Staatliche Regulierung von Kryptografie – ein Überblick

Von Dr. Andreas Fiessler, Ingenieur Forschung und Entwicklung, genua GmbH

Zusammenfassung

Ein geleaktes Dokument der deutschen Ratspräsidentschaft [1] sorgte kürzlich für Aufsehen. Es zeigt einen neuen Versuch innerhalb der EU, staatliche Zugriffsmöglichkeiten auf verschlüsselte Kommunikation gesetzlich vorzuschreiben.

Dabei ist das Thema keineswegs neu: Die unter dem Namen Crypto Wars bekannte Debatte zu staatlicher Reglementierung von Kryptografie geht bis in den kalten Krieg zurück [2]. Diese Vorstöße wurden stets von Experten auf dem Gebiet heftig kritisiert und abgelehnt, dennoch werden sie seitens der Politik immer wieder neu vorgebracht.

Doch wo genau liegen die Probleme der Forderungen? Wie kann ein solcher Zugriff überhaupt realisiert werden? In diesem Artikel gehen wir allgemeinverständlich auf die technischen Hintergründe des Vorstoßes ein und beleuchten dabei die Gefahren, die jeder dieser Ansätze mit sich bringt.

Der aktuelle EU-Vorstoß

Bei dem vom ORF geleakten Dokument [1] handelt es sich um einen Entwurf für eine Resolution mit dem Titel „Security through encryption and security despite encryption“. Die zeitliche Nähe der internen Veröffentlichung lässt es als eine mögliche Reaktion auf Terrorattentate in Wien erscheinen. Schon in der Vergangenheit wurden ähnliche Vorfälle gerne als Anlass für neue Anläufe zur Ausweitung staatlicher Überwachung genommen. Dabei deutet vieles darauf hin, dass nicht fehlende Daten oder Befugnisse, sondern Ermittlungspannen ursächlich für das Versagen der Behörden in Wien waren [3].

Im jetzt vorliegenden Entwurf wird zunächst betont, dass die EU sich auch weiter für starke Verschlüsselung einsetze und diese als wichtig erachte. Mit der Begründung einer Nutzung durch Kriminelle und erschwerte Strafverfolgung wird – eher abstrakt – eine „Balance“ gefordert. Diese wird im Weiteren ausgeführt als die Möglichkeit für Ermittler, bei Bedarf direkten Zugriff auf den Inhalt jeglicher verschlüsselter Kommunikation zu erhalten. Der Ursprung des Entwurfs in der deutschen Ratspräsidentschaft ist überraschend, da sich die deutsche Bundesregierung weiter offiziell gegen diesen Ansatz ausspricht [4, 5].

Sehr ähnlich liest sich ein Papier der UKUSA, bzw. Five Eyes [6]. Auch hier wird zunächst der Stellenwert sicherer Kryptografie betont, dann allerdings mit Verweis auf Strafverfolgung von Terrorismus und Kindesmissbrauch staatlicher Zugriff gefordert. Genau wie im EU-Entwurf gibt es keine konkreten Vorgaben zur Umsetzung – Hintertüren werden nicht explizit genannt. Stattdessen sehen die Behörden die privaten Hersteller in der Pflicht, einen entsprechenden Zugang zu entwickeln

und bereitzustellen. Das in der Volksrepublik China am 1.1.2020 in Kraft getretene, neue Kryptografiegesetz [7] enthält bemerkenswert ähnlich lautende Standpunkte, Begründungen und Forderungen. Um zu verstehen, weshalb diese Forderungen so kritisch sind, ist es zunächst notwendig, sich die Möglichkeiten der Umsetzung anzusehen.

Zugriff auf verschlüsselte Kommunikation

In der Vergangenheit war ein verdecktes Überwachen durch Behörden vergleichsweise einfach und selektiv möglich, beispielsweise durch Abhören einer analogen Telefonleitung. Mit der zunehmenden Verlagerung der Kommunikation in das Internet und der Tendenz zu allgemeiner Verschlüsselung werden auch berechtigte Zugriffsinteressen im Rahmen der Strafverfolgung schwieriger. Ein solcher Zugriff auf verschlüsselte Kommunikation kann auf verschiedene Arten versucht werden:

1. Zugriffe direkt am Endgerät
2. Zweitschlüssel erzwingen
3. Abhörschnittstellen
4. Schwächung von Kryptografie
5. Man-in-the-Middle-Angriffe
6. Verbot von Kryptografie

Dabei sind die unerwünschten Nebeneffekte – also Folgen für die Allgemeinheit – deutlich gravierender und schwieriger zu begrenzen, als dies bisher der Fall war. Im Folgenden gehen wir näher auf diese Möglichkeiten ein und beleuchten die Risiken, die damit einhergehen.

