# Sichere Kommunikation

G. Brands[1], C.B. Roellgen[2]

18. April 2016

Angesichts zunehmender Überwachung der Kommunikation durch den Staat, global agierender Cyber-Krimineller und der voranschreitenden Vernetzung selbst banalster Geräte stellt sich die Frage, ob die Kommunikation noch sicher zu gestalten ist und die Gesellschaft sich mit zunehmender Beobachtung und die Absicherung gegen wirtschaftlichen Schaden der Versicherungsbranche überlässt.

Dabei ist die Fragestellung zentral, warum es PGP und X.509-Zertifikate nicht geschafft haben, von der breiten Masse der Anwender verwendet zu werden, obwohl die Lösungen grundsätzlich von jedem Menschen als sinnvoll erachtet und teilweise kostenlos zur Verfügung gestellt werden.

Wir präsentieren hier ein Modell, das eine weitestgehend sichere Kommunikation ermöglicht und welches derart massentauglich ist, dass eine regelrechte Bewegung ausgelöst werden kann. Dazu bedarf es einer offenen Diskussion. Dieser Artikel wird daher „leben“ und damit über die Zeit einige Veränderungen und Anpassungen erfahren.

Dazu muss man wissen, dass jedwede Diskussion über Datenverschlüsselung und Verschlüsselungsalgorithmen immer auf „unterirdischem Niveau“ geführt wird und dass es eine überwältigende Anzahl an Zeitgenossen nur auf das Zerlegen jeglicher Argumente abgesehen hat.

Im Ergebnis bleibt es dann beim heutigen Stand: elektronische Kommunikation zwischen Menschen zu mehr als 99% im Klartext – und das in einer Zeit, in der so mancher Jugendliche mit einem Smartphone in der Hand geboren worden zu sein scheint.

## Ein Wort an die Nutzer

Jeder ist sich darüber im Klaren, dass man seine Wohnung oder sein Auto abschließen muss, um es Dieben nicht zu einfach zu machen. Während im täglichen Leben jeder einen gewissen Aufwand treibt, sich und sein Eigentum zu schützen, scheint auf dem Gebiet der elektronischen Kommunikation die Erwartung vorzuherrschen, Sicherheit sei zum Nulltarif zu haben und man brauche als Nutzer nichts zu tun. DAS IST EIN IRRTUM!! Auch als Nutzer elektronischer Medien ist man gehalten, ein Minimum an eigenem Aufwand für den eigenen Schutz zu treiben. Wer dazu nicht bereit ist, dem gebührt auch kein Mitleid, wenn Kriminelle ihn ausnehmen.

Vielfach hört man „die Sache ist so kompliziert, dass man sie nicht versteht“. Das stimmt nicht. Es gibt viele Leute, die regelmäßig zu Selbstverteidigungskursen gehen, um sich gegen böse Wichte zu schützen. Effektive Selbstverteidigung ist wesentlich komplizierter als viele elektronische Schutzmaßnahmen. „Zu kompliziert“ ist lediglich eine Ausrede, die eigene Trägheit zu verstecken.

Auch heißt es oft „ich habe nichts zu verbergen“. Da sollten Sie nicht zu sicher sein! Was gestern noch lustig und harmlos erschien, hat so manchen den Job oder den Partner gekostet oder nach Drehen des politischen

1 Gilbert Brands, D-26736 Krummhörn, e-mail: gilbert(at)gilbertbrands.de

2 Bernd Röllgen, D-35576 Wetzlar, e-mail: roellgen(at)globaliptel.com

Windes einen kostenlosen Aufenthalt in gesiebter Luft nach sich gezogen. Man hat vor seinen Angehörigen vielleicht nichts zu verbergen, aber sicherlich vor Menschen, die man nicht persönlich kennt.

## Laws and Emotions

Vor der Technik wirft man sinnvollerweise einen Blick auf die gesellschaftspolitischen Rahmenbedingungen. Geschichte wiederholt sich öfter als man denkt. Kurz nach dem 2. Weltkrieg war das Briefgeheimnis aus gutem Grund ein unverzichtbarer Bestandteil jeder ernst zu nehmenden Verfassung.

Artikel 10 des Grundgesetzes garantiert das Briefgeheimnis. Beschlagnahmte Briefe dürfen grundsätzlich nicht durch Polizei oder Staatsanwalt geöffnet werden, sondern nur durch einen Richter. Als verschlossene Sendung gilt übrigens auch die Postkarte.

