Die technische Seite des NSA/Snowden-Skandals

Stefanie Ziltener und Christoph Schwizer
stefanie.ziltener@uzh.ch, christoph.schwizer@uzh.ch
Universität Zürich, Institut für Informatik

Zusammenfassung. Die Enthüllung von geheimdienstlichen Dokumenten durch Edward Snowden im Sommer 2013 gewährte der Öffentlichkeit Einblicke in die Tätigkeiten verschiedener Geheimdienste, insbesondere der NSA. Diese Arbeit stellt die wichtigsten Programme, die aufgedeckt wurden, vor und erklärt, wie technischer Fortschritt und gesellschaftliche Veränderungen die Tätigkeiten der NSA beeinflusst haben.

1 Einleitung

(Christoph)

Die National Security Agency (NSA) ist ein amerikanischer Geheimdienst mit dem Auftrag, nachrichtendienstliche Informationen zu sammeln und zu verarbeiten [1]. Dafür macht sie sich viele Mittel zu Nutze, die aber meist geheim bleiben oder erst veröffentlicht werden, wenn sie schon veraltet und seit Jahrzehnten nicht mehr im Dienst sind. Die einzige Gelegenheit, welche die Allgemeinheit hat, um einen Blick in aktuelle Programme der NSA zu erlangen, bieten Whistleblower. Leute also, die für die NSA gearbeitet haben und über deren Praktiken Auskunft geben oder geheime Dokumente veröffentlichen. Eine der grössten solchen Enthüllungen geht zurück auf Edward Snowden, einen ehemaligen NSA-Systemadministrator, der NSA-interne Unterlagen an die britische Zeitung *The Guardian* und die amerikanische Zeitung *The Washington Post* übergab, welche einen Teil davon im Sommer 2013 veröffentlichten. Die Unterlagen geben Details über Programme, welche die NSA verfolgt, bekannt. Diese Arbeit soll einen Überblick geben über die wichtigsten Überwachungstechnologien der NSA, die im Zusammenhang mit dem Snowden-Skandal ans Licht gekommen sind, und versucht zu erörtern, wie technischer Fortschritt die Vorgehensweise der NSA verändert haben.

2 PRISM

(Christoph)

Ein Programm, dessen Aufdeckung besonders hohe Wellen schlug, war PRISM. Den Grund dafür nennt die Washington Post und bezeichnet es als die reichhaltigsten Depots an persönlicher Information der Geschichte: “PRISM draws from data held by Google, Yahoo, Microsoft and other Silicon Valley giants, collectively the *richest depositories of personal information in history*” [3]. Selbst die NSA nennt es in der von Snowden veröffentlichten Präsentation “eines der wertvollsten, einzigartigsten und produktivsten Zugriffe für die NSA” [2].

PRISM ermöglicht es der NSA, auf die Daten von neun führenden Internetkonzernen (Microsoft, Google, Yahoo, Facebook, PalTalk, YouTube, Skype, AOL und Apple) zuzugreifen. Es erlaubt dabei ”direkten Zugriff auf die Server der Konzerne” [2]. Die genaue Funktionsweise der Datengewinnung und deren Ausmass hängen von den einzelnen Internetkonzernen und deren Diensten ab. Aus den NSA-Dokumenten geht hervor, dass Analysten unter anderem Zugang zu E-Mails, Video- und Voice-Chats, gespeicherten Dateien sowie Aktivitäten auf sozialen Netzwerken haben. Viele Anfragen werden in Echtzeit bearbeitet: “Noch während Sie eine E-Mail tippen, bevor Sie sie abschicken, bei manchen Programmen bevor die Mail verschlüsselt wird, kann ich sie sehen”, erwähnt Thomas Drake, ehemaliger NSA-Mitarbeiter, in einem Interview [4]. Bei Facebook soll es zudem möglich sein, “vollen Zugriff auf Facebooks extensive Such- und Überwachungsfunktionen [...] zu erlangen” [3]. Ausserdem steht in PRISM eine Benachrichtigungsfunktion zur Verfügung, welche gewisse Aktivitäten einer Interessensperson (z.B. eine Anmeldung an einem Konto oder den Verbindungsaufbau zu einem Chat) meldet.

