

Too smart for you? – Anforderungen an den Einsatz von mobilen Informatiksystemen in der Schule

An dieser Stelle möchte ich mich noch einmal beim FIF für die Auszeichnung meiner Examensarbeit¹ bedanken. Im Folgenden möchte ich die Chance ergreifen, die gesellschaftlichen Veränderungen näher zu charakterisieren, die ich in meiner Arbeit im Wesentlichen aus der informatisch-didaktischen Perspektive betrachtet habe. Auf die tatsächliche Umsetzung, die Wahl der Programmiersprache, die Python-Klassenbibliothek und deren didaktische Begründungen gehe ich hier nicht weiter ein.

Ein dominierendes Thema des Jahres 2013 war die von Edward Snowden losgetretene Debatte, die dessen Enthüllung der globalen, digitalen Spionagetätigkeiten der NSA² folgte. Plötzlich wurde einer breiten Öffentlichkeit bewusst, dass flächendeckende Überwachung weder eine wirre Idee von seltsamen Nerds mit Aluhüten auf dem Kopf, noch eine eher theoretische Möglichkeit ist. Vielmehr ist dies – nicht nur seitens der NSA und des britischen GCHQ³ – inzwischen Alltag.

Auch private Akteure strecken beinahe wie gierige Kraken ihre Arme nach den privaten Daten nahezu aller Internetnutzer aus. So weiß nicht nur *Amazon*, was einem gefallen könnte, und kann so in naher Zukunft die Waren absenden, bevor der Kunde überhaupt weiß, dass er sie bestellen will⁴, auch *Google Now* kann dem Smartphonennutzer sofort mitteilen, was dieser als Nächstes zu tun gedenkt und wo er sich voraussichtlich in der nächsten Stunde aufhalten wird.

Die diversen Internetdienste und Apps bringen allesamt nützliche Funktionen mit, die den Anwendern das Leben einfacher machen können. Durch die sich immer weiter verbreitenden mobilen Informatiksysteme (u. a. Smartphones und Tablets) und die nahezu flächendeckende Verfügbarkeit von mobilem Internet sind diese Dienste nicht nur immer verfügbar; vielmehr verliert die Frage ihren Sinn, ob man gerade online ist. Schlagwörter wie *Always-On* oder das „Internet der Dinge“ machen deutlich, wohin die Reise geht.

Dass neben diesen nützlichen Funktionen perfekte, digitale Wanzen in unseren Alltag einzogen, die die flächendeckende Überwachung erst möglich machten, beginnt vielen Menschen erst heute, nach den Veröffentlichungen von Edward Snowden, klar zu werden.

Allgegenwärtige Informatik

In allen modernen Gesellschaften nehmen Informatiksysteme inzwischen einen wichtigen Platz ein. Man findet kaum ein elektrisches Gerät, das ohne Mikroprozessoren und Software auskommt. Selbst Kühlschränke, Toaster und Bügeleisen erfüllen heute die Definition von Informatiksystemen. Mal transparent für den Anwender, indem etwa der Teekessel per WLAN an das Smartphone meldet, wenn das Wasser kocht. Mal weniger transparent, wenn das Bügeleisen das Notebook mit einem Trojaner infiziert⁵.

Unsere Welt ist durchdrungen von Informatik. Überall finden sich Informatiksysteme, ständig sind um uns herum informati-

sche Prinzipien am Werk, laufen Algorithmen ab, die unser Leben für uns – und für Dritte – auswerten und berechenbar machen. Viele davon füttern wir selbst mit Daten, doch noch mehr sind uns im Alltag oft gar nicht bewusst. Die informatischen Systeme werden immer kleiner und unscheinbarer. Wo vor wenigen Jahrzehnten eine Fabrikhalle und noch vor wenigen Jahren ein Desktopcomputer notwendig waren, reicht heute für dieselbe Rechenleistung ein einfaches Smartphone.

Besonders stark sind die Veränderungen an den mobilen Informatiksystemen zu erkennen. Kaum jemand hat heute noch kein Mobiltelefon in der Tasche, die meisten verwenden sogar ein Smartphone, das beständig mit dem Internet verbunden ist. Mobile Datenflattrates machen dies möglich und erschwinglich.

