Universität Hamburg
DER FORSCHUNG | DER LEHRE | DER BILDUNG

GESELLSCHAFT FÜR INFORMATIK

Deutscher Bundestag
Ausschuss für Inneres und Heimat

Ausschussdrucksache
19(4)434

STELLUNGNAHME

Öffentliche Anhörung des Innenausschusses zum Thema „Recht auf Verschlüsselung – Privatsphäre und Sicherheit im digitalen Raum stärken“ am 27. Januar 2020

Prof. Dr. Hannes Federrath
Universität Hamburg, Fachbereich Informatik
Präsident der Gesellschaft für Informatik e.V. (GI)

27. Januar 2020

Kurzfassung

In den vergangenen Jahrzehnten hat die Bundesregierung mehrfach bestätigt, „dass es bei der uneingeschränkten Freiheit der Nutzer bei der Auswahl und dem Einsatz von Verschlüsselungssystemen bleibt“, wie es im Eckpunktepapier der Bundesregierung zur deutschen Kryptopolitik [BT1999, IMK2002] von 1999 heißt. Dies ist nachdrücklich zu begrüßen und sollte so beibehalten werden, da sich die Rahmenbedingungen zumindest aus technischer Sicht seitdem nicht verändert haben.

Die verfügbaren kryptographischen Algorithmen sind seit Jahren so ausgereift, dass ihr breiter Einsatz problemlos möglich ist. Die EU-Datenschutzgrundverordnung (DSGVO) [DSGV2016] verpflichtet in Art. 32 explizit zur „Verschlüsselung personenbezogener Daten“. Die Umsetzung solcher technischen und organisatorischen Maßnahmen zum Schutz der informationellen Selbstbestimmung ist dementsprechend unabdingbar.

In diesem Sinn ist es sowohl für den Schutz von Betriebs- und Geschäftsgeheimnissen als auch zur Durchsetzung des Rechts auf informationelle Selbstbestimmung aus technischer Sicht möglich und mit Blick auf die Risiken der Digitalisierung geboten, ein Recht auf Verschlüsselung für Wirtschaft, Verwaltung und Bürgerinnen und Bürger zu verankern und – noch weitergehend – eine Pflicht des Diensteanbieters zur Datenverschlüsselung zu etablieren, soweit dies technisch möglich und zumutbar ist.

Unwirksame und schlimmstenfalls gefährliche Kryptoregulierung

Zuletzt bestätigt wurde die Position der Bundesregierung zum freien Einsatz von Kryptographie zumindest im Jahr 2015: „Die Entwicklung und durchgängige Verwendung vertrauenswürdiger IT-Sicherheitstechnologien ist von entscheidender Bedeutung für Unternehmen, Verwaltung und Bürger in unserer heutigen Informationsgesellschaft. Daher wird die gezielte Schwächung oder Regulierung von Verschlüsselungstechniken von der Bundesregierung nicht verfolgt.“ [BT2015]

An diesen Eckpunkten sollte weiter festgehalten werden, da sich die technischen Rahmenbedingungen, die gegen eine Kryptoregulierung sprechen, seither kaum geändert haben. Im Wesentlichen gilt die wichtige, bereits 1997 formulierte Aussage [Fed1998] fort, dass die gesetzliche Einschränkung von Verschlüsselung oder gar das Verbot von Verschlüsselung nicht durchsetzbar und nicht kontrollierbar sind.