Das Ganze geschieht, “ohne die Dienstanbieter dazu auffordern zu müssen und ohne einzelne gerichtliche Beschlüsse einholen zu müssen” [2]. Beachtlich ist bei PRISM auch, dass nicht wie bei anderen NSA-Programmen nur Metadaten, sondern der tatsächliche Inhalt der Daten eingesehen werden kann.

Obwohl von Vertretern der involvierten Unternehmen dementiert (“We have never heard of PRISM”, Steve Dowling, Apple Pressesprecher, [3]) oder zumindest stark relativiert (“[...] we carefully scrutinize any such request [...] and provide information only to the extent required by law“, Joe Sullivan, Chief Security Officer von Facebook, [3]), ist von einer engen Zusammenarbeit der genannten Unternehmen mit der NSA auszugehen: “The NSA document notes the operations have 'assistance of communications providers in the US' ” [2].

3 Upstream, TEMPORA und Five Eyes

(Christoph)

Neben PRISM verfolgt die NSA einen weiteren Ansatz, die Internetkommunikation zu überwachen. Unter dem Stichwort “upstream” betreibt sie vier Programme, welche Datenströme in Unterseekabeln abfangen. Diese Kabel, welche heute aus Glasfaser bestehen, verbinden die Kontinente miteinander und ermöglichen die weltweite Internet- und Telekommunikation. Damit erlangt die NSA nicht nur Zugriff auf den Grossteil des Internettraffics, sondern ebenfalls auf Telefonverbindungen. Nachdem die Daten abgefangen wurden, werden sie zur NSA weitergeleitet, wo sie mit einem Data Mining Tool analysiert werden [6]. Damit können zum Beispiel alle E-Mails einer bestimmten Zielperson und deren Empfänger abgerufen werden (vgl. Abschnitt 4 XKeyscore (Stefanie)). Das Geheimdienst-Programm, das in diesem Zusammenhang am meisten genannt wird, ist FAIRVIEW. Hierbei arbeitet die NSA laut The Guardian mit einer grossen US-Telekommunikationsfirma zusammen, welche wiederum mit ausländischen Telekomfirmen kooperiert und so den Zugriff auf Telekommunikationsnetzwerke im Ausland ermöglicht: “[...] the NSA partners with a large US telecommunications company [...] and that US company then partners with telecoms in the foreign countries. Those partnerships allow the US company access to those countries' telecommunications systems” [7].

Abb. 1: Die Folie zeigt einen Überblick über PRISM und die Upstream Programme. Im Hintergrund sind die Verbindungen über Unterseekabel angedeutet.[2]

Ein ähnliches Programm betreibt der britische Nachrichtendienst GCHQ unter dem Codenamen TEMPORA. In geheimen Abkommen mit Privatunternehmen, sogenannten “intercept partners”, werden massenweise transatlantische Glasfaserkabel angezapft, mit dem Ziel, “alles zu sammeln” [8]. Aus den Snowden-Unterlagen geht hervor, dass zum Zeitpunkt Sommer 2011 mehr als 200 Kabel und täglich 600 Millionen “Telefonereignisse” abgehört wurden [8]. Im Zusammenhang mit TEMPORA verwendete Internetpuffer erlauben es dem GCHQ, Inhalte während drei, Metadaten gar während 30 Tagen zu speichern. Um uninteressante Informationen zu filtern und die Datenmenge zu reduzieren, werden die Rohdaten von Rechenzentren analysiert, bevor sie gespeichert werden. Dabei kommen “Selektoren”, eine Art Suchbegriffe, zum Einsatz, welche vom GCHQ und der NSA festgelegt werden. Das können beispielsweise Telefonnummern oder E-Mail-Adressen sein, die von Interesse sind, oder auch Schlüsselwörter.