Die sichtbarste gesellschaftliche Veränderung ist die der Kommunikation. Immerwährende Erreichbarkeit und ständig verfügbare globale Kommunikationskanäle haben direkten Einfluss auf das menschliche Verhalten. Sei es die von manchen Sprachforschern gescholtene Veränderung der Sprache (SMS-Sprache), die Hoffnung auf friedlicheres, demokratischeres Zusammenleben oder die Zunahme von Stress, da Beruf und Privatleben durch die ständige Erreichbarkeit nicht mehr klar zu trennen sind⁶.

Ebenso offensichtlich ist der potenzielle Nutzen als universelles Werkzeug. Diese mobilen, digitalen *Schweizer Taschenmesser* sind inzwischen so mit Sensoren vollgestopft, dass es für viele Nutzer eine Freude ist, damit herumzuspielen – dank *Gamification*⁷ im wahrsten Sinne des Wortes. Erweitert werden die Datenerfassungsmöglichkeiten dabei noch um externe Sensoren. Besonders beliebt sind derzeit diverse Fitness- und Gesundheitsgadgets wie Pulsmesser und Schrittzähler.

Die schiere Menge der verfügbaren Daten macht die mobilen Informatiksysteme dank – mal mehr, mal weniger – ausgeklügelter Software zu den persönlichen Assistenten, die schon vor Jahren mit den ersten Generationen der PDAs versprochen wurden. Durch GPS und andere Methoden der Positionsbestimmung, den Abgleich mit Kartenmaterial und den Daten aus dem persönlichen Kalender kennen diese Assistenten uns und unsere Verhaltensweisen und Gewohnheiten teilweise besser als wir uns selbst. Dabei hören sie dank *Siri*, *Google Voice* oder *S-Voice* auf's Wort und das mit verblüffender Genauigkeit. Die nächste Generation der mobilen Geräte steht mit Datenbrillen wie *Google Glass* bereits in den Startlöchern – noch unscheinbarer, nützlicher, allgegenwärtiger und datenhungriger als bisherige Systeme. In Zukunft werden sie wohl direkt Personen, mit denen wir reden, identifizieren können und uns live mit Zusatz-

informationen zu diesen und zu den Gesprächsinhalten versorgen können. Smart, fast magisch.

Doch auf wessen Wort hören die klugen Helferlein eigentlich? Mit wem reden sie? Diese und andere Fragen sind durch die reine Anwendungsperspektive nicht zu klären, sie stellen sich mitunter gar nicht erst. Von außen erscheinen die Systeme als Blackboxen, die mehr oder weniger das tun, was wir von ihnen erwarten. Dass unsere braven Assistenten sich jedoch stetig im Hintergrund mit ihrer jeweiligen Assistentenzentrale beraten, wird erst deutlich, wenn man sich mit dem informatischen Hintergrund beschäftigt. Für den normalen Nutzer wird selten ersichtlich, was die Geräte tatsächlich anstellen, da dies meist alles andere als offensichtlich ist.

Es ist sogar so, dass sich die Hersteller alle Mühe geben durch fortschreitende Simplifizierung entscheidende Aspekte der Funktionsweise vor den Anwendern zu verbergen. Denn schließlich wollen diese doch eigentlich gar nicht wissen, wie es funktioniert! Oder etwa doch? Nein, denn sie haben es nicht zu wollen. Neugierige Blicke werden durch technische und juristische Kunstgriffe gezielt abgelenkt. Bei Verstößen drohen Verlust von Garantie oder Benutzerkonten, inklusive gekaufter Inhalte.