Zugriff am Endgerät

In der Diskussion um staatlichen Zugriff wird oft die Ende-zu-Ende (E2E)-Verschlüsselung als größtes Problem erwähnt, weil hier die Daten nur an den Endpunkten selbst entschlüsselt vorliegen. Eine Zugriffsmöglichkeit stellt die in Deutschland auch als „Bundestrojaner“ bekannte Online-Durchsuchung dar. Hierbei wird unter Ausnutzung von Sicherheitslücken versucht, direkt am Endgerät den Verkehr vor der Verschlüsselung, bzw. nach der Entschlüsselung abzuhören.

Eingriffe am Endgerät sind für den Nutzer unauffällig und nicht nachvollziehbar. Der Staat entdeckt oder kauft also selbst Wissen um Sicherheitslücken, welche anschließend nicht behoben werden, sondern weiter Nutzer gefährden. Alternativ können solche Hintertüren direkt vom Hersteller in Geräte oder Messenger eingebaut werden.

Problematisch ist dabei einerseits, dass die Geräte so beliebig manipuliert werden können, eine Beweissicherung somit höchst fraglich ist. Andererseits werden auf diese Weise künstlich unzählige Endgeräte mit Sicherheitslücken versehen, die früher oder später auch von anderen genutzt werden können und werden.

So musste etwa der Firewall-Hersteller Juniper kürzlich zugeben, dass eine auf Verlangen der NSA eingebaute Hintertür von einem anderen Staat – mutmaßlich China – erfolgreich übernommen wurde [8]. Bekannt geworden sind in diesem Bereich auch Fälle wie Apple, die seitens des US-amerikanischen FBI zur Mithilfe beim Knacken von Smartphones verpflichtet wurden, oder durch die NSA auf dem Versandweg mit Hintertüren manipulierte Geräte.

Vorsätzlich eingebaute Hintertüren sind ein reales Phänomen [9] und werden immer wieder mit gut- oder böswilligem Hintergrund entdeckt. Nutzer werden dadurch einem hohen Sicherheitsrisiko ausgesetzt. Für Hersteller mit dem TeleTrusT-Vertrauenszeichen IT Security made in Germany, zu denen auch genua gehört, ist es aus gutem Grund Bedingung, dass ihre Produkte keine Hintertüren enthalten dürfen.

Zweitschlüssel

In der Politik wird bei komplexen technischen Themen gerne mit greifbaren Analogien gearbeitet, so auch beim oft genannten „Generalschlüssel“ für verschlüsselte Daten. Im Gegensatz zu mechanischen Schlössern kennen die bewährten Algorithmen allerdings kein Konzept von mehreren Schlüsseln, eine Kommunikation zwischen zwei Partnern ist entweder sicher oder nicht sicher. Zum Mitlesen muss der Angreifer daher entweder im Besitz der Schlüssel, bzw. der Geheimnisse der Kommunikationspartner sein, oder die Nachricht muss noch einmal extra für ihn verschlüsselt werden.

In der Praxis teilweise aus Performance-Gründen verwendete Gruppenschlüsselverfahren (z. B. in VPNs) verletzen oft kryptografische Grundbedingungen und sind entsprechend eingeschränkt sicher [10]. Will man eine Nachricht für n Empfänger gleichzeitig sicher verschlüsseln, geht dies nur über Umwege. Beim für E-Mail-Verschlüsselung verwendeten Standard S/MIME wird hierzu beispielsweise ein zufälliger Schlüssel S_M generiert, mit dem die Nachricht selbst symmetrisch verschlüsselt wird. Anschließend wird ein asymmetrisches Verfahren, d.h. eine Verschlüsselung, die keinen vorherigen Schlüsselaustausch erfordert, verwendet. Damit wird S_M für jeden Empfänger jeweils kopiert und verschlüsselt und mit der Nachricht verschickt. So kann jeder Empfänger S_M für sich entschlüsseln.

Ein Staat könnte folglich vorschreiben, bei jeder Nachricht immer auch für einen staatlichen Zweitschlüssel mitzuverschlüsseln.

Als Variante wird auch ein Key Escrow vorgeschlagen, bei dem ein werksseitig erzeugter Schlüssel direkt hinterlegt wird. Ein bekanntes Beispiel sind die Clipper-Chips der NSA [11]. Der Schlüssel kann dabei auch auf mehrere Parteien aufgeteilt werden, beispielsweise zur Hälfte beim Diensteanbieter und zur Hälfte bei einer staatlichen Behörde. Er wird dann nur bei Bedarf zusammengesetzt, um den Zugriff zu ermöglichen. Alternativ könnten Diensteanbieter wie z. B. WhatsApp gezwungen werden, den initialen Schlüsselaustausch beim Aufbau einer Verbindung derart zu manipulieren, dass sie das Schlüsselmaterial (identisch zu den Kommunikationspartnern) selbst vorhalten können.

