Unschuldsvermutung ad absurdum, wenn ohne einen konkreten Anfangsverdacht nach Mustern gesucht wird, um daraus auf ein bestimmtes Verhalten der Nutzer zu schließen.

Neben diesen Betrachtungen gibt es noch zahlreiche weitere rechtliche Problemkreise. Problematisch sind auch Fragen der Netzneutralität, Meinungs- und Informationsfreiheit, Beweislast bei Online-Diensten wie z. B. De-Mail oder das Grundrecht auf Vertraulichkeit und Integrität informationstechnischer Systeme. Auch ergeben sich durch mögliche Analysen allgemeine datenschutzrechtliche Probleme wie z. B. die Frage, ob man QoS widersprechen darf, da personenbezogene Daten erhoben und verarbeitet werden. Doch auch wenn, wäre es technisch nicht realisierbar, die einen Pakete zu analysieren und die anderen nicht, so dass im Endergebnis dem Nutzer nur übrig bliebe, den Provider zu wechseln oder das Internet gar nicht mehr zu nutzen, wenn er einer Überwachung entgehen will.

Diese Schlussfolgerung ist jedoch bedenklich. Die Vielfalt der Nutzung führt über die Möglichkeit reiner Kommunikation hinaus. Und daher ist nicht nur ein einzelnes, sondern eine Vielzahl von Grundrechten betroffen: Angefangen bei dem TK-Recht und Recht auf Selbstbestimmung kommt das Recht eines jeden gem. Art. 5 Abs. 1 GG hinzu, „*seine Meinung in Wort, Schrift und Bild frei zu äußern und zu verbreiten und sich aus allgemein zugänglichen Quellen ungehindert zu unterrichten*", Vereinigungen zu bilden (Art. 9 Abs. 2 GG) oder seinen Beruf auszuüben (Art. 12 GG). Ein Verzicht auf das Nutzen des Internets kann keine Freiheitsausübung sein, wenn damit so viele Freiheitsverzichte einhergehen. Auf der anderen Seite ist die Aufgabe der Privatsphäre und die Kontrolle des Nutzerverhaltens ebenfalls kein Ausweg.

Was noch bleibt

Wenn grundrechtlich geschützte Kommunikation nur noch unter bestimmten Umständen und wenn überhaupt nur technischen Experten offen steht, bietet dies keine Grundlage für eine freie Informations- und Kommunikationsgesellschaft [20].

Es ist daher die Aufgabe des Gesetzgebers, klarzustellen, welche Rechte und Pflichten die einzelnen Akteure haben, welche rechtliche Grenzen bei der Verwendung von PI zu beachten sind und auch Sanktionen zu definieren. Es ist Aufgabe der TK-Anbieter ihre Systeme offenzulegen und jeden Nutzer darüber aufzuklären, was eigentlich mit seinen Daten passiert. Denn Freiheit kann nur derjenige ausüben, der die Folgen seines Handeln abschätzen kann.

Aus technischer Sicht gilt es, Verfahren zu finden, technische Prozesse wie Paketdiskriminierung in einer Form sichtbar zu machen, dass es nicht mehr Expertenkreisen vorbehalten ist, diese Techniken zu benutzen und zu verstehen, was im Netz passiert. Der nächste Schritt ist die Entwicklung von weiteren Schutzmaßnahmen, die nicht nur theoretisch oder im Labor erfolgreich sind, sondern ebenfalls auf breiter Basis angelegt auch für den Laien verständlich konzipiert sind. Die vorgestellten Verfahren sind ein Anfang, jedoch ist es bis zu einer Standardimplementation solcher Werkzeuge noch ein weiter Weg.

Schließlich ist nicht nur beim Nutzer, sondern in der Politik, den Juristen und verschiedenen Entscheidungsträgern Aufklärungsarbeit notwendig, um die Problematik der Manipulation im Netz deutlich zu machen.

Referenzen

[1] Pfitzmann, Andreas/Rost, Martin: Datenschutz-Schutzziele – revisited, in: Datenschutz und Datensicherheit (DuD), (2009), S. 353 – 358.

[2] Wright, Charles V./Ballard, Lucas/Coull, Scott E./Monrose, Fabian/ Masson Gerald M.: Spot me if you can: Uncovering spoken phrases in encrypted VoIP conversations, in: Proceedings of the 2008 IEEE Symposium on Security and Privacy, May 2008.