1949 lautete der Artikel 10 des Grundgesetzes: „Das Briefgeheimnis sowie das Post- und Fernmeldegeheimnis sind unverletzlich. Beschränkungen dürfen nur auf Grund eines Gesetzes angeordnet werden."

Der zweite Satz wurde freudig zum Anlass genommen, am Grundrecht wie mit einer Kettensäge zu modellieren. Seit 1968, als Teil der Notstandsgesetze, lautet Art. 10 GG:

> „ (1) Das Briefgeheimnis sowie das Post- und Fernmeldegeheimnis sind unverletzlich.
>
> (2) Beschränkungen dürfen nur auf Grund eines Gesetzes angeordnet werden. Dient die Beschränkung dem Schutze der freiheitlichen demokratischen Grundordnung oder des Bestandes oder der Sicherung des Bundes oder eines Landes, so kann das Gesetz bestimmen, daß sie dem Betroffenen nicht mitgeteilt wird und daß an die Stelle des Rechtsweges die Nachprüfung durch von der Volksvertretung bestellte Organe und Hilfsorgane tritt."

Laut [1] wurden im Jahr 2010 alleine durch deutsche Geheimdienste 37 Millionen E-Mails und Verbindungsdaten analysiert. Die „Nachprüfung durch von der Volksvertretung bestellte Organe und Hilfsorgane" ist offensichtlich nicht gewährleistet.

Mit der NSA ist zudem ein Ableger des U.S.-Verteidigungsministeriums mit der systematischen Generierung von Profilen über die gesamte Menschheit betraut. Diese Organisation muss sich nicht an die europäische oder deutsche Gesetzgebung halten. Sie hatte im Gegenteil in der Vergangenheit sogar Schwierigkeiten, sich an die Gesetze des eigenen Landes zu halten. Die Geheimdienste anderer Staaten werden logischerweise analog zur NSA verfahren.

Offensichtlich verfügen Privatpersonen und Firmen über Informationen, die relevant für das Verteidigungsministerium der USA und anderer Länder sind (JA, SIE LESEN RICHTIG! ES IST DAS MILITÄR), obgleich eine Vielzahl versendeter Nachrichten auf vorteilhafte Weise als „banal" charakterisiert werden kann.

Der jüngeren Leserschaft ist mittlerweile sogar der Schutz der Privatspäre fremd. Worte wie „das Briefgeheimnis sowie das Post- und Fernmeldegeheimnis sind unverletzlich" rufen heute Verwunderung und Unglaube hervor, wenngleich diese Erkenntnis aus den bittersten Erfahrungen mehrerer Generationen gewonnen wurde.

Es ist rechtlich einwandfrei für EU-Bürger und für in der EU ansässige Firmen, ihre Kommunikation gegen das massenhaftes Abhören zu sichern und das wird, vorbehaltlich grundlegender politischer Verwerfungen, auch so bleiben.

Sicher kommunizieren kann man auf elektronischem Wege nur, wenn man die Nachrichten verschlüsselt und zudem weiß, dass man mit dem richtigen Partner kommunziert. Zwar lassen sich auch aus vielen nicht oder nur schwer verschleierbaren Daten wie Verbindungen oder Standorten erhebliche Informationsgewinne erzielen, aber die wesentlichen schädlichen Auswirkungen des Ausspähens lassen sich durch Verschlüsselung weitestgehend beseitigen. Trotz aller in den Medien berichteten bedenklichen Fällen bleibt jedoch bislang die breite Reaktion der Gesellschaft aus. Verschlüsselt werden zwar zunehmend Webseiten, aber fast alle anderen Bereiche tauschen Daten unverschlüsselt aus.

## Das Versagen aktueller Lösungen

Außer den emotionalen Einflüssen arbeiten auch konzeptionelle Probleme am fehlenden Sicherheitsbewusstsein mit, sind womöglich sogar der größere Hemmschuh, den es zu überwinden gilt. Es gibt heute gute Lösungen zur Verschlüsselung von Nachrichten jedweder Art. Offenbar hat sich jedoch keine davon als massentauglich erwiesen.