Bei allen Verfahren besteht die Herausforderung darin, den Zugriff wirksam gegen Missbrauch zu reglementieren und außerdem zu verhindern, dass die Zweitschlüssel in falsche Hände gelangen. Ein solches System ist nicht nur schwierig zu konstruieren [12], sondern auch ein sehr attraktives Ziel für Angreifer.

Es darf dabei nicht vergessen werden, dass nicht wie bei einem mechanischen Schloss einfach später der Schließzylinder getauscht werden kann. Eine einmal verschlüsselte Datei, die verschickt wurde, lässt sich für immer mit dem Material entschlüsseln, welches eine Überwachungsbehörde dazu vorhalten muss – selbst wenn dieses erst Jahre später bekannt wird. Die Snowden-Leaks legen nahe, dass die NSA mit genau dieser Hoffnung im Utah Data Center im großen Stil verschlüsselte Kommunikation sammelt, um sie zu brechen, wenn effizientere Wege dafür zur Verfügung stehen.

Ein weiteres Problem betrifft zusätzliche Schutzmechanismen, die bei verschlüsselter Kommunikation wichtig sind. Oft werden verschiedene Algorithmen geeignet kombiniert, um weitere Eigenschaften zu erreichen. Ein Beispiel ist die Perfect Forward Secrecy (PFS), welche verhindert, dass alte Daten entschlüsselt werden können, wenn das lokale Langzeitgeheimnis eines Gerätes in falsche Hände gerät. Das Signal-Protokoll unterstützt diese gerade auf verlustgefährdeten Mobilgeräten wichtige Vorkehrung. Auf diese Eigenschaften können verpflichtende Zweitschlüssel fatale Auswirkungen haben.

Abhörschnittstellen beim Diensteanbieter

In einigen Fällen liegt der Verkehr beim Diensteanbieter selbst entschlüsselt vor. Beispiele sind die meisten Webdienste oder normale und Gruppenchats im Messenger Telegram. Ein weiteres Beispiel ist der neue Mobilfunkstandard 5G, der vom Prinzip her in dieser Hinsicht jedoch deutlich mehr Sicherheit als seine Vorgänger bietet. Verschiedene Länder, darunter Deutschland, arbeiten daher auf EU-Ebene auf gesetzlich verpflichtende Abhörschnittstellen und Speicherung des Datenverkehrs bei den Telekommunikationsanbietern hin [13].

Abhörschnittstellen und Datensammlungen ohne zuverlässige Kontrollmechanismen bergen Missbrauchspotential, sowohl von privater als auch staatlicher Seite. So werden z. B. die Inhalte sämtlicher E-Mails in Googles Gmail automatisiert durchsucht, der Konzern nutzte dies für die Personalisierung von Werbung. Spätestens die durch die Snowden-Leaks bekannt gewordenen, illegalen Abhöraktivitäten und Wirtschaftsspionage [14] haben gezeigt, wie wichtig eine effektive Kontrolle von Behörden mit derartigen Fähigkeiten auch in demokratischen Ländern ist. Um sich als Nutzer effektiv vor Zugriffen dieser Art, unabhängig von welcher Seite, schützen zu können, ist eine sichere E2E-Verschlüsselung notwendig.

Schwächung von Kryptografie

Hier wird das Sicherheitsniveau künstlich abgeschwächt, damit es bei Bedarf leichter gebrochen werden kann. Bekannte Fälle sind die US-Exportrestriktionen z. B. für die Schlüssellänge von 3DES. Auch die Verschlüsselung A5/1 des GSM-Mobilfunkstandards wurde in einer weiteren Variante A5/2 deutlich abgeschwächt, kam damit in Europa aber letztlich nicht zum Einsatz. Der mit einer NSA-Hintertür geschwächter Zufallszahlengenerator Dual_EC-DRBG wurde hingegen von der NIST tatsächlich standardisiert und erst nach dem Aufdecken Jahre später entfernt [15]. Ein Teil der in Junipers ScreenOS entdeckten Hintertüren wurde durch eine schwachen Implementierung des Dual-EC-Zufallszahlengenerators verursacht [9]. Dieser Generator basiert wie andere Elliptic Curve Cryptography (ECC)-Verfahren auf elliptischen Kurven, die bei geschickter Wahl das Sicherheitsniveau stark reduzieren.

Von staatlichen Institutionen vorgeschlagene Kurven werden daher oft misstrauisch bewertet. Da sich auch ein IT-Sicherheitsunternehmen wie genua an entsprechenden Standards orientieren muss, wären wir von solchen Schwachstellen direkt betroffen. Fragwürdige staatliche Vorgaben haben somit direkten Einfluss in das Vertrauen der Kunden in IT-Sicherheitsdienstleister.