[3] Liu, Yali/Sadeghi, Ahmad-Reza/Ghosal, Dipak/Mukherjee, Biswanath: Video Streaming Forensic – Content Identification with Traffic Snooping, in: M. Burmester et al. (Hrsg): Information Security, 13th International Conference, ISC 2010, LNCS 6531, Berlin, Heidelberg, Springer-Verlag, 2011, S. 129–135.

[4] Dusi, Maurizio/Crotti, Manuel/Gringoli, Francesco/Salgarelli, Luca: Tunnel hunter: Detecting application-layer tunnels with statistical fingerprinting, in: Elsevier Computer Networks, Volume 53, Nr. 1, S. 81–97, 2009.

[5] Panchenko, Andriy/Niessen, Lukas/Zinnen, Andreas/Engel, Thomas: Website Fingerprinting in Onion Routing- based Anonymization Networks, in: Proceedings of the Workshop on Privacy in the Electronic Society, 2011, S.103– 114.

[6] Herrmann, Dominik/Wendolsky, Rolf/Federrath, Hannes: Website fingerprinting: attacking popular privacy enhancing technologies with the multinomial naïve-bayes classifier, in CCSW '09: Proceedings of the 2009 ACM workshop on Cloud computing security. New York, NY: ACM, 2009, S. 31 – 42.

[7] Bernaille, Laurent/Teixeira, Renata: Early recognition of encrypted applications, in: Proceedings of the Eighth Passive and Active Measurement Conference, 2007.

[8] Hjelmvik, Erik: The SPID Algorithm – Statistical Protocol IDentification, URL: http://sourceforge.net/apps/mediawiki/spid/index.php?title=Main_Page [8.2.2014].

[9] Ipoque: Supported Protocols and Applications, URL: http://www.ipoque.com/sites/default/files/mediafiles/documents/data-sheet-supported-protocols.pdf [8.2.2014].

[10] Bar-Yanai, Roni/Langberg, Michael/Peleg, David/Roditty, Liam: Realtime Classification for Encrypted Traffic, in: Festa, Paola (Hrsg.): Proceedings of the 9th International Symposium on Experimental Algorithms, (SEA 2010), LNCS 6049, 2010, Berlin, Heidelberg, Springer-Verlag, 2010, S. 373–385.

[11] Procera: PacketLogic Real-Time Enforcement platforms (PRE), http://www.proceranetworks.com/pre-packetlogic-real-time-enforcement.html [8.2.2014]

[12] DE-CIX: Statistiken, http://www.de-cix.net/about/statistics/ [8.2.2014].

[13] Sokolov, Daniel/Ungerer, Bert: Berichte: Iran kappt sichere Internet-Verbindungen, Artikel auf Heise vom 11.2.2012, URL: http://www.heise.de/newsticker/meldung/Berichte-Iran-kappt-sichere-Internet-Verbindungen-1432960.html [8.2.2014].

[14] Houmansadr, Amir/Borisov, Nikita: SWIRL: A scalable watermark to detect correlated network flows, in: Proc. NDSS, 2011.

[15] Wright, Charles V./Coull, Scott E./ Monrose, Fabian: Traffic Morphing: An Efficient Defense Against Statistical Traffic Analysis, in: Proceedings of the 16th Network and Distributed Security Symposium, S. 237 – 250. IEEE, 2009.

[16] Basso, Simone/Servetti, Antonio/De Martin, Juan Carlos: The network neutrality bot architecture: a preliminary approach for self-monitoring of Internet access QoS, in: Proceedings of the 16th IEEE Symposium on Computers and Communications (ISCC), 2011, S. 1131–1136.

[17] Kanuparthy, Partha/Dovrolis, Constantine: Diffprobe: detecting ISP service discrimination, in: INFOCOM, 2010 Proceedings IEEE, 2010, pp. 1–9.

[18] Dischinger, Marcel/Marcon, Massimiliano/Guha, Saikat/ Gummadi, Krishna P./Mahajan, Ratul/Saroiu, Stefan: Glasnost: Enabling End Users to Detect Traffic Differentiation, in: Proceedings of the 7th USENIX conference on Networked systems design and implementation, 2010.

[19] Durner zu Art. 10 GG in: Epping, Volker/Hillgruber, Christian (Hrsg.): Beck'scher Online-Kommentar GG, München: Springer Verlag, Edition 13, 2012.