Da die Geheimdienste eingeschränkt sind auf das Anzapfen der Unterseekabel, die an ihr eigenes Land führen, wird eine weltweite Überwachung erst durch Zusammenarbeit mit anderen Geheimdiensten möglich. Die USA und das Vereinigte Königreich haben schon seit Nachkriegszeiten Abkommen zur nachrichtendienstlichen Kooperation [13]. Im Verlaufe der Zeit sind die Geheimdienste von Australien, Kanada und Neuseeland dazugestossen und bilden zusammen die “Five Eyes”, eine nachrichtendienstliche Allianz.

4 XKeyscore

(Stefanie)

XKeyscore ist ein Programm der NSA, das verschiedene Zwecke hat. Zum einen ist es eine Datenbank. XKeyscore speichert Metadaten wie beispielsweise E-Mail- oder IP-Adressen und Zeitstempel. Zusätzlich speichert es andere Daten wie E-Mail Inhalte, Chat-Gespräche, Freundeslisten und weiteres einer Session im Internet. Laut The Guardian speichert es so “ziemlich alles (in Echtzeit), was ein normaler User im Internet tut”: “One presentation claims the program covers 'nearly everything a typical user does on the internet', including the content of emails, websites visited and searches, as well as their metadata” [9].

Natürlich ist die Datenmenge zu gross, um sie komplett und dauerhaft zu speichern. Des Weiteren sind viele Daten gar nicht interessant für die NSA. Die Daten können angeblich 3 bis zu 5 Tage und Metadaten für 30 Tage gespeichert werden. Analysten der NSA können jedoch 'interessante' Inhalte in anderen Datenbanken abspeichern, wo sie bis zu 5 Jahren liegen bleiben können [9].

Weiter kann XKeyscore auch dazu benutzt werden, die gesammelten Daten zu durchsuchen. Dies wird mithilfe von Data Mining gemacht, womit grosse Datenmengen verarbeitet und Zusammenhänge statistisch analysiert werden können. Die NSA-Analysten können mit der Angabe spezifischer Informationen, zum Beispiel der Name einer Zielperson oder ihrer E-Mail Adresse, alle zugehörigen Daten mit einem Klick finden. Darunter gehören: “[...] Nutzernamen, Freundeslisten und Cookies in Verbindung mit Webmail und [können auf] Chats eines Nutzers zugreifen oder auf Google-Suchanfragen [...]” [10]. Für diese Art der Überprüfung ist keine offizielle Genehmigung von Nöten (wenn die überprüfte Person kein Amerikaner ist), eine grobe Angabe eines Grundes bei der Suchanfrage ist dafür schon genug: ”One document [...] explains that analysts can begin surveillance on anyone by clicking a few simple pull-down menus designed to provide both legal and targeting justifications” [9].

Beachtenswert ist hierbei nicht nur das Ausmass der Sammlung an Daten (“In 2012, there were at least 41 billion total records collected and stored in XKeyscore for a single 30-day period.” [9]), sondern auch, dass man diese Daten effizient durchsuchen kann. Natürlich können wir nur über den tatsächlichen Umfang dieses Programms spekulieren, da es für die Öffentlichkeit nicht vollständig transparent ist und vermutlich auch nie sein wird. Doch scheint es mit heutigem Wissen eher realistisch, auch im Bezug darauf, dass Snowdens Informationen schon beinahe wieder veraltet sind, in grösseren Dimensionen zu denken.

5 Boundless Informant

(Stefanie)

Boundless Informant ist ein Programm, das die gesammelten Daten der NSA katalogisiert. Wie man auf der Abbildung 2 sehen kann, bestimmt es unter anderem die Menge an Daten, die aus einem Land gesammelt wurden. Wie man sieht, sind vor allem die Vereinigten Staaten im Vergleich zu ihren Nachbarländern oder zu Südeuropa relativ stark von der NSA überwacht (in dem Sinne, dass viele Daten gesammelt werden). Boundless Informant nutzt Metadaten um Geräte zu lokalisieren. IP-Adressen sind beispielsweise keine genauen