Erstens existieren mit steganographischen Verfahren zahlreiche technische Alternativen, deren Verwendung durch Kriminelle (bei richtigem technischen Einsatz) nicht einmal mehr erkennbar ist. Steganographie schützt sowohl die Vertraulichkeit des Inhalts einer Nachricht als auch deren Existenz. Steganographie wäre für textbasierte Kommunikation heute grundsätzlich genauso effizient und bequem einsetzbar, wie wir es von gängigen Messenger-Diensten kennen. Sie wäre in moderne Messenger-Apps leicht integrierbar und ist in Verbindung mit existierenden Anonymisierungsverfahren wie etwa dem TOR-System dazu geeignet, geheime Kommunikation noch effektiver zu schützen als wir es von heutigen Produkten kennen. Bisher existieren allerdings keine bzw. wenn überhaupt nur wenige für Endnutzer geeignete Apps zur steganographischen Kommunikation. Eine Kryptoregulierung würde die Entwicklung und die Verbreitung von solchen Schutzsystemen vorantreiben. Dies könnte die Aufklärung von Straftaten sogar schwerer machen als bisher.

Zweitens erfordern die in heutigen Kommunikationsnetzen notwendigen Schutzmaßnahmen den zwingenden Einsatz von Kryptographie. Verfahren zur rechtsverbindlichen Kommunikation (Elektronische Signatur) und zum Schutz vor unbemerkten oder unerlaubten Veränderungen von Nachrichten und Dokumenten sind ohne Kryptographie nicht denkbar. Sehr eindringlich hat dies bereits 1998 Ronald Rivest gezeigt, indem er mit Hilfe eines Verfahrens zum Schutz der Integrität (Message Authentication Codes) gezeigt hat, wie damit vertrauliche Nachrichten sicher und ohne Verschlüsselung übermittelt werden können [Riv1998].

Im Ergebnis läuft somit eine etwaige Einschränkung von Kryptographie leer, schwächt sowohl die Wirtschaft als auch das Recht auf informationelle Selbstbestimmung und erschwert schlimmstenfalls sogar die Strafverfolgung.

Einsatz von starker Verschlüsselung

Die meisten verfügbaren und heute praktisch genutzten kryptographischen Verschlüsselungsalgorithmen, etwa der Advanced Encryption Standard (AES) [NIST2001] sind seit Jahren gut untersucht, technisch ausgereift, kostengünstig einsetzbar und werden vermutlich noch für viele Jahre (mindestens 20 Jahre) ausreichenden Schutz auch gegen starke Angreifer bieten.

Durch die Fortschritte bei der Entwicklung von Quantencomputern werden vermutlich einige der weit verbreiteten Algorithmen in einigen Jahren nicht mehr einsetzbar sein (z.B. das Verfahren von Rivest, Shamir, Adleman [RSA1078]) und müssen durch sichere Alternativen ersetzt werden. Das amerikanische NIST (National Institute of Standards and Technology) hat bereits 2016 die Standardisierung von sog. Post-Quantum-Kryptographie initiiert [NIST2016], so dass zu erwarten ist, dass auch in Zukunft langfristig sichere Verfahren zur Verfügung stehen.

Eine verpflichtende Verbindungsverschlüsselung, bei der einzelne Teilabschnitte der Kommunikation zwischen den beteiligten Endgeräten, Routern und Servern abgesichert werden, wird trotz der jahrelangen technischen Verfügbarkeit, der geringen Kosten und des sehr wirksamen Schutzes vor Outsidern (Angreifer auf den Kommunikationsverbindungen) selten in den technischen Standards und bisher überhaupt nicht in der Rahmengesetzgebung zur Telekommunikation gefordert.

Obwohl die verfügbaren kryptographischen Algorithmen seit Jahren offene Standards sind und zudem sehr ausgereift sind, wurden in den standardisierten, offenen Kommunikationsprotokollen des Internet, etwa dem Simple Mail Transfer Protocol (SMTP), Post Office Protocol (POP) und dem Internet Message Access Protocol (IMAP) über die Jahre hinweg kaum Fortschritte beim obligatorischen Einsatz von Verschlüsselung erzielt.