So würde man für gewöhnlich kaum vermuten, dass das Verschönern eines Fotos mit lustigen Effekten voraussetzt, dass dieses Foto zunächst auf den Server des Anbieters geladen wird und sich dieser in seinen AGBs sämtliche Nutzungsrechte dafür einräumen lässt. Ebenso zeigen sich viele Nutzer überrascht, dass die elektronische Kommunikation mit ihren Freunden und Bekannten auf den Servern der Anbieter landet und von diesen ausgewertet werden kann, da dies den bekannten und erprobten Kommunikationskonzepten aus dem Alltag nicht entspricht. Mögliche Risiken lassen sich dabei durch die Nutzer selten richtig einschätzen, da die notwendigen informatischen Grundlagen fehlen. Fordert ein kostenloses Spiel für ein Smartphone den Zugriff auf Kalender- und Kontaktdaten und gleichzeitig vollen Internetzugang an, so reagieren viele Anwender nicht skeptisch, sondern mit einem Klick auf ‚Ok‘. Skepsis tritt höchstens im Nachhinein auf, wenn man feststellt, dass die smarten Gadgets in der Grundkonfiguration bereits alle Daten in die Cloud synchronisiert haben.

Die Hersteller der Geräte bzw. die Betreiber der zugrunde liegenden Dienste erhalten also einen Informationsvorsprung gegenüber den Anwendern. Zusätzlich geraten letztere in eine Abhängigkeitsfalle gegenüber ersteren. Dies sieht man am Lock-In bei den verschiedenen Smartphone-Plattformen: Wer die Plattform wechselt, verliert alle Investitionen, die bisher getätigt wurden. Gekaufte Apps sind nicht mehr nutzbar, kopiergeschützte Medien auf der anderen Plattform nicht mehr verfügbar und gekaufte Zusatzhardware ist oft schlicht nicht kompatibel. Noch deutlicher wird dies bei sozialen Kommunikationsplattformen: Man muss eine Plattform nicht nutzen, doch wenn die sozialen Kontakte zum Beispiel *Facebook* oder *Whatsapp* verwenden, verliert man beim Verzicht auf diese Dienste den Anschluss.

Es droht also ein Verlust an Selbstbestimmung zugunsten nützlicher Unterstützung. Ein Teil unseres Denkens geben wir an smarte Gadgets ab, die dies doch soviel effizienter erledigen als wir. Zusätzlich bezahlen wir diesen Service mit unseren privaten

Daten. Dies geht natürlich mit dem Verlust von Freiheit einher, was durch die Möglichkeit zur Totalüberwachung durch die Anbieter der entsprechenden Plattformen und aller anderen, die Zugriff auf die anfallenden Daten erlangen, verstärkt wird.

Sind diese mobilen Informatiksysteme somit vielleicht sogar zu smart für uns? Oder stellt sich die Frage nach einer mündigen, aufgeklärten Teilhabe an der Gesellschaft gar nicht mehr, wenn mein Smartphone doch genau weiß, was ich wo und auf welche Weise als Nächstes tun sollte?

Ein – notwendiger – breiter gesellschaftlicher Diskurs, der den gesellschaftlichen Veränderungen Rechnung trägt, findet hier jedenfalls nicht statt. Bestenfalls werden Teilaspekte wie einzelne Facetten des Datenschutzes erörtert.

Notwendigkeit informatischer Bildung

Aus meiner Sicht ist es zwingend erforderlich, sich über die reine Anwendungsperspektive hinaus zu erheben, will man nicht Jahrhunderte gesellschaftlicher Entwicklung und Aufklärung verwerfen. Die reine Anwendungssicht wird der Realität der allgegenwärtigen Informatik nicht gerecht. Vielmehr kostet sie letztlich die Selbstbestimmtheit der handelnden Akteure. Wie schon Goethe schrieb: „Was man nicht versteht besitzt man nicht.“

Es ist zwingend notwendig, Menschen in die Lage zu versetzen, moderne Informatiksysteme selbstbestimmt und verantwortungsbewusst zu verwenden und die mit Ihnen verbundenen Risiken und Nebenwirkungen einschätzen zu können, ohne zunächst den Informatiker ihres Vertrauens zu befragen, will man die mündige Teilhabe in demokratischen Gesellschaften sicherstellen.

Aktueller Stand in der Schule

Besonders bei Kindern und Jugendlichen sind die gesellschaftlichen Veränderungen längst angekommen⁸. Es findet sich kaum eine Klasse, in der nicht die große Mehrheit der Schülerinnen und Schüler über Smartphones verfügt. Doch von bewusster und mündiger Nutzung kann hier nur selten die Rede sein. Das ist natürlich nur logisch, denn nirgendwo wird dieser bewusste Umgang tatsächlich vermittelt.