[20] Gusy, Christoph: Gewährleistung der Vertraulichkeit und Integrität informationstechnischer Systeme, in: Datenschutz und Datensicherheit (DuD), 2009, S. 33-41.

Anmerkungen

1 *Transmission Control Protocol/Internet Protocol.*

2 *Quality-of-Service.*

3 *Grundgesetz für die Bundesrepublik Deutschland in der im Bundesgesetzblatt Teil III, Gliederungsnummer 100-1, veröffentlichten bereinigten Fassung, das zuletzt durch Artikel 1 des Gesetzes vom 11. Juli 2012 (BGBl. I S. 1478) geändert worden ist.*

4 *Telekommunikationsgesetz vom 22. Juni 2004 (BGBl. I S. 1190), das zuletzt durch Artikel 2 des Gesetzes vom 22. Dezember 2011 (BGBl. I S. 2958) geändert worden ist.*

5 *Voice over IP.*

6 *File Transfer Protocol.*

7 *BT-Drs. 16/3078.*

8 *Strafprozessordnung in der Fassung der Bekanntmachung vom 7. April 1987 (BGBl. I S. 1074, 1319), die zuletzt durch Artikel 2 Absatz 30 des Gesetzes vom 22. Dezember 2011 (BGBl. I S. 3044) geändert worden ist.*

Julia Hofmann

FIfF-Studienpreis 2013
3. Preis

Zweckgebundener Datenbrief

für das Identitätsmanagementsystem mittels Web-basiertem Benutzerinterface

Mit der fortgeschrittenen Durchdringung des Alltags mit Web-basierten Computeranwendungen ist beinahe kein Verwaltungsprozess mehr denkbar, ohne dass personenbezogene Daten verarbeitet werden. Mit dem zweckgebundenen Datenbrief können sich Angehörige der TU Darmstadt über ein Web-basiertes Benutzerinterface selbstständig informieren, welche ihrer personenbezogenen Daten für welchen Zweck am Hochschulrechenzentrum verarbeitet werden. Ohne weiteren Schriftverkehr, transparent und tagesaktuell ist so die im Bundesdatenschutzgesetz §34 geforderte Auskunftspflicht umgesetzt. Der technische Datenschutz orientiert sich an den Schutzzielen als Richtschnur für gutes Design (Privacy by Design). Die Schutzziele dienen daher als eine Anleitung, wie die Interessen der TU-Angehörigen zu wahren sind und verbinden damit Gesetz und Technik. Der zweckgebundene Datenbrief wurde an der TU Darmstadt umgesetzt und ist das Ergebnis einer Abschlussarbeit zur Fachinformatikerin Fachrichtung Anwendungsentwicklung an der IHK Darmstadt. Dieser Beitrag erklärt, wie der Datenbrief für die Selbstauskunft technisch realisiert ist.

Die durch das Hochschulrechenzentrum bereitgestellten Dienste nutzen personenbezogene Daten der Menschen an der Technischen Universität Darmstadt. Ziel des zweckgebundenen Datenbriefs ist es, alle Personen darüber zu informieren, welche Daten wozu genutzt werden. Sie sollen nachvollziehen können, zu welchem Zweck ihre Daten verarbeitet werden, und sollen letztlich die Möglichkeit haben, anhand dieser Information zu intervenieren, wenn sie nicht einverstanden sind. Die TU-Angehörigen können den Datenbrief als Web-Anwendung zu jeder Zeit und an jedem Ort mit einem üblichen Web-Browser aufrufen. Das erfüllt auch die Anforderungen an die Systemverantwortlichen, die nach Telemediengesetz §5 und §13 verpflichtet sind, „Informationen leicht erkennbar, unmittelbar erreichbar und ständig verfügbar zu halten" [BMJustizTMG2010].

Identitätsmanagement (IDM) bedeutet die Verwaltung von personenbezogenen Daten für alle Angehörigen der TU Darmstadt. Das Hochschulrechenzentrum (HRZ) übernimmt diese Verwaltung in Vertretung, um geregelte und geschützte verwaltungstechnische Prozesse in IT-Dienstleistungen abzubilden [BT2011]. Die digitale Identität repräsentiert die Summe aller Merkmale, die elektronisch verarbeitet werden. Diese Merkmale sind in der