X.509-Zertifikate zum Beispiel: Salopp ausgedrückt sollen die Leute Zertifikaten vertrauen, weil irgendjemand, den sie auch nicht kennen und schon gar nicht vertrauen, diese signiert hat (eine Signatur ist ein nicht fälschbarer Zusatz, der die Echtheit der Daten bestätigen soll; im klassischen Sinn ein Dienstsiegel mit Unterschrift, aber eben elektronisch). Obwohl immer wieder vorgeschoben, ist mit Zertifikaten i.d.R. auch keine Rechtssicherheit verbunden. Nicht alle Aussteller erfüllen die Voraussetzungen des Signaturgesetzes aus dem Jahre 2001, und längst nicht alle Zertifikate dieser Aussteller fallen in diese Kategorie. Außerdem ist das Verfahren kostspielig: wenn man selbst eine Webseite betreibt, sind die Kosten des Zertifikats nicht selten so hoch wie die für den Webhoster, und das für Nichtstun. Diese Lizenz zum Gelddrucken, an dem alle großen Unternehmen irgendwie beteiligt sind, zusammen mit dem aufwändigen Drumherum schränkt den Nutzerkreis auf Serverbetreiber ein; Privatpersonen halten sich – mit Recht und nicht aus Trägheit, kann man vermerken – fern. Die neuen Personalausweise mit Chip wären eine Möglichkeit gewesen, das Problem aus der Welt zu schaffen. Die Regierung hätte durchaus einen Coup landen können. Es zeigt sich wieder einmal, dass der Anwender letztlich für seine eigene Sicherheit verantwortlich ist.

Das Konzept ist somit durchaus zum Absichern von Betriebssystemen und verschlüsseltem Websurfen auf kommerziellen Seiten geeignet und dort auch erfolgreich im Einsatz, kann jedoch prinzipbedingt nirgends sonst punkten. Vertrauen im Bereich der E-Mails ist hingegen völlig sinnlos, weil lediglich der Verkehr zwischen privatem Rechner und dem Server verschlüsselt wird und an zentraler Stelle immer mitgelesen werden kann – und zwar massenhaft, und im Bereich der Streaminganwendungen (Telefonie, Chats, usw) tut sich mehr oder weniger nichts, wenn auch einige Anbieter inzwischen proprietäre Lösungen anbieten (WhatsApp, Telegram, Threema, usw.).

PGP verfolgt einen grundlegend massentauglicheren Ansatz: Anwender erzeugen sich ihre Schlüsselpaare einfach selbst. Man behält dabei den privaten Teil der Schlüssels für sich und schützt ihn möglichst vor Diebstahl. Der öffentliche Teil der Schlüssels kann beliebig unter Freunden, Bekannten oder sogar „Nicht-Freunden“ herumgereicht werden. Jeder, der den öffentlichen Schlüssel eines Anwenders „Bob“ kennt, kann Bob eine verschlüsselte Nachricht schicken. Nur Bob kann diese entschlüssen. Bob kann verschlüsselt antworten, sodass nur die beiden Kommunikationspartner die Daten entschlüsseln können. Ein wirklich tolles Prinzip!

Um die in den 1990-ziger Jahren in den USA geltenden Exportbeschränkung zu umgehen, wurde der Quellcode 1995 in dem Buch „PGP Source Code and Internals“ vom Autor Phil Zimmermann veröffentlicht. Als man ihm den Prozess machen wollte, wurde schnell klar, dass die Behörden das Verfahren nicht knacken konnten, wodurch PGP zum Erfolg wurde. Seitdem wendet man in den USA die sehr erfolgreiche Methode des „Bashing“, um neue Verschlüsselungsverfahren in Grund und Boden zu „diskutieren“.

Jürgen Schmidt von heise.de charakterisiert den Zustand von PGP in [3] in diesem Sinne besonders unzutreffend: *„... PGP ist technisch veraltet, schon auf PCs schwer zu bedienen und auf Smartphones ein nahezu hoffnungsloser Fall. Allein die Existenz dieses Dinosauriers blockiert die Entwicklung neuer, innovativer E-Mail-Verschlüsselungstechniken.*

*Das zentrale Problem aller Verschlüsselungskonzepte - die Verwaltung der Schlüssel - schiebt PGP komplett auf den Anwender ab. Er muss sich nicht nur um seine eigenen Schlüssel kümmern, sondern sogar um die aller Leute, denen er Mails schicken will. Das Resultat: Mehr als die Hälfte der PGP-verschlüsselten Mails, die mich in den letzten Monaten erreichten, kann ich nicht lesen. Irgendwer kann sie entschlüsseln - aber nicht ich. Sie wurden nämlich mit gefälschten Schlüsseln erstellt, die irgendein Scherzkeks auf meinen Namen ausgestellt und auf die Key-Server geladen hat...*