Jeder Mensch müsste heute über eine grundlegende informatische Vernunft⁹ verfügen, die weit über reines Anwendungswissen hinausgeht. Natürlich fällt diese nicht vom Himmel, sondern muss sich zunächst entwickeln. Hier sind die bestehenden Bildungsinstitutionen gefragt, allen voran die allgemeinbildenden Schulen. Doch leider findet an vielen Schulen kein geregelter und zielgerichteter Informatikunterricht statt, der die notwendigen Anforderungen zur Entwicklung informatischer Vernunft erfüllen kann. Informatik ist nur in wenigen Bundesländern ein Pflichtfach und es mangelt an ausgebildeten Lehrkräften. Wenn überhaupt Informatik unterrichtet wird, handelt es sich oft um einseitige Computernutzungs- oder Programmierkurse. Erstere verharren wiederum in der reinen Anwendungsperspektive, letztere verlieren viel zu häufig den Anspruch der allgemeinen Bildung aus den Augen und beschränken sich darauf, gute

Programmierer hervorzubringen¹⁰. Beide sind damit zu einseitig aufgestellt, um dem Ziel der Entwicklung informatischer Verunft zu dienen.

Nebenbei vermittelt der Informatikunterricht häufig ein falsches Bild von Informatik, da die exklusive Nutzung von Computerräumen den Eindruck zementiert, dass sich die Informatik nur mit Computern beschäftigen würde. Außerdem stehen die räumlich festgelegten Computerarbeitsplätze moderneren Unterrichtsformen im Weg und erschweren oftmals die wichtige Kommunikation zwischen den Schülerinnen und Schülern.

Die Nutzung mobiler Informatiksysteme verspricht hier Abhilfe zu schaffen und den Informatikunterricht zu flexibilisieren sowie Fehlvorstellungen entgegenzuwirken. Die häufigste Reaktion auf die gesellschaftlichen Veränderungen durch die Verfügbarkeit mobiler Informatiksysteme ist jedoch – keine. Die zweithäufigste ist die Einführung von Verboten. Natürlich ist es nicht die Aufgabe der Schule, Modetrends hinterherzulaufen, jedoch zeichnet sich deutlich ab, dass klassische Informatiksysteme an Bedeutung verlieren¹¹.

Erfolgt die Nutzung von mobilen Informatiksystemen im Unterricht, wie es in Leuchtturmprojekten und an einzelnen Schulen geschieht, so wird diese häufig von überbordendem Enthusiasmus und größtenteils unkritisch begleitet. Dies wird von den Herstellern von Konsumgeräten vorangetrieben, so strebt etwa Apple an die Schulen¹² und umwirbt diese mit speziellen Angeboten und Inhalten. Das Verlassen der Anwendungsperspektive unterbleibt.

Bisherige Ansätze

Jenseits der Informatik beschränkt sich die Beschäftigung mit den mobilen Informatiksystemen leider allzu häufig auf reine Klickanleitungen, begrenzte, künstliche Lernumgebungen¹³ oder Informationsbroschüren für Eltern, Lehrer und Schüler, die oft sehr einseitig auf die möglichen Gefahren ausgerichtet sind und kaum hilfreiche Handlungsalternativen anbieten. Natürlich kann man Schülerinnen und Schülern raten, bei der Nutzung sozialer Kommunikationsplattformen besonders zurückhaltend zu sein. Besonders sinnvoll ist dies jedoch nicht, denn hier wirkt sich der oben beschriebene Lock-In-Effekt besonders deutlich aus: Wer online nicht dabei ist, verpasst den Anschluss.

Hilfreiche Handlungsalternativen zu geben, ist auf einer anwendungsorientierten Ebene nur schwer möglich, da – wie bereits erwähnt – der notwendige informatische Hintergrund fehlt. Doch was man nicht versteht, kann man nicht sinnvoll anwenden.

