Fachgruppe für Angewandte Kryptographie in der GI

Kryptographie schützt Grundrechte – gerade im Zeitalter der massenhaften Ausforschung des Datenverkehrs im Internet

Die Informationen, die durch Edward Snowden nach und nach an die Öffentlichkeit kommen, geben ein erschreckendes Bild von den aktuellen Möglichkeiten der großen Nachrichtendienste. Es häufen sich in letzter Zeit Berichte, dass der US-amerikanische Geheimdienst NSA kryptographische Verfahren im Internet aushebeln kann. Wir möchten als Fachgruppe Krypto der Gesellschaft für Informatik hierzu Stellung nehmen und erläutern, welches die Verwundbarkeiten bei der Anwendung der Kryptographie im Internet sind, die von Nachrichtendiensten ausgenutzt werden können, und wie man sich möglichst dagegen schützen kann.

Der Schutz der Freiheit vor willkürlichen Eingriffen in die Privatsphäre ist sowohl ein UNO Menschenrecht (AEMR Artikel 12) als auch per Grundgesetz in Form von der freien Entfaltung der Persönlichkeit (GG Artikel 2), Brief- und Fernmeldegeheimnis (GG Artikel 10) und der Unverletzlichkeit der Wohnung zugesichert (GG Artikel 13). Weiterhin hat das Bundesverfassungsgericht bereits 2008 entschieden, dass eine demokratische Gesellschaft ein berechtigtes Interesse an der Vertraulichkeit und der Integrität von informationstechnischen Systemen wie z.B. Smartphones, Tablets, Notebooks oder Desktop-PCs hat.

Der aktuelle Ausspähskandal, den Edward Snowden mit seinen Enthüllungen ins Rampenlicht gebracht hat, zeigt deutlich, dass Grundrechte wie das Recht auf Privatsphäre in einer vernetzten Welt nicht mehr durch Gesetze, sondern nur noch durch Technik geschützt werden können. Falls Dienste eine Möglichkeit sehen, an Daten zu kommen - sei es durch Anzapfen von Glasfaserleitungen, Kooperation mit befreundeten inländischen/ausländischen Diensten oder Rechenzentren von global agierenden Firmen wie Yahoo, Facebook und Google - werden sie diese auch nutzen; bestehende Gesetze hindern die Dienste hieran offensichtlich nicht . Aufgrund der aktuellen Informationspolitik ist anzunehmen: Alles, was technisch möglich ist, wird seitens staatlicher Dienste zur Überwachung und Manipulation der Kommunikation im Internet eingesetzt. Auch wenn es sich bisher zunächst nur um Einzelfälle von betroffenen Bürgern mit potentiellem Kontakt zu Spionagezielen der Nachrichtendienste handeln mag, so kann dies auch ein Vorreiter sein für eine weitaus größere Bedrohung: der massenhaften gezielten Ausforschung und Manipulation von Bürgern, Unternehmen, Organisationen und letztendliche ganzer Staaten durch das Internet. Dies erlaubt Einflussnahmen bisher unbekannten Ausmaßes.

Ein Weg der digitalen Spionage zu entgehen - und seine digitale Privatsphäre wieder herzustellen - ist die korrekte Anwendung von Kryptographie. Allerdings hilft dabei nur eine Ende-zu-Ende Verschlüsselung, das heißt eine kryptographisch geschützte Kommunikation direkt von Sender zu Empfänger – ohne Umschlüsselungsstationen auf dem Übertragungsweg. Ansonsten können nicht nur Sender und Empfänger mitlesen,sondern auch Dienstanbieter wie Google, GMX, Web, Yahoo, Microsoft usw. Aber kann man diesen auch vertrauen? In der USA ist es möglich, Firmen mittels eines "National Security Letter" zur Kooperation und gezielten Herausgabe von Daten zu zwingen. Es ist inzwischen davon auszugehen, dass eine freiwillige oder aufgezwungene Kooperation zwischen den Geheimdiensten und großen Firmen in den USA stattfindet, was dazu führt, dass man diesen Firmen sowie deren Software, Apps und Diensten im Zweifelsfall nicht rückhaltslos vertrauen sollte. Diese Praxis ist beispielsweise bekannt geworden durch Lavabit, ein Anbieter verschlüsselter E-Mails, dessen Gründer Lader Levision diese Kooperation nicht eingehen wollte und als Folge dessen den E-Mail-Dienst im August 2013 einstellte. In einer Erklärung hierzu warnte er auf der Webseite www.lavabit.com davor, schützenswürdige Daten einer Firma mit physischen Wurzeln in den USA anzuvertrauen.