Zwar können offene Sicherheitsstandards wie OpenPGP/GnuPG (Pretty Good Privacy) und S/MIME (Secure Multipurpose Internet Mail Extensions) als optionale Verfahren zur Ende-zu-Ende-Verschlüsselung eingesetzt werden, bei der zwischen den Endgeräten der beteiligten Kommunikationspartner alle übertragenen Inhalte wirksam vor Outsidern (Angreifer auf den Kommunikationsverbindungen) als auch Insidern (Kommunikationsnetzbetreiber) geschützt sind. Allerdings ist dies für die Endbenutzer aufgrund der aufwendigen Installation von Software (GnuPG) und/oder Konfiguration (sowohl OpenPGP/GnuPG als auch S/MIME) sehr mühsam und fehleranfällig.

Selbst breit etablierte Lösungen wie etwa die Ende-zu-Ende-Verschlüsselung von https-Webseiten, die auf technisch ausgereifte Standards wie TLS (Transport Layer Security) zurückgreifen, sind nur optional. Noch immer sind viele Webangebote als unverschlüsselte http-Webseiten verfügbar.

Förderung frei verfügbarer, offener Krypto-Protokolle und Standards

Quelloffene und benutzerfreundliche Implementationen kryptographischer Protokolle und Verschlüsselungsstandards dienen der Allgemeinheit, da sie allen Menschen kostengünstigen Zugang zu kryptografischen Funktionen bieten. Durch die Offenlegung der zugrunde liegenden Techniken besteht die Möglichkeit, frühzeitig Sicherheitsschwächen zu finden und Verbesserungsvorschläge einzubringen.

TLS (Transport Layer Security) ist ein Beispiel für ein standardisiertes kryptographisches Protokoll, welches omnipräsent ist und die komplette Kommunikation zwischen Browser und Webserver durch Ende-zu-Ende-Verschlüsselung schützt. Ohne TLS wären Onlineshopping und Onlinebanking unsicher, könnten keine Anmeldedaten sicher übertragen werden, wäre nicht garantiert, dass Transaktionen unverändert und vertraulich zwischen Bürgerinnen und Bürgern und Staat bzw. Kunden und Händlern ablaufen.

Dennoch existieren auch in TLS systematische Schwächen in der Umsetzung (etwa die Möglichkeit, die TLS-Verschlüsselung durch Man-in-the-Middle-Angriffe und durch „on-the-fly“ erzeugte Schlüsselzertifikate aufzubrechen), die den Schutz von Geschäfts- und Firmengeheimnissen und personenbezogenen Daten gegenüber starken Angreifern (Insider, z.B. Kommunikationsnetzbetreiber; Outsider, z.B. Nachrichtendienste) nicht ausreichend gewährleisten. Im Kern hat sich die derzeit übliche Beglaubigung von Schlüsselmaterial nach dem X.509-Standard [ITU1988] und deren Überprüfung auf Echtheit nicht bewährt. Hier ist dementsprechend Forschungs- und Entwicklungsbedarf.

Paradoxerweise haben Messenger-Apps und (Bild)-Telefon-Software wie etwa iMessage, FaceTime (beide Apple), WhatsApp (Facebook), Signal und OTR innerhalb weniger Jahre gezeigt, dass eine nahtlose und sichere Integration von Ende-zu-Ende-Verschlüsselung in proprietäre Apps möglich ist. Diese existierenden Lösungen sind nur mit der App des jeweiligen Anbieters nutzbar und nicht miteinander kompatibel.

Die hohe Sicherheit und der Anwendungskomfort solcher proprietären Apps gehen somit zu Lasten der Interoperabilität und zumeist auch zu Lasten einer Offenlegung des Quellcodes, die eine Überprüfbarkeit der fehlerfreien Implementierung ermöglicht. Quelloffene Krypto-Bibliotheken sind durch unabhängige Stellen überprüfbar und stellen eine sehr kostengünstige Möglichkeit dar,

aktuelle kryptographische Techniken in diversen Kommunikationsplattformen anzuwenden. Ein Beispiel dafür ist das Signal-Protokoll, das sowohl im Signal-Messenger als auch im Messenger WhatsApp zum Einsatz kommt und so die Kommunikation von Millionen Menschen schützt.