Natürlich kann prinzipiell fast jede Kryptografie mit entsprechendem Aufwand gebrochen werden. Die Frage ist dabei, wer über die Mittel verfügt und in welchen Fällen es dem Angreifer den Aufwand wert ist. Eine gezielte Abschwächung senkt diese Schwelle für jeden Angreifer. Da eine wichtige Anforderung an Verschlüsselung ist, auch mit zukünftigen Entwicklungen (z. B. schnellere Rechner) noch ausreichenden Schutz zu bieten, ist eine solide Abschätzung der Folgen nicht trivial.

Gerade im Kontext von staatlichen Angriffen und Industriespionage muss zudem auch mit Angreifern mit großen Ressourcen gerechnet werden. Das Risiko besteht also darin, dass damit die Kommunikation von Bürgern, Unternehmen und auch Behörden zu einem zu leichten Ziel auch für andere Angreifer wird.

Man-in-the-Middle (MITM)-Verfahren

Dies stellt ein Verfahren dar, bei dem der Angreifer die Kommunikation aktiv verändert, indem er als Mittelsmann in beide Richtungen die verschlüsselte Verbindung führt und dadurch selbst lesend und schreibend Zugriff auf den unverschlüsselten Verkehr hat. Wenn keine oder unzureichende Authentisierung verwendet wird, ist dies vergleichsweise trivial umzusetzen, sofern man dafür einen geeigneten Zugangspunkt hat.

Als Staat bestehen allerdings auch Möglichkeiten, die Authentisierung zu umgehen: So könnte per gesetzlicher Vorgabe jedes Gerät gezwungen werden, einer staatlichen Certificate Authority (CA) bedingungslos zu Vertrauen. Fortan könnte mit dieser CA ein für das Endgerät gültig erscheinendes Zertifikat für jeglichen Dienst signiert werden. Ein aktuelles Beispiel für dieses Vorgehen ist Kasachstan [16].

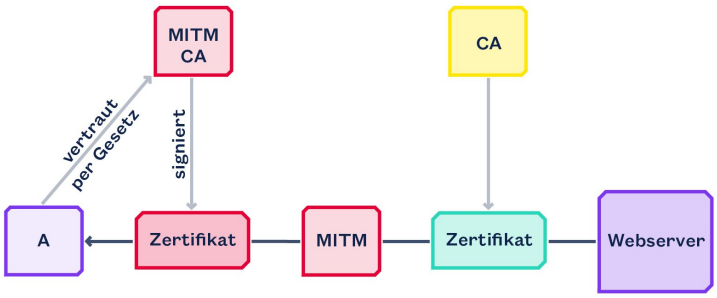

Abbildung 1: Vereinfachte Darstellung Authentisierungs-MITM mit staatlicher CA. Die MITM-Instanz gibt sich dem Endgerät durch das falsche Zertifikat als der Webdienst aus und schaltet sich auf diese Weise zwischen die Verbindung.

MITM-Angriffe erfordern einen vergleichsweise geringen Aufwand. In kleinerem Maßstab genügt ein handelsüblicher Rechner als Plattform. Dies ermöglicht einen großflächigen, automatisierten Einsatz. Gleichzeitig muss der geheime Schlüssel der staatlichen CA auf jeder dieser Instanzen vorliegen, was einen effektiven Schutz dieses Schlüssels schwierig macht. Gelangt er in die Hände eines anderen Angreifers, kann dieser damit fortan jegliche Dienste (E-Mail-Anbieter, Online-Banking, behördliche Portale, Industriesteuerungen, etc.) unbemerkt imitieren und ausspähen. Die staatliche Anwendung von MITM untergräbt damit das grundlegende Vertrauen in die Integrität von elektronischer Kommunikation.

Verbot/Blockade von Kryptografie

Chinas Goldener Schild behindert aktiv den Durchsatz verschlüsselter Verbindungen und treibt Nutzer damit zu unverschlüsselter Kommunikation. In Deutschland ist historisch Verschlüsselung auf den Amateurfunkfrequenzen untersagt.

Ähnlich wie die vorsätzliche Schwächung verhindert ein Verbot von Kryptografie jegliche Möglichkeit, sich vor Überwachung jedweder Seite zu schützen. Der Stellenwert sicherer, elektronischer Kommunikation für Bürger, Wirtschaft und Staat steht selbst in den benannten Vorstößen außer Frage. Selbst wenn Ausnahmen für bestimmte Bereiche zugelassen werden würden, ist eine Entwicklung und Evaluation verlässlicher Sicherheitsprodukte in einem Umfeld strenger Verbote kaum vorstellbar.