*Wie gute Ende-zu-Ende-Verschlüsselung heute aussehen muss, demonstriert Apple mit iMessage: Millionen von iPhone-Besitzern wissen nicht einmal, dass sie ihre Kurznachrichten verschlüsseln. Das Chat-Programm TextSecure zeigt, wie man das in Bezug auf Offenheit und Sicherheit noch verbessern kann und dass es keinen Multi-Milliarden-Dollar-Konzern braucht, um das umzusetzen.*

*Wir brauchen auch für E-Mail solche massentauglichen Verschlüsselungssysteme. Doch statt weiter zu versuchen, den lahmenden Dinosaurier PGP aufzupäppeln, sollte man ihn lieber aussterben lassen. Das schafft Raum für Neues - es ist höchste Zeit, die Arbeit an zeitgemäßen Nachfolgern aufzunehmen."*

Schmidt hat Recht – und wieder auch nicht. PGP als solches ist nicht technisch veraltet, im Gegenteil. Sein Einsatzspektrum ist aber auf Datenverschlüsselung wie beispielsweise in E-Mails beschränkt und umfasst keine Stromverschlüsselung wie in Telefonaten oder Messenger-Anwendungen. PGP ist schwer zu bedienen, ja, aber nur, weil sich insbesondere ein de facto Monopolist aus den USA sich standhaft weigert, die Schnittstellen sinnvoll zu unterstützen (wir erwähnten schon die Verstrickung in das gewinnträchtigere X.509-Geschäft; es werden selbst freie X.509-Versionen blockiert, auf die auch Privatleute aufspringen könnten, weil der Kostenfaktor entfällt). PGP überlässt die Schlüsselverwaltung dem Anwender – wie wir noch nachweisen werden, eine sehr sinnvolle Strategie für eine allgemeine Sicherheit, die lediglich modernisiert werden müsste. PGP kann zwar die Gesamtbedürfnisse nicht erfüllen, aber die Tür von einem zumindest für E-Mails sehr brauchbaren Verfahren, das relativ leicht massentauglich aufgerüstet werden könnte, zuzuschlagen bedeutet nichts anderes, als die Tür für die Massen zuzuschlagen, zumal die anderen von Schmidt erwähnten Verfahren nicht in der Lage sind, die Lücke zu füllen.

Gesucht wird ein massentaugliches Verschlüsselungssystem. Nur für E-Mails und Websites wird das heute nicht mehr ausreichen, auch Telefonie, Streaming und Messenger-Dienste müssen enthalten sein. Chat könnte eine ausbaufähige Basis sein. Quelloffen muss die API auf jeden Fall sein. Die eierlegende Wollmilchsau kann es jedoch nicht sein. Perfekte Sicherheit und einfachste Bedienung auf möglicherweise von Trojanern verseuchten Endgeräten schließen sich jedenfalls gegenseitig aus.

Nach nahezu 20 Jahren intensiver Erfahrungen mit der Diskussion über Datenverschlüsselung und Verschlüsselungsalgorithmen lassen sich eine Reihe ernüchternder Erkenntnisse festhalten:

- Öffentliche Diskussionen und Diskussionen zwischen Experten werden IMMER auf „unterirdischem Niveau" geführt
- 99% der Beiträge haben ausschließlich das Zerlegen jeglicher Argumente zum Ziel
- Lösungen sind grundsätzlich „Snakeoil" (betrügerische Machenschaften)
- Es bleibt (außer natürlich bei den Angreifern, die irgendwie immer über die neueste Technik verfügen) alles wie gehabt: Heute wird – wie vor 20, 40 oder 60 Jahren immer noch mehr als 99% der elektronischen Kommunikation zwischen Menschen im Klartext abgewickelt.