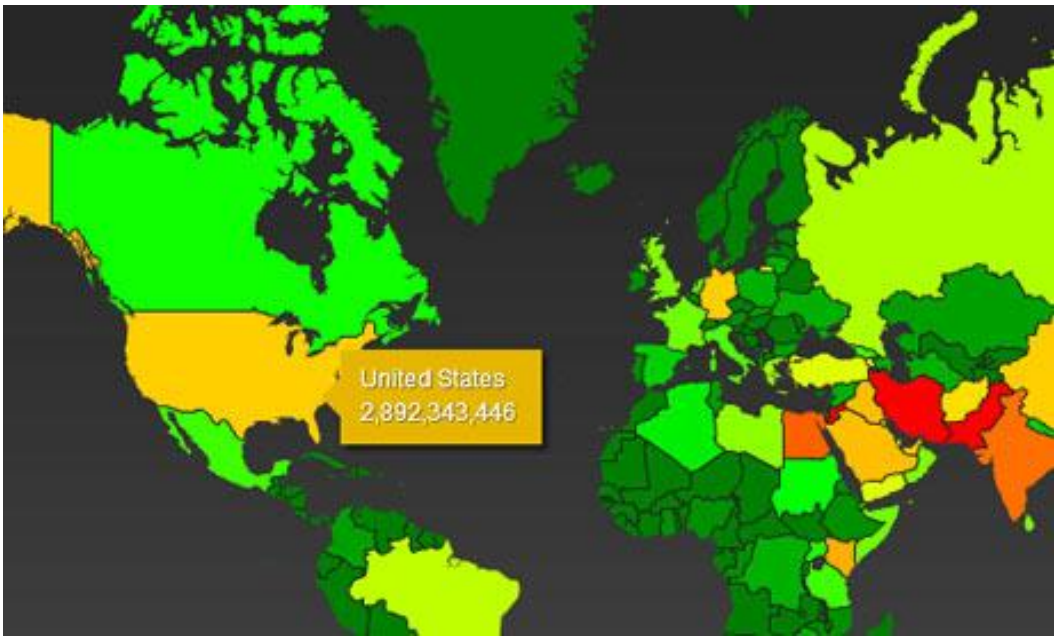

Abb. 2: Das Farbspektrum reicht von grün (wenige Daten gesammelt) bis zu rot (die grösste Sammlung). [18]

Indikatoren für den Standort, jedoch kann man über sie das Ursprungsland und die ungefähre Region eines Endgeräts bestimmen.

Das Interessante an diesem Programm ist, dass die NSA seit Beginn des Snowden-Skandals immer wieder versichert hat, dass sie nicht mit Sicherheit bestimmen kann, woher ihre Überwachungsdaten stammen. Des Weiteren sagt die NSA aus, dass sie den Standort des jeweiligen Kommunikationspartners ebenfalls nicht bestimmen kann. Die Informationen, die Boundless Informant uns zeigt, deuten etwas anderes an [18].

6 Kryptographie / Kryptoanalysis

(Stefanie)

Die NSA nutzt verschiedene Mittel, um an kryptographischen Verschlüsslungen vorbeizukommen, sie zu brechen oder von vornherein zu untergraben. Dies vermuteten Experten der Internet-/Netzwerk-Sicherheit schon lange: “Independent security experts have long suspected that the NSA has been introducing weaknesses into security standards, a fact confirmed for the first time by another secret document” [17]. Mit den Snowden-Files und weiteren darauf folgenden Ermittlungen aber hat man nun eine gewisse Vorstellung, wie weit dies geht.

Eine Möglichkeit, Verschlüsselung zu umgehen, ist, sie erst gar nicht zuzulassen: Das ist machbar, wenn die Nachricht vor der Verschlüsselung abgefangen werden kann. Eine weitere, naheliegende Möglichkeit ist es, die Daten auf der Empfängerseite nach der Entschlüsselung zu kopieren. Natürlich benutzt die NSA auch Supercomputer, um gewisse, kritische Verschlüsselungen zu knacken, und benutzt dabei auch ihr Wissen über eventuelle Schwächen in kryptologischen Verfahren [14].

Es wurde auch bekannt, dass die NSA daran arbeitet, die Sicherheitsmassnahmen in Virtual Private Networks (VPNs), Voice-over-IP und 4G-Netze für Smartphones zu umgehen, um an die dort ausgetauschten Daten zu kommen [14].