Zusammenfassung staatliche Zugriffsmethoden

Ein ganz allgemeines Problem bei staatlicher Regulierung stellt nicht zuletzt die Umsetzung der sogenannte Krypto-Agilität dar. Werden Schwächen in einem genutzten Verschlüsselungsverfahren festgestellt, so muss dieses schnellstmöglich ausgetauscht werden. Hierbei zusätzlich staatliche Vorgaben für einen geregelten Zugriff zu erfüllen und die Auswirkungen zu bewerten, würde diesen Prozess erheblich verzögern.

Es lässt sich also feststellen, dass ein geregelter, allgemeiner Zugriff auf verschlüsselte Kommunikation wie er aus den formulierten Forderungen hervorgehen würde,

erhebliche Risiken mit sich bringt. Die Auswirkungen können dabei sowohl Kommunikation von Personen, Infrastruktur, Industrie und auch Behörden betreffen. Dies exponiert die Teilnehmer gegenüber Kriminellen und gefährdet die deutsche Wirtschaft durch Industriespionage aus dem Ausland. Eine allgemeine Kompromittierung der Sicherheit mit entsprechendem Vertrauensverlust wäre die Folge.

Selbst wenn man die zuständigen staatlichen Organe als vertrauenswürdig einstuft, können diesen Fehler unterlaufen, welche entsprechend massive Auswirkungen nach sich ziehen. Kriminelle selbst können hingegen weiterhin unter Missachtung von Gesetzen starke Kryptografie einsetzen.

Gerade aufgrund der bislang sehr klaren Positionierung gegen staatlichen Einfluss auf Kryptografie genießen deutsche Hersteller für IT-Sicherheitsprodukte einen gewissen Vertrauensvorsprung gegenüber US-amerikanischen oder chinesischen Herstellern. Dieses Argument wäre mit einer entsprechenden Gesetzgebung irreversibel hinfällig, was den gesamten Markt und damit deutsche, bzw. europäische Kompetenz in diesem Bereich gefährdet. Folglich müsste sich die europäische IT noch stärker in die Abhängigkeit von ausländischen Herstellern begeben, wo eigentlich gerade das Gegenteil angestrebt wird.

Insbesondere staatliche Stellen selbst vertrauen gerne auf nationale Hersteller für ihre IT und sollten ein Interesse daran haben, diesen Schlüsselsektor zu erhalten. Als Hersteller von Sicherheits-Appliances spricht sich genua daher gegen derartige Ansätze aus.

Notwendigkeit und gesellschaftliche Konsequenzen

Neben der technischen Machbarkeit stellt sich die Frage nach der Sinnhaftigkeit des Vorstoßes. Zweifelsohne gibt es ein berechtigtes Interesse von Ermittlungsbehörden, in einem klar definierten Rahmen auf Kommunikation von Verdächtigen zugreifen zu können.

Sowohl die elektronische Kommunikation als solche als auch der Einsatz von Verschlüsselung werden weiter zunehmen und die Behörden dadurch vor Herausforderungen stellen. Es müssen Wege gefunden werden, damit umzugehen. Wie so oft geht es um Verhältnismäßigkeit der Eingriffe und darum, diese so gezielt wie möglich vorzunehmen. Wenn der Maßstab für die Verabschiedung von Überwachungsbefugnissen lediglich die Frage ist, was eventuell bei der Verbrechensbekämpfung hilft, könnten wir ebenso die Unverletzlichkeit der Wohnung gänzlich und ohne Vorbehalte aufheben. Wer nichts zu verbergen hat, hat schließlich nichts zu befürchten.

Dieses Narrativ führt dazu, dass alleine die Nutzung von starker Kryptografie schon ein Verdachtsmoment ist. Versierte Verbrecher werden sich im Gegensatz zu normalen Bürgern und Unternehmen dabei kaum an gesetzliche Vorgaben halten, sondern weiterhin starke Kryptografie für ihre Kommunikation verwenden.

Viele Ansätze bedeuten einen massiven Eingriff in die Privatsphäre jeden Bürgers, insbesondere wenn sie unselektiv sind und im Vorfeld großflächig und verdachts-

unabhängig installiert werden müssen. Auf diese Weise werden gesetzestreue Bürger und Unternehmen gezwungen, auf Selbstschutz zu verzichten und sich damit auch gegenüber anderen Angreifern zu exponieren.

Ein unzureichend kontrollierter Zugang zu verschlüsselter Kommunikation birgt zudem ein Missbrauchsrisiko und kann somit selbst in demokratischen Gesellschaften für Journalisten und politische Gegner zum Problem werden. Auch der BND hat nachweislich wiederholt seine Abhörbefugnisse weit überschritten, u.a. am deutschen DE-CIX-Internet-Knoten [17].