Insbesondere für die sichere E-Mail-Kommunikation besteht Forschungs- und Entwicklungsbedarf. Während private Kommunikation zumeist mit geeigneten Messenger-Apps heute ausreichend gesichert werden kann, ist die E-Mail-Kommunikation für die Wirtschaft und Verwaltung vermutlich auch auf längere Sicht unverzichtbar. Daher ist es notwendig, Protokolle zur einfach anwendbaren, standardisierten und automatischem E-Mail-Verschlüsselung endlich umzusetzen. Hierbei ist GnuPG eines von vielen prominenten Beispielen für quelloffene Implementationen. Es muss jedoch bei der Entwicklung und Verbesserung quelloffener kryptographischer Implementationen und Protokolle auch ein Fokus auf eine extrem einfache Anwendbarkeit für die Endnutzer gelegt werden. Insbesondere die bereits angesprochene Problematik der vertrauenswürdigen Schlüsselzertifikate ist noch nicht ausreichend gelöst. Vielversprechende Initiativen wie etwa die vom Fraunhofer-Institut für Sichere Informationstechnologie (SIT) entwickelte und in Partnerschaft mit der Gesellschaft für Informatik e.V. (GI) vorangetriebene Volksverschlüsselung [VV2016, GI2017, GI2018] müssen gestärkt werden, zumal dort die komplizierte Zertifikatsbeantragung und die Übertragung der Schlüssel in die lokalen Anwendungsprogramme der Nutzer zumindest ansatzweise verbessert wird. Allerdings ist auch diese Lösung noch weit von einer breiten und leicht anwendbaren Lösung entfernt.

Ausnutzung von unbekannten Sicherheitslücken

Zum Schutz der Allgemeinheit und im Interesse des Staates, seine Bürgerinnen und Bürger zu schützen, muss bei der Entdeckung von Sicherheitslücken (Backdoors) von höchster Priorität sein, diese an die verantwortlichen Stellen zu melden und sie zu schließen.

Eine Backdoor stellt eine verwundbare Stelle in einem System dar, die Angreifer dazu benutzen können, in das System einzudringen um vertrauliche Daten zu lesen, sie zu verändern oder sie zu zerstören. Backdoors entstehen entweder beabsichtigt, indem sie die Softwarehersteller gezielt einbauen oder unbeabsichtigt, indem die Sicherheitslücke selbst als Backdoor fungiert.

Sicherheitsschwächen in Kryptographie und Sicherheitslücken in Software können selten und im besten Fall zur Aufklärung von Straftaten genutzt werden, überwiegend schwächen sie jedoch massenhaft gesetztestreue Bürgerinnen und Bürger, Wirtschaft und Verwaltung, da sie auf dem Schwarzmarkt angeboten werden und nicht nur Hackern und inländischen staatlichen Stellen zum Kauf angeboten, sondern insbesondere auch durch ausländische Staaten angekauft

werden und somit schlimmstenfalls auch gegen Deutschland und andere EU-Staaten eingesetzt werden können.

Gerade vor dem Hintergrund der Vermeidung von Hintertüren in sicherheitsrelevanter Software ist die Offenlegung des Quellcodes – zwecks Überprüfbarkeit durch die Öffentlichkeit oder zumindest durch Experten – eine zwingende Voraussetzung für die Vertrauenswürdigkeit von Sicherheitstechnologie.

Verankerung eines Rechts auf Verschlüsselung

Zahlreiche Sicherheitsfunktionen, die nicht notwendigerweise unmittelbar als Verschlüsselung im engeren Sinn wahrgenommen werden, nutzen Verschlüsselungstechnologien. Die sichere Überprüfung von Passwörtern ist beispielsweise ohne kryptographische Verfahren heute undenkbar. Kryptographie ist somit eine wichtige Basistechnologie der Digitalisierung.