Es gibt einige Beiträge aus der Informatik-Fachdidaktik, die den Einsatz von mobilen Informatiksystemen untersuchen. Hervorzuheben sind besonders die Arbeiten von Ralph Carrie¹⁴, Matthias Heming¹⁵ sowie die Beiträge und Pilotkurse von Ludger Humbert¹⁶.

Matthias Heming zeigte in seiner Arbeit, dass ein Informatikunterricht, der auf Mobiltelefone als einzige Informatiksysteme setzt, nicht nur möglich ist, sondern auch den Bildungsstandards

der Gesellschaft für Informatik (GI) für die Sekundarstufe I als auch den Vorgaben und Anforderungen des Zentralabiturs in NRW genügt.

Es wurden auch erste Konzepte zum Einsatz mobiler Informatiksysteme im Informatikunterricht entwickelt, die später weiterentwickelt und in mehreren Kursen an der Willy-Brandt-Gesamtschule in Bergkamen erprobt wurden. Dabei entstanden auch umfangreiche Unterrichtsmaterialien¹⁷, die aufgrund ihrer Ausrichtung auf das nicht mehr verfügbare Symbian OS leider nur noch begrenzt anwendbar sind.

Die Erfahrungen hiermit waren insgesamt sehr gut. Die Lernziele wurden erfolgreich erreicht und der Unterricht war für die Schülerinnen und Schüler motivierend und spannend.

Kriterien für den Einsatz mobiler Informatiksysteme

Ein wesentlicher Teil meiner Arbeit war die Suche nach Kriterien für den Einsatz mobiler Informatiksysteme im Informatikunterricht. Die grundlegenden Anforderungen erscheinen dabei zunächst offensichtlich: Die Geräte müssen grundsätzlich sinnvoll in den Unterricht eingebunden werden können und – speziell für den Informatikunterricht – programmierbar sein. Prinzipiell sollten dies fast alle heutigen mobilen Informatiksysteme erfüllen¹⁸, allerdings errichten die Hersteller hier unterschiedlich hohe Hürden technischer und rechtlicher Natur. So benötigt man teilweise teure Lizenzen oder spezielle Hard- und Software für die Programmierung. Sie verbieten teilweise auch die Programmierung der Geräte mit den Geräten selbst, sodass zusätzliche Informatiksysteme benötigt werden. Dies verhindert einen Großteil der möglichen Flexibilisierung des Unterrichts, da man weiterhin an Informatikräume gebunden wäre. Außerdem werden wesentliche Aspekte der Betriebssysteme vor dem Nutzer versteckt – etwa die Dateisysteme, sodass ein Verlassen der Anwendungsperspektive unmöglich gemacht wird. Speziell Apple ist hier für derartige Einschränkungen bekannt.

In diesem Sinne ist es wünschenswert, dass die Geräte freie Software verwenden. Denn hier ist es am ehesten möglich, alle Anforderungen zu erfüllen und künstlichen Einschränkungen zu entgehen. Außerdem kann benötigte Software in der Regel ohne relevante Einschränkungen und Kosten an die Schülerinnen und Schüler weitergegeben werden, sodass diese auch zuhause mit den Geräten arbeiten können.

Eine hohe Verbreitung der Plattform ist aus zwei Gründen unerlässlich: Erstens sollten die Geräte sich im Alltag der Schülerinnen und Schüler wiederfinden lassen, zweitens ist nur so eine breite Unterstützung und die Verfügbarkeit entsprechender Werkzeuge und Dokumentationen wahrscheinlich.

Der Motivation zuträglich ist es, wenn auf die Geräte der Schülerinnen und Schüler zurückgegriffen werden kann. Nichtsdestotrotz ist es erforderlich, dass eine gewisse Menge an schulischen Geräten zur Verfügung steht, damit Schülerinnen und Schüler ohne eigene Geräte mitarbeiten können und nicht etwa auf Emulatoren angewiesen sind. Außerdem muss darauf geachtet werden, dass Schülerinnen und Schüler, die über teurere

und besser ausgestattete Systeme verfügen, keine übermäßigen Vorteile erlangen.

Spezielle Anforderungen gelten auch in Bezug auf die Haltbarkeit der Geräte. Aus finanziellen wie aus Umweltschutzgründen sollte hierauf viel Wert gelegt werden. So kann bereits ein fest verbauter Akku einer dauerhaften, langfristigen Nutzung in der Schule entgegenstehen.