Wünschenswert wäre an dieser Stelle eine sachliche Diskussion über alle Aspekte des Problems mit einer objektiven Abwägung der Maßnahmen, statt als Reaktion nur einseitig neue Befugnisse zu fordern.

Viel zu selten wird die Frage in der Diskussion aufgeworfen, welche Möglichkeiten den Behörden einen tatsächlichen Vorteil bringen würden. Noch 2011 wurde in einem US-Bericht veröffentlicht, dass von 3194 dort registrierten Abhörfällen lediglich in sechs Fällen die Kommunikation verschlüsselt war, was in keinem der Fälle die Beweisaufnahme verhindert hat [11]. Nach mehreren der in jüngster Vergangenheit stattgefundenen Attentaten in Frankreich wurde immer wieder die anlasslose Massenüberwachung des Internets – besser bekannt als Vorratsdatenspeicherung – gefordert, um weitere Anschläge zu verhindern. Dabei wurde offenbar vergessen, dass Frankreich dieses Instrument bereits seit 2006 hat. Auch bei anderen Terrorattentaten, bzw. Vorbereitungen im In- und Ausland zeigte sich im Rahmen der Aufarbeitung immer wieder, dass die Attentäter bekannt waren und umfassend überwacht wurden [18].

Ermittlungs- und Kommunikationspannen waren ausschlaggebend, dass die Attentate nicht rechtzeitig verhindert wurden. Die anschließende Beweissicherung und das schnelle Auffinden von Kontaktpersonen war gemäß der öffentlich bekannten Informationen nie das große Hindernis, auch nicht mit der bereits in Deutschland stattfindenden Datensammlung. Selbst von den Behörden wird die Ermittlung der entscheidenden Informationen in großen Datenmengen gerne mit der Suche der Nadel im Heuhaufen verglichen. Ob die Forderung nach noch mehr Heu dabei zielführend ist, darf bezweifelt werden.

In diesem Kontext sind die Forderungen nach mehr Überwachungsbefugnissen sogar kontraproduktiv, da sie von der Aufarbeitung der eigentlichen Missstände ablenken.

Nicht zuletzt entspricht eine verdachtsunabhängig vorhandene Abhörschnittstelle, deren Zustand nicht bekannt ist, genau dem Prinzip eines Panoptikums. Da ein Großteil unserer Kommunikation elektronisch abläuft, riskieren wir eine massive Einschränkung der freien Meinungsäußerung – die Schere im Kopf jedes Einzelnen beginnt zu wirken, lange bevor konkrete Folgen sichtbar oder beabsichtigt werden.

Eine unvorsichtige Einschränkung von Verschlüsselung würde also zwangsläufig zu einer massiven Einschränkung der informationellen Selbstbestimmung führen und betrifft auch die Wirtschaft und Staat, die auf sichere Kommunikationsmittel ange-

wiesen ist. Der Wirtschaftsstandort Deutschland, mit dem politisch getragenen Selbstbild der Vorreiterrolle bei der Digitalisierung, würde durch den Vertrauensverlust irreversiblen Schaden nehmen. Die Frage, wie sich jeder Einzelne vor den erwähnten Risiken - Schlüsselverlust, Schwachstellen in den Verfahren, Missbrauch - schützen soll, bleiben im Entwurf hingegen gänzlich unerwähnt.

Literatur

[1] Auf den Terroranschlag folgt EU-Verschlüsselungsverbot.
https://fm4.orf.at/stories/3008930/

[2] Whitfield Diffie und Susan Landau. Privacy on the Line: The Politics of Wiretapping and Encryption, Updated and Expanded Edition. The MIT Press, 2007. ISBN: 0262042401

[3] LVT-Chef nach weiterer Ermittlungspanne abberufen.
https://www.wienerzeitung.at/nachrichten/politik/oesterreich/2081771-LVT-Chef-nach-weiterer-Ermittlungspanne-abberufen.html

[4] Bericht der Bundesregierung zu den Auswirkungen der Nutzung kryptografischer Verfahren auf die Arbeit der Strafverfolgungs- und Sicherheitsbehörden.
https://www.innenministerkonferenz.de/IMK/DE/termine/to-beschluesse/2002-06-06/anlage-15.pdf

[5] Drucksache 18/5013 Anstrengungen von Europol, INTERPOL und der Europäischen Kommission zum Aushebeln von Verschlüsselungstechniken.
http://dipbt.bundestag.de/dip21/btd/18/051/1805144.pdf

[6] INTERNATIONAL STATEMENT: END-TO-END ENCRYPTION AND PUBLIC SAFETY.
https://assets.publishing.service.gov.uk/government/uploads/system/uploads/attachment_data/file/925601/2020.10.11_International_statement_end-to-end_encryption_and_public_safety_for_publication_final.pdf