In der Vergangenheit hat der Gesetzgeber durchaus proaktiv dazu beigetragen, den Schutz von Bürgerinnen und Bürgern und Wirtschaft im Internet zu stärken. So hat etwa der Diensteanbieter nach § 13 Abs. 6 des Telemediengesetzes (TMG) „die Nutzung von Telemedien und ihre Bezahlung anonym oder unter Pseudonym zu ermöglichen, soweit dies technisch möglich und zumutbar ist. Der Nutzer ist über diese Möglichkeit zu informieren.“ In Anlehnung an den § 13 Abs. 6 TMG wäre es daher möglich und zur Stärkung des Schutzes geboten, eine analoge Vorschrift zum Angebot von Verschlüsselungsdiensten (nicht notwendigerweise im TMG) zu erlassen.

Die Durchsetzung des Rechts auf informationelle Selbstbestimmung in der digitalen Gesellschaft basiert ebenso wie die praktische Umsetzung des Grundrechts auf Gewährleistung der Vertraulichkeit und Integrität informationstechnischer Systeme auf der Verfügbarkeit wirksamer kryptographischer Verfahren. Über die EU-Datenschutzgrundverordnung (DSGVO) [DSGV2016] sind die verantwortlichen Stellen gemäß Art. 32 explizit zur „Verschlüsselung personenbezogener Daten“ verpflichtet.

Weiterhin ist ein Recht auf Verschlüsselung auch für die freie Berufsausübung notwendig. Hierzu zählen etwa der Schutz vor Industriespionage und der Schutz journalistischer Berufe und ihrer Quellen. Freie Anwendbarkeit von Verschlüsselung und ein Recht auf Verschlüsselung schützen in diesem Sinn auch die Pressefreiheit.

Fazit

Die Forderungen des Antrags „Recht auf Verschlüsselung – Privatsphäre und Sicherheit im digitalen Raum stärken“ [BT2020] sind in vollem Umfang aus informatisch-technischer Perspektive zu begrüßen.

Literaturverzeichnis

[BT1999] Bundesregierung: Eckpunkte der deutschen Kryptopolitik. 1999. Originalquelle beim BMWI nicht mehr vorhanden, Kopie unter https://hp.kairaven.de/law/eckwertkrypto.html (letzter Abruf am 24.01.2020)

[BT2015] Bundesregierung: BT-Drucks. 18/5144 vom 11.06.2015, S. 4. http://dipbt.bundestag.de/dip21/btd/18/051/1805144.pdf (letzter Abruf am 24.01.2020)

[BT2020] Deutscher Bundestag: Antrag der Fraktion der FDP: Recht auf Verschlüsselung – Privatsphäre und Sicherheit im digitalen Raum stärken. BT-Drucks. 19/5764 vom 13.11.2018. http://dip21.bundestag.de/dip21/btd/19/057/1905764.pdf (letzter Abruf am 24.01.2020)

[DSGV2016] Verordnung (EU) 2016/679 des Europäischen Parlaments und des Rates vom 27. April 2016 zum Schutz natürlicher Personen bei der Verarbeitung personenbezogener Daten, zum freien Datenverkehr und zur Aufhebung der Richtlinie 95/46/EG (Datenschutz-Grundverordnung). https://eur-lex.europa.eu/legal-content/DE/TXT/PDF/?uri=CELEX:32016R0679 (letzter Abruf am 24.01.2020)

[Fed1998] Hannes Federrath: Steganographie -- Vertrauliche Kommunikation ohne Kryptographie. in: Rainer Hamm, Klaus Peter Möller (Hrsg.): Datenschutz durch Kryptographie -- ein Sicherheitsrisiko? Nomos Verlagsgesellschaft, Baden-Baden 1998, 42-51.