Die äußerst wünschenswerte Diskussion über ein massentaugliches Verschlüsselungssystem wird unvermeidbar auf die übelste Art und Weise torpediert werden. Üblicherweise treten Personen wie Bruce Schneier erst dann auf, wenn etwas Unerwünschtes zum Mainstream wird. Viele Menschen wissen nicht dass Schneier beim U.S. Verteidigungsministerium (DoD) gearbeitet hat, dem die NSA untersteht. Bei wikipedia.org kann man seit einigen Jahren natürlich nichts mehr drüber nachlesen. Nicht nur seit Isaac Newton weiß man dass der Apfel - aus welchem Grund auch immer - nicht weit vom Stamm fällt.

Die Abwehr böswilliger Kommentare ist bei Verschlüsselungsprojekten erfahrungsgemäß eine zeitintensive, jedoch notwendige Arbeit. Alleine schon deshalb ist es erforderlich, sich zu organisieren.

Aus den meisten Kommentaren lassen sich jedoch fast immer verwertbare Erkenntnisse gewinnen, so auch aus den Kommentaren zum obigen Artikel:

*„Die einzige Instanz, die an Privatsphäre interessiert ist, ist die Person, um deren Privatssphäre es geht und deshalb gehört auch da die Schlüsselverwaltung hin. Die im Artikel beschriebenen Probleme sind einfach zu umgehen, in dem Sie die Schlüsselserver außen vorlassen und Ihren Nachrichten standardmäßig einfach Ihren öffentlichen Schlüssel anhängen und das Ganze signieren."*

*„Wenn man erfolgreiche und beliebte Software analysiert, wird man folgende Aspekte festellen:*

*1. Software muss einfach sein! ...*

*2. Jeder sollte Software bedienen können! Flache Lernkurve! Software dient nicht dem Selbstzweck eine Technik umzusetzen. Sie dient dazu benutzt zu werden.*

*3. Technik muss in den Hintergrund! ..."?*

*4. Gute Softwarentwickler müssen sich auch Gedanken über den Benutzer machen und nicht nur um technische Aspekte. ...“*

*„Sinnvoll ist eine Möglichkeit, sich die Public Keys direkt beim Adressaten abzuholen, und das könnten die Mailer unauffällig im Hintergrund abwickeln. Im schlimmsten Fall dauert es einen Tag länger, bis die Mail da ist, das ist aber auch alles. Im Vergleich zur Flaschenpost früherer Zeiten immer noch schnell genug.“*

## Ein schwacher Lichtblick ?

Zweifelsfrei hat sich die aktuell verfügbare Verschlüsselungssoftware nicht durchgesetzt und sogar den breiten Einsatz von Datenverschlüsselung verhindert. Einige der Schwächen sind jedoch durchaus erkannt worden und die Dinge scheinen lösbar zu sein. Ein aktuelles Beispiel zeigt sogar dass sie lösbar sind:

Wenngleich es Telekommunikationsanbietern in Europa verboten ist, Ende-zu-Ende zu verschlüsseln, bietet seit kurzem der bekannte Dienst WhatsApp genau dies an (wir beschränken die Diskussion hier auf WhatsApp, weil es der größte und bekannteste Dienst ist. Telegram, Threema und andere bieten die End-2-End-Verschlüsselung schon länger an, Threema sogar im Gruppenmodus, was die anderen Anbieter noch nicht angedacht haben. WhatsApp als Begriff in diesem Paper kann daher jederzeit mit einem der anderen Systeme ausgetauscht werden). In einem neueren Beitrag des gleichen Redakteurs (Jürgen Schmidt) [4] steht zu lesen:

*„Verschlüsselung für die Massen: WhatsApp wird mit einem Schlag zum meistgenutzten Krypto-Messenger. Jetzt müssen wir zeigen, dass uns Privatsphäre wichtig ist: "Ohne Ende-zu-Ende-Verschlüsselung machen wir es nicht mehr", fordert Jürgen Schmidt.*

*WhatsApp bringt uns funktionierende Ende-zu-Ende-Verschlüsselung, die auf technisch höchstem Niveau arbeitet und dabei nicht einmal weh tut. Man muss nichts zusätzlich installieren, keine Schlüssel erzeugen, zertifizieren oder herunterladen – es funktioniert einfach.*

*Wenn ich meiner Freundin eine WhatsApp-Nachricht schicke, wird die selbst WhatsApp nicht mehr lesen und auch nicht speichern können. Wenn das BKA oder FBI bei WhatsApp vorbei kommt und sagt: "Wir wollen jetzt die Nachrichten des Jürgen Schmidt der letzten Jahre haben", kann WhatsApp nur mit den Schultern zucken: "Haben wir nicht, bekommen wir auch nicht mehr rein." ...“*

Ob Anfragen durch Behörden tatsächlich wie in dem (vermutlich nicht sonderlich ernst gemeinten) Szenarium abgefrühstückt werden, bleibt abzuwarten.