Die NSA nimmt ebenfalls Einfluss auf Entscheidungen bei Designfragen in kryptographischen Standards. Ein konkretes Beispiel: “Die NSA baute eine Backdoor direkt in einen Standard für einen Pseudo-Zufallszahlengenerator des US-amerikanischen National Institute of Standards and Technology (NIST) ein. Der Dual_EC_DRBG_Standard wurde 2007 als Teil der NIST Special Publication 800-90 herausgegeben” [15].

Dies hatte weitreichende Konsequenzen: Der Standard wurde in kommerziell benutzter Sicherheits-Software verwendet, wie Microsoft SChannel und RSA BSafe. Microsoft SChannel enthielt den Generator nur

als eine optionale Erweiterung. Bei dem RSA-Produkt wird dieser Generator jedoch standardmässig benutzt und nur durch eine aktive Umstellung des Users ausgewechselt. Es wird vermutet, dass die NSA die Firma RSA Security für diese Backdoor bezahlt hat, um so die generierten pseudo-zufälligen Zahlen vorhersagen zu können und Verschlüsselungsalgorithmen zu kompromittieren, dessen Sicherheit auf diesen Pseudo-Zufallszahlen basiert. RSA dementiert dies, die Snowden-Dokumente machen jedoch misstrauisch.

Es ist schwer, zu beweisen, dass Zahlen nicht zufällig sind. Jedoch ist es einfach herauszufinden, welche Zahl als nächste generiert wird, wenn man die Hintertür kennt. Forschern ist es gelungen, bei dem Dual_EC_DRBG die Chiffrierung über die Hintertür zu knacken [16]. Da dies aber nicht überall möglich ist, kann man nur spekulieren, wo die NSA die Designs verschiedener kryptographischer Implementationen beeinflusst. Bei einer fehlerhaften Implementierung nützt das beste mathematisch korrekte Modell zur Verschlüsselung nichts. Zufallszahlengeneratoren sind davon sehr stark betroffen. Viel hängt davon ab, wie zufällig sie wirklich sind. Zufallszahlen werden in den meisten Verschlüsselungsverfahren benötigt.

7 Technologische Entwicklung im Zusammenhang mit dem Snowden-Skandal

(Stefanie & Christoph)

Wenn man in der Geschichte zurückblickt, hat sich in Bezug auf Abhörtechniken nicht viel verändert. So waren beispielsweise Unterseekabel zwischen den Kontinenten schon immer ein Ziel der amerikanischen Überwachung. Früher, als die Kabel noch aus Kupfer bestanden, wurden Taucher eingesetzt, die Abhörgeräte an der Aussenseite der Kabel platzierten [11]. Da das Anzapfen von heutigen Glasfaserkabeln um einiges schwieriger ist und von den Kabelbetreibern erkannt wird, suchte man wohl die Zusammenarbeit mit den Telekommunikationsfirmen. Zu Zeiten der Kupferkabel war auch die Kommunikation über Satelliten und Mikrowellentürme aktuell. Mit Spionagesatelliten, welche die Mikrowellen abfingen, konnte die NSA auf solche Verbindungen zugreifen [12]. Diese Art der Informationsbeschaffung ist heute eher unwesentlich und gilt als veraltet.

Obwohl sich die Abhörtechniken nur in geringem Masse verändert haben, so hatte der technologische Fortschritt dennoch indirekt einen Einfluss auf die Informationsbeschaffung der NSA. Durch den Fortschritt sind die Herstellungskosten für Elektronik drastisch gesunken und es werden unzählige Geräte mehr produziert und nachgefragt. Zusätzlich werden auch immer mehr Geräte ans Internet angeschlossen. Mit dem Einzug des “Internet of Things” sind heute bereits Mobiltelefone, Fernseher oder Haushaltgeräte mit dem World Wide Web verbunden. Als eine Auswirkung davon hat sich die Art und Weise, wie das Internet verwendet wird, stark verändert. Es ist nicht mehr nur ein Ort, an dem Information abgerufen wird. Heutzutage gibt jeder Internetbenutzer auch Information über sich preis. Entweder ganz bewusst, indem er zum Beispiel einen Eintrag auf Facebook verfasst, oder eher unbewusst, indem er Services wie Google Maps verwendet und so Google seinen Standort mitteilt.