[7] Cryptography Law of the P.R.C.
https://www.chinalawtranslate.com/en/cryptography-law/

[8] Spy agency ducks questions about 'back doors' in tech products.
https://www.reuters.com/article/us-usa-security-congress-insight-idUSKBN27D1CS

[9] Stephen Checkoway u. a. A Systematic Analysis of the Juniper Dual EC Incident. Cryptology ePrint Archive, Report 2016/376. https://eprint.iacr.org/2016/376

[10] M. Bellare u. a. Multi-Recipient Encryption Schemes: Efficient Constructions and their Security. https://www.cc.gatech.edu/~aboldyre/papers/bbks.pdf

[11] M. Blaze. „Key escrow from a safe distance: looking back at the Clipper Chip“. In: ACSAC '11. 2011

[12] M. Uma und Ganapathi Padmavathi. „A Survey on Various Cyber Attacks“, IJ Network Security 15.5 (2013), S. 390-396

[13] Drucksache 19/11396 - Europäische Initiativen zur Überwachung der 5G-Telefonie. http://dipbt.bundestag.de/doc/btd/19/121/1912117

[14] BBC: NSA 'engaged in industrial espionage'.
https://www.bbc.com/news/25907502

[15] Did NSA Put a Secret Backdoor in New Encryption Standard?
https://www.wired.com/2007/11/securitymatters-1115/

[16] Kasachstan versucht erneut, sichere Verbindungen zu torpedieren.
https://www.heise.de/news/Kasachstan-versucht-erneut-sichere-Verbindungen-zur-torpedieren-4981706.html

[17] Große Koalition will Geheimdienst-Überwachung legalisieren.
https://netzpolitik.org/2016/wir-veroeffentlichen-den-gesetzentwurf-zur-bnd-reform-grosse-koalition-will-geheimdienst-ueberwachung-legalisieren/

[18] Polizei fahndet nach Tunesier Anis A. https://web.archive.org/web/20161224150141/ http://www.tagesschau.de/inland/suche-tatverdaechtiger-103.html

[18] WhatsApp Encryption Overview.
https://www.whatsapp.com/security/WhatsApp-Security-Whitepaper.pdf

Hintergrundwissen Kryptografie

Zum besseren Verständnis des Themenkomplexes folgen noch einige grundlegende Informationen über die prinzipielle Funktionsweise von gebräuchlichen Kryptografieverfahren.

In der heutigen Kommunikation wird zumeist eine Kombination aus sog. symmetrischer und asymmetrischer Verschlüsselung eingesetzt. Bei einer symmetrischen Verschlüsselung nutzen Sender und Empfänger jeweils den gleichen Schlüssel K für Ver- und Entschlüsselung. Dieser Modus setzt ein gemeinsames Geheimnis voraus, auf welches sich beide vorab geeignet verständigt haben müssen, beispielsweise als pre-shared Key (PSK). Je nach Implementierung kann der statische Schlüssel K selbst dieses Geheimnis sein.

Varianten, wie sie z. B. beim Signal-Protokoll (u. a. in Signal und WhatsApp) zum Einsatz kommen, verwenden für jede Nachricht, bzw. Sitzung einen neuen, symmetrischen ephemeral Key, welcher über ein spezielles Verfahren aus einem Langzeitgeheimnis abgeleitet wird [18]. Dies verhindert, dass bei Bekanntwerden eines dieser temporären Schlüssel jegliche jemals mit dem Langzeitgeheimnis getätigte Kommunikation kompromittiert wird.

Wird durch geeignete Verfahren zudem verhindert, dass bei späterem Bekanntwerden (z. B. durch Diebstahl eines Geräts) des Langzeitgeheimnisses alte ephemeral Keys berechnet werden und damit alte Nachrichten entschlüsselt werden können, spricht man von Perfect Forward Secrecy. Das Signal-Protokoll unterstützt auch diese Eigenschaft. Ein bekannter Algorithmus für symmetrische Verschlüsselung ist der AES.

Bei der asymmetrischen Verschlüsselung generieren die Kommunikationspartner ein Schlüsselpaar, welches aus einem öffentlichen Teil (public Key) und einem geheimen Teil (private Key) besteht. Wird eine Datei mit einem public Key verschlüsselt, so kann sie nur mit dem zugehörigen private Key entschlüsselt werden. Der klare Vorteil hiervon ist, dass vorab kein gemeinsames Geheimnis notwendig ist. Ein bekannter Vertreter ist das RSA-Kryptosystem.

Oft werden beide Varianten kombiniert, da asymmetrische Kryptografie deutlich aufwendiger ist. So kann beispielsweise hierüber ein Schlüssel versendet bzw. vereinbart werden, mit dem die eigentliche Kommunikation dann symmetrisch verschlüsselt wird. Eine Variante davon ist der oft initial verwendete Diffie-Hellman-Schlüsselaustausch.