Es ist jedoch tatsächlich technisch möglich, dass Massen von Menschen abhörsicher kommunizieren können und dabei noch nicht einmal von der Verschlüsselungsmaschinerie Kenntnis haben. Wesentlich ist dabei der Begriff Ende-zu-Ende- oder end-2-end-Verschlüsselung, d.h. die Nachricht wird bei Erzeuger verschlüsselt und erst beim Konsumenten wieder entschlüsselt, dazwischen aber nicht (!).

Bissige, wenn auch ernst zu nehmende Kommentare auf den Beitrag [4], haben beispielsweise diesen Inhalt:

*„- Nicht jeder nutzt Facebook/WhatsApp. An manchen Stellen (Schulen, Behörden) ist eine Nutzung geradezu verboten.*

*- Die WhatsApp Software schnüffelt noch genau so in meiner Privatsphäre herum wie zuvor. Meine Kontakte und Bilder werden gelesen und abgeglichen.*

*- Steht in den Nutzungsbestimmungen immer noch, dass die WhatsApp Software mein Mikrofon nutzen darf wann immer sie "will"? Dann ist diese Software sowieso schon unten durch und die Nutzung in vielen Szenarien (Praxen, Behörden, ...) illegal.*

*- Die ach so tolle Verschlüsselung ist Closed Source. Keiner weiß wer wirklich mitlesen kann. Wo ist der private key? Viele Fragen sind offen, ganz im Unterschied zu richtigen Messengern, die ordentlich verschlüsseln.“*

Abgesehen vom Closed Source-Vorwurf wird hier eine weitere Baustelle angesprochen, ohne dass die Kommentatoren das bemerken, und diese hat gar nichts mit Verschlüsselung zu tun. Ein Problem ist nämlich das weiterhin unzureichende Rechtemanagement der Betriebssysteme, das gar keine andere Möglichkeit lässt, den Anwendungen Rechte an Systemressourcen zu geben, die sie zum Teil gar nicht benötigen. Die Windows-Welt kümmert sich selbst in den neuesten Versionen nicht oder nur marginal um eine Rechteverwaltung aus Sicht der Nutzerinteressen, und selbst Linux tut sich schwer, Nutzerfreundlichkeit mit funktionierenden Anwendungen zu vereinbaren und wird durch Ableger wir Android eher stark aufgeweicht als verbessert. Eine eigenartige Geisteswelt spiegeln die Kommentare allerdings doch wider: man misstraut den Verschlüsslern, dass sie gesicherte Nachrichten doch verraten könnten, denkt sich aber nichts dabei, die Nachrichten gleich ganz unverschlüsselt zu senden.

Die hohe politische Brisanz des Themas wird in [5] deutlich:

*„Warum WhatsApps neueste Funktion Terroristen gelegen kommen dürfte ...*

- *WhatsApp ist jetzt komplett verschlüsselt.*
- *Experten loben das System als sehr sicher.*
- *Für Ermittler erschwert das die Arbeit weiterhin.*

*... „Die Verschlüsselung von WhatsApp macht unsere Ermittlungen auf jeden Fall schwieriger“, erklärt Georg Ungefuk, Staatsanwalt bei der Zentralstelle zur Bekämpfung der Internetkriminalität. Diese sei ohnehin auch bisher schon kompliziert gewesen, wie Ungefuk ausführt. Wenn die in Hessen sitzende Internetkriminalitätsbehörde eine Information von WhatsApp benötigt, muss sie Rechtshilfe bei Kollegen in den USA beantragen. Ein langwieriger und formal aufwändiger Prozess, der über mehrere Behörden, Landes- und Bundesministerien läuft.*

*... Sicher ist jedoch, dass Kriminelle zum Leidwesen der Ermittler schon jetzt zahlreiche Methoden haben, um ihre Spuren digital zu verschlüsseln. WhatsApp ist nun eine mehr.*