Es ist davon auszugehen, dass die NSA schon immer mit Firmen zusammengearbeitet hat, welche Informationen verarbeiten, die von Interesse für den Geheimdienst sind. So wurden bereits 1945 in Kooperation mit privaten Telegrafengesellschaften Telegramme überwacht [20]. Der Nutzen solcher Partnerschaften war aber wohl noch nie so gross wie im heutigen Internetzeitalter. Noch nie benutzten so viele Menschen das Internet wie in 2013 (38.8 % im Vergleich zu 15.8 % in 2005 [5]) und noch nie war Elektronik so allgegenwärtig wie heute.

Datenbeschaffung ist für Anbieter von Internetdiensten wie Google oder Facebook das Kerngeschäft. Dass viele dieser führenden Internetkonzerne in den USA ansässig sind, vereinfacht die Zusammenarbeit für die NSA zusätzlich. In der Präsentation über PRISM nennt die NSA diesen Umstand passend “home-field advantage” [2]. Dieser Heimvorteil hat wichtigen Anteil am Erfolg und der Mächtigkeit von PRISM, aber auch XKeyscore. Ob dies auch in Zukunft bestehen wird oder ob sich Internetgrössen aus anderen Ländern durchsetzen werden, bleibt offen. Klar ist, dass erst der technologische Fortschritt, die zunehmende Verbreitung des Internets und die Veränderung in dessen Benutzung ein Programm wie PRISM möglich machten. Es wäre vor wenigen Jahrzehnten undenkbar gewesen. Während in der Nachkriegszeit Telegramme noch auf Lochkarten und Magnetbänder kopiert und der NSA physisch zugestellt wurden, läuft der ganze Informationsfluss heute automatisch und in Echtzeit.

Der Fortschritt hat aber nicht nur die Gesellschaft und somit die Art und Weise der Datengewinnung verändert. Er beeinflusst auch, wie mit den erfassten Daten umgegangen wird. Leistungsfähigere Prozessoren, billigerer und physisch kleinerer Speicherplatz haben dazu geführt, dass Datenbanken und Rechenzentren

riesiger Ausmasse keine Unmöglichkeit mehr sind. Datenmengen solcher Grössenordnungen, wie die NSA sie sammelt, kann man daher erst seit kurzer Zeit sinnvoll auswerten. Deshalb ist Data Mining heute auch ein wichtiges Forschungsgebiet.

Im Gebiet der Kryptographie sind zum Ärger der Geheimdienste wiederum Fortschritte gemacht worden, die das Sammeln von Informationen erschweren. Wie erwähnt sind kommerzielle (aber auch kostenlose) Verschlüsselungsprodukte keine Seltenheit mehr. Jedoch ist davon auszugehen, dass eher eine Minderheit der Internetbenutzer sich mit diesem Thema auseinandergesetzt hat und Verschlüsselungsverfahren aktiv und bewusst einsetzt. Auf diesem Gebiet kann sich in naher Zukunft jedoch noch viel ändern. Wie auch andere Forscher arbeitet die NSA angeblich an einem Quantencomputer, der die Welt der Kryptologie revolutionieren könnte [19].

8 Schlussfolgerungen

(Christoph)

Wenn man auf die NSA-Affäre rund um Edward Snowden zurückblickt, ist man nicht besonders beeindruckt von den technischen Möglichkeiten der NSA. Viele der Abhörtechniken haben sich vom Prinzip her kaum verändert und sind höchstens effizienter geworden.

Viel bemerkenswerter ist die Tatsache, dass sich die NSA Veränderungen in der Gesellschaft, die durch technologischen Fortschritt entstanden sind, zu Nutze macht. Die Menschen sind heute stärker mit dem Internet verbunden und geben mehr Information von sich preis denn je. Während ein Geheimdienst früher Satelliten ins All schicken und U-Boote aussenden musste, um Spionage zu betreiben, genügt es heute, das Internet zu kontrollieren. Wir verwanzen uns gewissermassen freiwillig, indem wir Smartphones und Internetservices benutzen, die eigentlich alles über uns wissen.