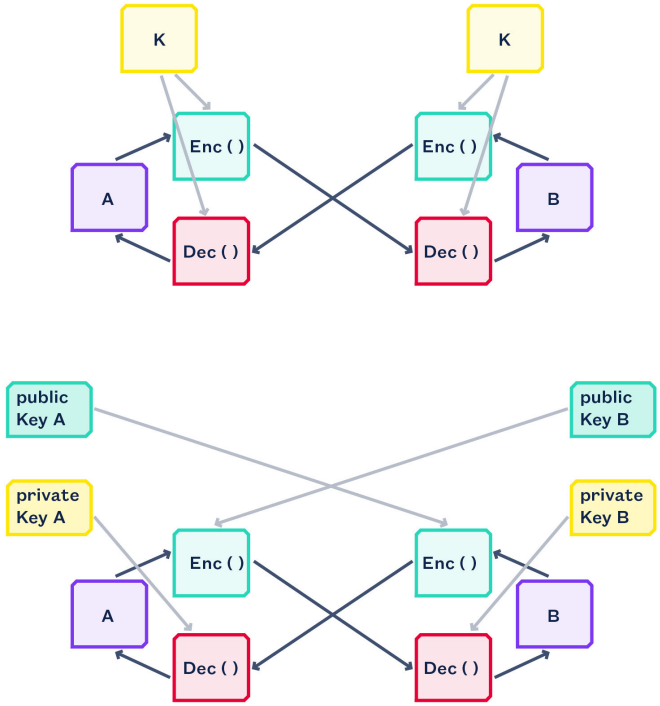

Abbildung 2: Prinzipieller Ablauf von symmetrischer und asymmetrischer Verschlüsselung zwischen den Kommunikationspartnern A und B.

Ein essentieller Teil verschlüsselter Kommunikation ist daneben die Authentisierung der Gegenstelle. Nur beim PSK erfolgt diese implizit. Ein anschauliches Beispiel für kryptografische Authentisierung ist ein HTTPS-Webserver.

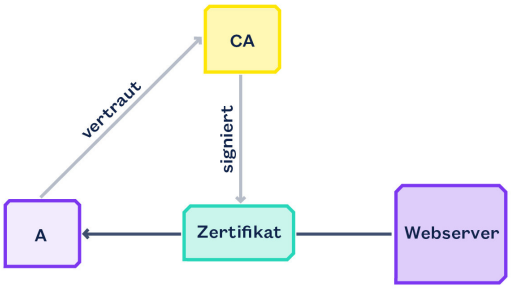

Abbildung 3: Vereinfachte Darstellung einer Authentisierung mittels CA.

In diesem Beispiel liefert der Webserver ein Zertifikat aus, welches von einer Certificat Authority (CA) unterschrieben wurde. Die CA bestätigt damit die Identität des Webservers, auf der anderen Seite vertraut der Browser des Nutzers allen Zertifikaten, die von der CA unterschrieben wurden. In der Praxis werden z. B. X.509-Zertifikate dafür verwendet. Eine andere Variante ist der manuelle Abgleich von Fingerprints von public Keys, um zu verifizieren, dass der zur Verschlüsselung verwendete public Key tatsächlich der des gewünschtem Empfängers ist.

Zuletzt ist es für die Bewertung geregelter Zugriffe noch wichtig, zwischen welchen Endpunkten verschlüsselt wird. So kann einerseits die Nutzung zwischen Anwender und einem zentralen Server verschlüsselt sein. Auf dem Server selbst liegen die Daten dann unverschlüsselt vor, der Diensteanbieter kann jederzeit darauf zugreifen und diese sowohl lesen als auch verändern. Dies ermöglicht gleichzeitig eine Abhörschnittstelle.

Die allermeisten Webdienste arbeiten in dieser Art, aber auch z. B. normale Chats und Gruppen im Messenger Telegram. Demgegenüber steht die Ende-zu-Ende-Verschlüsselung E2E , bei der jede Nachricht nur vom Empfänger entschlüsselt werden kann. Wenn wir beim Beispiel Messenger bleiben, wären dabei WhatsApp, Signal, geheime Telegram-Chats, einige Implementierungen des Matrix-Protokolls sowie Threema zu nennen. Meist wird die Komplexität des Schlüsselmanagements vor dem Nutzer verborgen und automatisiert und stellt damit einen Angriffspunkt dar. Lediglich Threema fordert recht deutlich dazu auf, die Identität der Nutzer manuell zu verifizieren. Die E2E-Verschlüsselung wird im Kontext von staatlichen Zugriffen meist als größtes Problem genannt – bei korrekter Implementierung bedarf es einer direkten Manipulation am Endgerät.