Unabhängig davon sollte die Schule sich ihrer Vorbildfunktion bewusst sein und generell soziale wie auch Umweltschutzaspekte berücksichtigen, sofern dies möglich ist.

Folgerungen und Forderungen

Die gesetzten Kriterien zu erfüllen, ist aktuell nicht ganz einfach. Am ehesten sind sie mit Android-Geräten zu erfüllen, die glücklicherweise momentan die höchste Verbreitung bei Schülerinnen und Schülern aufweisen.

Windows-Systeme sind zwar (je nach Version unterschiedlich stark) eingeschränkt, könnten jedoch mutmaßlich sinnstiftend genutzt werden. Die (noch) sehr geringe Verbreitung macht allerdings entsprechende Überlegungen derzeit weitgehend überflüssig.

Es besteht zudem die Hoffnung, dass weitere offene Systeme einen relevanten Verbreitungsgrad erreichen können. Hier sind etwa Sailfish OS, Tizen oder Firefox OS zu nennen. Diese haben durchaus das Potential, die Kriterien besser zu erfüllen als Android.

Völlig ungeeignet sind hingegen rein auf den Konsum gerichtete Plattformen wie Amazons Kindle oder Apples iOS. Hier sollten Informatiklehrkräfte dringend Widerstand leisten, sollte die Einführung derartiger Systeme an ihren Schulen zur Debatte stehen.

Die Erfahrung mit Symbian OS zeigt, dass nach Möglichkeit ein plattformübergreifender Wrapper als Schnittstelle entwickelt werden sollte, sodass bestehende Unterrichtsmaterialien in Zukunft weiterverwendet werden können. Diesen Weg habe ich im Rahmen meiner Arbeit eingeschlagen und gehe ihn jetzt in meinem Referendariat weiter.

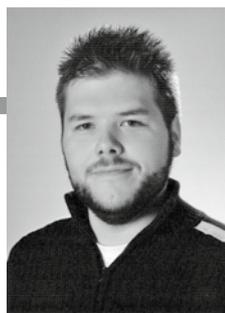
Die gesellschaftsverändernden Systeme sollten auf die eine oder andere Weise in der Schule berücksichtigt werden. Dies kann am ehesten im Rahmen eines verpflichtenden Informatikunterrichts

geleistet werden, der diesem Namen gerecht wird (auch und insbesondere in den unteren Jahrgängen).

Dabei ist darauf zu achten, dass nicht nur die reine Anwendungsperspektive, sondern auch die Analyse und die Veränderung von Wirklichkeit¹⁹ berücksichtigt werden. So kann nicht nur der allgemeinbildende Anspruch und das Ziel der mündigen Gesellschaftsangehörigen erreicht werden, sondern auch ein Beitrag zu einem aktuellen, motivierenden und zielgerichteten Informatikunterricht geleistet werden.