So gesehen macht es aus Sicht der NSA Sinn, sich mit Datensammlern aus der Privatwirtschaft zusammenzutun, seien das nun Telekomfirmen, Internetdienstleister oder Kabelfirmen. Es scheint sich eine Tendenz herauszustellen, die Datenbeschaffung zu delegieren, entweder auf private Unternehmen oder andere Geheimdienste, und sich auf die Verarbeitung, Speicherung und Analyse der Daten zu fokussieren. Dort sind denn auch technologisch gesehen die grössten Fortschritte gemacht worden. Im Bereich des Data Mining stehen der NSA heute Instrumente zur Verfügung, die vor ein paar Jahren undenkbar gewesen wären.

Insgesamt gilt anzumerken, dass die Öffentlichkeit mit den Enthüllungen Snowdens nur einen kleinen Einblick in die Tätigkeiten der NSA erhalten hat. Es wird angenommen, dass Snowden über 1,7 Millionen Dokumente gesammelt hat [21]. Davon überreichte er nur einen Teil der Presse und diese veröffentlichte wiederum nur einen Bruchteil davon. Man darf folglich davon ausgehen, dass die NSA über viele weitere und wahrscheinlich noch fortgeschrittenere und potentere Mittel verfügt, um Personen zu überwachen.

Begriffe

Metadaten: Metadaten oder Metainformationen sind Daten, die Informationen über Merkmale anderer Daten enthalten, aber nicht diese Daten selbst. Zum Beispiel wann Daten gesendet wurden, von welcher IP-Adresse Daten stammen, welche E-Mail Adresse als Sender angegeben wird.
Quelle: http://www.theguardian.com/world/2013/sep/30/nsa-americans-metadata-year-documents

Data Mining: "Unter Data Mining versteht man die Anwendung von Methoden und Algorithmen zur möglichst automatischen Extraktion empirischer Zusammenhänge zwischen Planungsobjekten, deren Daten in einer hierfür aufgebauten Datenbasis bereitgestellt werden." Quelle: http://wirtschaftslexikon.gabler.de/Definition/data-mining.html

Kryptologie: Kryptologie ist die Wissenschaft, die sich mit Informationssicherheit beschäftigt. Sie besteht aus der Kryptographie und der Kryptoanalysis.

Kryptographie: In der Kryptographie geht es grundsätzlich um die Verschlüsselung von Informationen und die Algorithmen und Verfahren, die dazu benutzt werden. Ausserdem gehören weitere Themen der Informationssicherheit dazu, wie etwa die Signierung von Daten oder die Authentifizierung eines Users.

Kryptoanalysis: Die Kryptoanalysis ist der Gegenpart zur Kryptographie, hier wird versucht, Schwachstellen in kryptographischen Verfahren zu finden und auszunutzen.