Die vermutlich wichtigste kryptographische Anwendung im Web ist SSL/TLS, mit der z.B. Zahlungstransaktionen im Internet abgewickelt werden. Die Infrastruktur des World-Wide-Webs basiert jedoch auf Hunderten von zumeist kommerziellen Wurzel-Zertifizierungsdiensten oder „Root Certification Authorities (Root-CAs)“, deren Zertifikaten ein Browser vertraut. Bei Kooperation von Geheimdiensten mit einer der Root-CAs kann sich ein Geheimdienst mittels gezielt gefälschter TLS-Zertifikate als beliebiger Dienstanbieter ausgeben. Daher können Webdienste für einen typischen Internetnutzer, der die Zertifikate nicht eingehend prüfen kann, Privatsphäre nur mit Einschränkungen garantieren. Wesentlich einfacher

wird es jedoch noch für die Dienste, wenn der Schlüsselaustausch bei SSL/TLS mit einem statischen Schlüssel des Diensteanbieters durchgeführt wird und dieser Schlüssel bei den Diensten hinterlegt wird. Damit lässt sich dann jede mit SSL/TLS verschlüsselte Kommunikation direkt entschlüsseln. Große amerikanische Internetfirmen wie google.com, facebook.com oder yahoo.com verwenden in der Tat einen statischen RSA-Schlüssel zur Schlüsselvereinbarung bei SSL/TLS.

Zur Zeit wird in der Öffentlichkeit über die Sicherheit von Verschlüsselungsverfahren und Sicherheitsprotokollen diskutiert.

"Gängige Verschlüsselungssysteme für Daten, E-Mails oder Bankgeschäfte stellen für den US-Dienst NSA und den britischen GCHQ kein Hindernis dar." (Manager Magazin Online, "NSA knackt Verschlüsselungen im Netz", 06. September 2013)

Aus der Sicht der Fachgruppe heißt dies nicht, dass Verschlüsselungssysteme leicht gebrochen werden können, sondern dass die Kommunikationsendpunkte Schwachstellen aufweisen. Die korrekte Verwendung etablierter kryptographischer Verfahren bietet ein ausreichendes Maß an mathematischer Sicherheit. Dies wird auch in einem Online-Interview des "The Guardian" mit Edward Snowden belegt. Auf die Frage hin, ob die Verschlüsselung von E-Mails eine guter Weg ist, der Überwachung der NSA zu entgehen, gab Snowden folgende Antwort:

"Verschlüsselung funktioniert. Starke kryptographische Verfahren,
richtig eingesetzt, ist eines von den wenigen Dingen, denen man vertrauen kann.
Leider jedoch ist die NSA in der Lage auf den Endgeräten der Benutzer unbemerkt
Schadsoftware zu installieren, da diese in hohem Maße unsicher sind."
(Interview vom 17. Juni 2013, sinngemäß übersetzt)

Jedoch, eine (absichtliche oder unabsichtliche) fehlerhafte Implementierung kann Sicherheitslücken öffnen, die von Geheimdiensten zum Entschlüsseln von Daten ausgenutzt werden können. Bei gängigen Open-Source-Produkten wie GnuPG (E-Mail-Verschlüsselung) oder TOR (Anonymisierung im Internet) ist es unwahrscheinlich, dass solche Fehler längere Zeit unentdeckt bleiben. Aber auch hier gab es in der Vergangenheit bereits sicherheitskritische Programmierfehler, ein prominentes Beispiel ist die Implementierung des Zufallszahlengenerators von OpenSSL bei debian Linux. Aufgrund der Offenlegung der Implementierung und damit der Prüfbarkeit von jedermann empfehlen wir die Verwendung von Open-Source-Produkten wie TrueCrypt (Festplatten-Verschlüsselung), GnuPG (E-Mail-Verschlüsselung), TOR und Pidgin-OTR (Chat mit Ende-zu-Ende-Verschlüsselung). Wir geben aber auch zu bedenken, dass dies letztendlich nur Anwendungen sind, die auf einer Plattform (Betriebssystem, Hardware) zur Ausführung kommen. Wenn die Integrität einer Plattform auf Grund von Sicherheitslücken oder Hintertüren nicht mehr sicher gestellt werden kann, so kann hierüber auch geheimes Schlüsselmaterial auf der Plattform kompromittiert werden und damit die Vertraulichkeit von verschlüsselten Informationen gebrochen werden.

Ausgehend von den Empfehlungen des Sicherheitsexperten Bruce Schneier von http://www.theguardian.com/world/2013/sep/05/nsa-how-to-remain-secure-surveillance möchten wir als Fachgruppe Krypto einige Empfehlungen aussprechen, die aus unserer Sicht den Schutz der Privatsphäre bedeutend erhöhen können:

1) Verbergen Sie Ihre Kommunikationswege im Internet durch Nutzung eines Netzwerks zur Anonymisierung der Verbindungsdaten, wie z.B. TOR. Dies verhindert, dass Geheimdienste Meta-Daten erhalten.