Anmerkungen

- 1 Daniel Spittank: *Auswahl und Gestaltung mobiler Informatiksysteme für den Einsatz im Informatikunterricht. Masterarbeit – Master of Education. Wuppertal: Bergische Universität – Fachbereich Mathematik und Naturwissenschaften, August 2012.* <https://edu.spittank.net/downloads/mobile/examensarbeit.pdf>.
- 2 National Security Agency, *Auslandsgeheimdienst der USA*
- 3 *Government Communications Headquarters, britischer Nachrichtendienst*
- 4 vgl. Spiegel u. a.: *Method and system for anticipatory package shipping. US 8,615,473. 24. Dezember 2013.* <http://pdfpiw.uspto.gov/piw?Docid=08615473>.
- 5 BBC. *Russia: Hidden chips ,launch spam attacks from irons'.* en. BBC. Oktober 2013. <http://www.bbc.co.uk/news/24707337>.
- 6 vgl. DGB. *Arbeitshetze, Arbeitsintensivierung, Entgrenzung – So beurteilen die Beschäftigten die Lage.* März 2012.
- 7 Sebastian Deterding u. a. *Gamication: Toward a Definition.* Mai 2011. <http://hci.usask.ca/uploads/219-02-Deterding,-Khaled,-Nacke,-Dixon.pdf>.
- 8 vgl. MPFS. *JIM 2013. Jugend, Information, (Multi-)Media. Basisuntersuchung zum Medienumgang 12- bis 19-Jähriger in Deutschland. Forschungsbericht. MPFS – Medienpädagogischer Forschungsverbund Südwest. Stuttgart: mpfs, November 2013.* <http://www.mpfs.de/fileadmin/JIM-pdf13/JIMStudie2013.pdf>.
- 9 vgl. Christian F. Görlich und Ludger Humbert: *Open Source – die Rückkehr der Utopie? In: Open Source Jahrbuch 2005. Zwischen Softwareentwicklung und Gesellschaftsmodell. 2005, S. 311-327.* http://www.opensourcejahrbuch.de/download/jb2005/OpenSourceJahrbuch2005_online.pdf, S. 311.
- 10 vgl. Ludger Humbert: *Schüler brauchen keine Entwicklungsumgebung – ein Editor reicht aus. In: If Fase 2.13 (November 2006), S. 2.* <http://humbert.in.hagen.de/iffase/Artikel/programmieren-2006-11-01.html>.
- 11 vgl. TMS-Infratest u. a.: *Our Mobile Planet Survey.* Hrsg. von Inc. Google. geprüft: 7. Juli 2012. Mountain View, CA, USA, 2012. <http://www.thinkwithgoogle.com/mobileplanet/de>.



Daniel Spittank

Daniel Spittank studierte bis 2013 an der Bergischen Universität Wuppertal Informatik und Sozialwissenschaften für das Lehramt an Gymnasien und Gesamtschulen. Im Rahmen des ersten Staatsexamens schrieb er seine Abschlussarbeit zum Einsatz von mobilen Informatiksystemen im Informatikunterricht. Derzeit absolviert er sein Referendariat und setzt die begonnene Arbeit fort.

- 12 Tarik Ahmia. Apple wird zum Bildungsmoloch. Januar 2012. <http://werkstatt.bpb.de/2012/01/apple-wird-zum-bildungs-moloch/>.
- 13 In der Regel sind dies bestimmte Apps oder Webseiten, die genau einer Unterrichtseinheit oder -reihe dienen, dabei aber häufig einen recht gezwungenen Eindruck vermitteln. Medieneinsatz um der Medien willen.
- 14 Ralph Carrie: Einsatz mobiler Informatiksysteme im Informatikunterricht der gymnasialen Oberstufe. Hausarbeit gem a OVP. Hamm: Studienseminar für Lehrämter an Schulen – Seminar für das Lehramt für Gymnasien Gesamtschulen, Juli 2006. <http://www.ham.nw.schule.de/pub/bscw.cgi/315319>.
- 15 Matthias Heming: Einsatzszenarien von Mobiltelefonen im Informatikunterricht. Masterarbeit – Master of Education. Wuppertal: Bergische Universität – Fachbereich Mathematik und Naturwissenschaften, November 2009. <http://blog.familie-heming.de/?p=111>.
- 16 Ludger Humbert: Mit Python auf dem Mobiltelefon bis ins Zentralabitor. April 2007. <http://humbert.in.hagen.de/iffase/Artikel/programieren-2007-04-01.html>.
- 17 vgl. Heming, a. a. O.
- 18 ebd.
- 19 vgl. Spittank, a. a. O., S. 32 f.



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 sich diese Ziele zur Bewertung der Technik und den juristischen Schutzziele. Wesentlichen wurden Integrität, Vertraulichkeit und Unverkettbarkeit als Metrik bei der Bewertung von Paketanalysemethoden 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/IP¹-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 Verschleiерungsmechanismen (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 Verschleiерung an. Verschlüsselt man die eigentlich übertragenen Protokolle auf der Anwendungsebene, sind die Daten nicht mehr sichtbar. Dennoch geben jedoch genug Informationen über die Daten und damit Klassifikatoren erstellt werden können. SPI 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 Verschleiерungsmechanismen 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 Verschleiерung 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-

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