Literatur

1. NSA, Mission (2011). Verfügbar unter: http://www.nsa.gov/about/mission/index.shtml (Stand 30.06.2014)
2. Greenwald, G. & MacAskill, E. (2013). NSA Prism program taps in to user data of Apple, Google and others. Verfügbar unter: http://www.theguardian.com/world/2013/jun/06/us-tech-giants-nsa-data (Stand 29.06.2014)
3. Gellman, B. & Poitras, L. (2013). U.S., British intelligence mining data from nine U.S. Internet companies in broad secret program. Verfügbar unter: http://www.washingtonpost.com/investigations/us-intelligence-mining-data-from-nine-us-internet-companies-in-broad-secret-program/2013/06/06/3a0c0da8-cebf-11e2-8845-d970ccb04497_story.html (Stand 29.06.2014)
4. Spiegel TV, (2014). Inside NSA: Hacker, Whistleblower und der Geheimdienst. Verfügbar unter: http://www.spiegel.de/video/inside-nsa-hacker-whistleblower-und-der-geheimdienst-video-1325011-iframe.html (Stand 29.06.2014)
5. International Telecommunication Union (2013). Key ICT indicators for developed and developing countries and the world (totals and penetration rates). Verfügbar unter: http://www.itu.int/en/ITU-D/Statistics/Documents/statistics/2013/ITU_Key_2006-2013_ICT_data.xls (Stand 29.06.2014)
6. Kloc, J. (2013). Forget PRISM: FAIRVIEW is the NSA's project to "own the Internet". Verfügbar unter: http://www.dailydot.com/news/fairview-prism-blarney-nsa-internet-spying-projects/ (Stand 29.06.2014)
7. Greenwald, G. (2013). The NSA's mass and indiscriminate spying on Brazilians. Verfügbar unter: http://www.theguardian.com/commentisfree/2013/jul/07/nsa-brazilians-globo-spying (Stand 29.06.2014)
8. MacAskill, E., Borger, J., Hopkins, N., Davis, N. & Ball, J. (2013). GCHQ taps fibre-optic cables for secret access to world's communications. Verfügbar unter: http://www.theguardian.com/uk/2013/jun/21/gchq-cables-secret-world-communications-nsa (Stand 29.06.2014)
9. Greenwald, G. (2013). XKeyscore: NSA tool collects 'nearly everything a user does on the internet'. Verfügbar unter: http://www.theguardian.com/world/2013/jul/31/nsa-top-secret-program-online-data (Stand 29.06.2014)
10. Bagger, J. (2013). Warum die NSA-Affäre auch Tante Grete betrifft, die gar nicht auf Facebook ist. Verfügbar unter: http://heise.de/-1939834 (Stand 29.06.2014)
11. Timberg, C. & Nakashima, E. (2013). Agreements with private companies protect U.S. access to cables' data for surveillance. Verfügbar unter: http://www.washingtonpost.com/business/technology/agreements-with-private-companies-protect-us-access-to-cables-data-for-surveillance/2013/07/06/aa5d017a-df77-11e2-b2d4-ea6d8f477a01_story.html (Stand 29.06.2014)
12. Wikipedia (2014). Microwave transmission. Verfügbar unter: http://en.wikipedia.org/wiki/Microwave_transmission#cite_ref-4 (Stand 29.06.2014)
13. National Security Agency (2010). Declassified UKUSA Signals Intelligence Agreement Documents Available. Verfügbar unter: http://www.nsa.gov/public_info/press_room/2010/ukusa.shtml (Stand 30.06.2014)
14. Schmidt, J. (2013). NSA und GCHQ: Grossangriff auf Verschlüsselung im Internet. Verfügbar unter: http://heise.de/-1950935 (Stand 29.06.2014)
15. Scherschel, F. (2013). NSA-Affäre: Generatoren für Zufallszahlen unter der Lupe. Verfügbar unter: http://heise.de/-1953716 (Stand 29.06.2014)
16. Schmidt, J. (2014). Mehr Details zur Hintertür im Zufallszahlengenerator Dual EC DRBG. Verfügbar unter: http://heise.de/-2159523 (Stand 29.06.2014)
17. Ball, J., Borger, J. & Greenwald, G. (2013). Revealed: how US and UK spy agencies defeat internet privacy and security. Verfügbar unter: http://www.theguardian.com/world/2013/sep/05/nsa-gchq-encryption-codes-security (Stand 29.06.2014)
18. Greenwald, G. & MacAskill, E. (2013). Boundless Informant: the NSA's secret tool to track global surveillance data. Verfügbar unter: http://www.theguardian.com/world/2013/jun/08/nsa-boundless-informant-global-datamining (Stand 29.06.2014)
19. Holland, M. (2014). "Penetrating Hard Targets": NSA arbeitet an Quantencomputern zur Kryptoanalyse. Verfügbar unter: http://heise.de/-2074540 (Stand 29.06.2014)
20. Supplementary detailed staff reports on intelligence activities and the rights of Americans, Book III (1976). Verfügbar unter: http://www.randomcollection.info/cointeldocs/churchfinalreportIIIj.htm (Stand 30.06.2014)
21. Carroll, R. (2014). Snowden used simple technology to mine NSA computer networks. Verfügbar unter: http://www.theguardian.com/world/2014/feb/09/edward-snowden-used-simple-technology-nsa (Stand 30.06.2014)