2) Verschlüsseln Sie Ihre Kommunikation Ende-zu-Ende (TLS, Ipsec, GPG). Nutzen Sie hierbei vom BSI empfohlene Chiffriermechanismen wie AES, RSA-2048 und ephemerale Diffie-Hellman Schlüsselaustauschprotokolle, die „Forward Secrecy“ garantieren können, d.h. die Sitzungsdaten können auch dann nicht entschlüsselt werden, wenn die statischen Schlüssel der Kommunikationspartner kompromittiert worden sind. Nutzen Sie nur Verschlüsselungssoftware mit offengelegten Quelldateien („Open Source“). Trauen Sie keiner kommerziellen Verschlüsselungssoftware. Bruce Schneier geht davon aus, dass große US-amerikanische Firmen bereits Hintertüren für die NSA eingebaut haben; Veröffentlichungen von Seiten Snowdens scheinen dies zu bestätigen. Prüfen Sie vor Versendung von hochsensitiven Informationen die öffentlichen Schlüssel und Zertifikate Ihrer Kommunikationspartner

dahingehend, ob diese Daten authentisch sind, ggf. durch direkte telefonische Anfragen bei Ihrem Kommunikationspartner.

3) Beachten Sie bei hochsensitiven Informationen, dass ein Computer im Internet durch Schadsoftware oder Hintertüren zum Erlangen eben dieser Informationen bereits kompromittiert sein könnte oder werden könnte. Wenn Sie für einen Geheimdienst ein Ziel sind können Sie können davon ausgehen, dass Schadsoftware auf Sie persönlich zugeschnitten ist und durch konventionelle Virenscanner nicht erkannt wird. Die Schadsoftware kann in einem pdf-Dokument enthalten sein, das Sie (scheinbar) von einem vertrauenswürdigen Absender per E-Mail erhalten. Bruce Schneier erwähnt, dass er sich für die Sichtung des Materials von Edward Snowden einen neuen Computer beschafft hat, der nicht an das Internet angeschlossen wird. Hierbei ist zu ergänzen, dass die Datenträger wie USB-Sticks zum Transfer der verschlüsselten Daten zu einem Internet-PC ebenfalls frei von Schadsoftware sein müssen und Nachrichtendienste auch konventionelle Wege nutzen können, um sich physischen Zugang zu einem Computer zu verschaffen. Erinnert sei hier an Einbrüche bei Vertrauten von Snowden in letzter Zeit, bei denen keinerlei Wertgegenstände entwendet worden waren.

4) Prüfen Sie, in welchem Land ein Diensteanbieter (z.B. Cloud, E-Mail, soziale Netzwerke) seine Server betreibt. Wählen Sie einen Anbieter aus, der in einem Staat mit hohen gesetzlichen Anforderungen an den Datenschutz beheimatet ist.

Sämtliche notwendigen Werkzeuge für einen effektiven Schutz der digitalen Privatshäre sind bereits jetzt kostenlos im Internet verfügbar. Bedauerlicherweise sind viele Empfehlungen für einen typischen Internet-Nutzer nur schwerlich umsetzbar, da die kostenlosen kryptographischen Anwendungen üblicherweise auf Nutzer mit Vorkenntnissen auf dem Gebiet der Netzwerksicherheit zugeschnitten sind. Der Einsatz dieser Anwendungen erfordert es, sich mit den kryptographischen Grundlagen auseinanderzusetzen. Ein Einsatz, der sich lohnt und die Analysearbeit der Nachrichtendienste definitv erheblich erschwert. Angemerkt sei allerdings, dass die Nutzung von Verschlüsselungs- und Anonymisierungsdienten offensichtlich das Risiko erhöht, das der hierfür genutzte Computer in das Visier der Nachrichtendienste gerät. Nach Einschätzung von Bruce Schneier ist jedoch die gezielte Kompromittierung eines individuellen Computers auch für die NSA mit nennenswerten Kosten verbunden und zudem auch mit einem Entdeckungsrisiko der ausgenutzten Sicherheitslücken und Hintertüren behaftet.

Aus Sicht der Fachgruppe Krypto ist eine breite Nutzung von kryptographischen Schutzmechanismen und deren nachvollziehbar transparente Umsetzung die bestmögliche Antwort auf die aktuellen technischen Möglichkeiten der Geheimdienste. Absolute Sicherheit gibt es in Zeiten von nicht-vertrauenswürdigen Computern, die über das Internet vernetzt sind, jedoch nicht. Resignation angesichts der Möglichkeiten zur Überwachung im Internet ist aber noch nicht angebracht. Was bleibt ist ein Spannungsfeld zwischen einer einfachen Bedienbarkeit von Internetanwendungen und einem hohem Bedürfnis nach Vertraulichkeit der Informationen, in dem jeder seine individuelle Lösung finden muss.