[GI2017] Gesellschaft für Informatik: Volksverschlüsselung muss kommen. Pressemitteilung vom 02.02.2017. https://gi.de/meldung/volksverschluesselung-muss-kommen (letzter Abruf am 24.01.2020)

[GI2018] Gesellschaft für Informatik: GI begrüßt Forderung nach einem Recht auf Verschlüsselung und fordert Anstrengungen von Webdiensten. Pressemitteilung vom 04.12.2018. https://gi.de/meldung/gi-begruesst-forderung-nach-einem-recht-auf-verschluesselung-und-fordert-anstrengungen-von-webdiensten/ (letzter Abruf am 24.01.2020)

[IMK2002] Innenministerkonferenz: Anlage zum Bericht der Bundesregierung zu den Auswirkungen der Nutzung kryptografischer Verfahren auf die Arbeit der Strafverfolgungs- und Sicherheitsbehörden (Ziffer 4 der Eckpunkte der deutschen Kryptopolitik vom 2. Juni 1999)

„Verschlüsselungsbericht. 2002. https://www.innenministerkonferenz.de/IMK/DE/termine/to-beschluesse/2002-06-06/anlage-15.pdf?__blob=publicationFile&v=2 (letzter Abruf am 24.01.2020)

[ITU1988] International Telecommunication Union (ITU): Information technology - Open Systems Interconnection - The Directory: Public-key and attribute certificate frameworks. 1988-2019. https://www.itu.int/rec/T-REC-X.509/en (letzter Abruf am 24.01.2020)

[NIST2001] National Institute of Standards and Technology: Advanced Encryption Standard. NIST FIPS PUB 197, 2001.

[NIST2016] National Institute of Standards and Technology: Post-Quantum Cryptography. 2016, https://csrc.nist.gov/Projects/Post-Quantum-Cryptography (letzter Abruf am 24.01.2020)

[Riv1998] Ronald L. Rivest: Chaffing and Winnowing: Confidentiality without Encryption. MIT Lab for Computer Science, March 22, 1998. http://people.csail.mit.edu/rivest/chaffing-980701.txt (letzter Abruf am 24.01.2020)

[RSA1978] Ronald L. Rivest, Adi Shamir, Leonard Adleman: A Method for Obtaining Digital Signatures and Public-Key Cryptosystems. Communications of the ACM, February 1978. https://doi.org/10.1145/359340.359342 (letzter Abruf am 24.01.2020)

[VV2016] Volksverschlüsselung. Offene Initiative für Ende-zu-Ende-Sicherheit. https://volksverschluesselung.de (letzter Abruf am 24.01.2020)

Danksagung

Für die fachliche Zuarbeit bei der Erstellung dieser Stellungnahme danke ich meinen wissenschaftlichen Mitarbeiterinnen und Mitarbeitern Christian Burkert, Matthias Marx, Johanna Nehring-Ansohn, Monina Schwarz sowie den Mitarbeitern der GI-Geschäftsstelle Nikolas Becker und Daniel Krupka.

Kontakt

Prof. Dr. Hannes Federrath
Präsident der Gesellschaft für Informatik e.V. (GI)

Universität Hamburg, Fachbereich Informatik,
Arbeitsbereich Sicherheit in Verteilten Systemen (SVS)
Web: svs.informatik.uni-hamburg.de
E-Mail: federrath@informatik.uni-hamburg.de

Gesellschaft für Informatik e.V. (GI)

Geschäftsstelle Berlin
im Spreepalais am Dom
Anna-Louisa-Karsch-Str.2, 10178 Berlin
Tel.: +49 30 7261 566-15
Mobil: +49 163 8694216
Fax: +49 30 7261 566-19
E-Mail: berlin@gi.de

Geschäftsstelle Bonn
im Wissenschaftszentrum
Ahrstr. 45, 53175 Bonn
Tel.: +49 228 302-145
Fax: +49 228 302-167
E-Mail: bonn@gi.de

Web: www.gi.de