*...Oder wie er (WhatsApp-Chef Jan Koum) in seinem Blog ganz persönlich und pathetisch schreibt: „Ich bin während der Herrschaft der Kommunisten in der Sowjetunion aufgewachsen und die Tatsache, dass Menschen nicht frei sprechen konnten, ist einer der Gründe, warum meine Familie nach Amerika ausgewandert ist. Heute verwenden mehr als eine Milliarde Menschen WhatsApp, um mit ihren Freunden und ihrer Familie auf der ganzen Welt in Kontakt zu bleiben. Jetzt kann jeder einzelne von ihnen frei und sicher auf WhatsApp sprechen.“ “*

Es ist ein Leichtes sich vorzustellen, welcher Druck auf einem kleinen Unternehmen oder auf einer kleinen Gruppe „Nerds“ lastet, die sichere Kommunikation für Alle anbieten möchte. Die Frage ist nur, weshalb diese Aufregung bei den politischen Instanzen herrscht. Methoden, sich in der Kommunikation durch Verschlüsselung wirksam abzusichern, gab es schon immer, und man darf wohl davon ausgehen, dass der Bachelor-Abschluss „Terrorist“ neben Waffen-, Bomben- und Infiltrationskunde auch ein Pflichtnebenfach „Kommunikationsabsicherung“ beinhaltet.

## Wie muss eine massentaugliche Lösung konzipiert sein?

Kommen wir nun etwas näher an ein technisches Konzept. Das hat mit zwei Problemen zu kämpfen: WhatsApp kann sich möglicherweise erlauben, die Gesetze einer Reihe von Ländern zu brechen. Eine ernst zu nehmende Peer-to-Peer-Verschlüsselung ruft jedoch unweigerlich die Behörden auf den Plan. Spätestens wenn Terroranschläge mit einem derartigen Dienst in Verbindung gebracht werden, zeigt sich ob es von vornherein eine geheime Vereinbarung mit den Behörden gegeben hat. Es geht somit um viel mehr als um die Technik. Ohne einen Stab von Rechtsanwälten ist ohnehin nicht viel zu machen.

Die Technik ist wichtig. Eine neue Technik gegen Bestehendes einzuführen ist schon ein Problem an sich, aber glücklicherweise ist die Zeit dazu derzeit äußerst günstig. Im Rahmen der Entwicklung möglicher Quantencomputer sind eine Reihe äußerst lautstarker Trommler unterwegs, die jedem, der es hören will, und auch denen die es nicht hören wollen verkünden „**RSA & Co sind tot!**“. Ob nun berechtigt oder nicht, der eine oder andere, der noch weniger Ahnung von der Sache hat als die Trommler, gerät in Panik, und damit ist der Weg für Neues schon halbwegs planiert. Die Erfahrung lehrt jedoch dass Organisation und Anwendbarkeit mindestens genauso wichtig sind.

### Technik:

| Eigenschaft | Wichtigkeit | Kommentar |
|---|---|---|
| Public Key Verfahren | notwendig | Public Key wie bei PGP ist die Basis einer optimalen Lösung |
| Schlüsselverwaltung lokal | notwendig | Jeder soll für seine Schlüssel selbst sorgen (wie bei PGP). Zentralen Stellen vertraut niemand. |
| Schlüsselserver | In geschlossenen Nutzerkreisen zwingend notwendig, in offenen Kreisen ggf. hilfreich, aber nicht notwendig | Probleme in offenen Kreisen wie bei PGP, Abhilfe ist jedoch durchaus möglich. |
| Verschlüsselung von E-Mails | notwendig | Unter einigen Betriebssystemen nur mittels Plug-Ins und damit nur SEHR lückenhaft realisierbar, teilweise Kompatibilitätsprobleme |
| Verschlüsselung von Chatnachrichten und Dateitransfers | notwendig | Lückenlos realisierbar, plattformabhängig |
| Verschlüsselung von Telefonie | notwendig | Realisierbar, jedoch anfänglich mit geringer Durchdringung |
| Streaming | notwendig | Realisiert, aber proprietär |

### Usability:

| Eigenschaft | Wichtigkeit | Kommentar |
|---|---|---|
| Für den Anwender unmerkbare Integration von Verschlüsselung und Schlüsselmanagement | notwendig | Machbar, jedoch ist die Lösung alles andere als trivial, wenn Anwender den Computer wechseln oder mehrere Endgeräte verwenden.<br>Einfachste Anwendbarkeit ist das zentrale Kriterium schlechthin. |
| Hohe Sicherheit | optional | Gesetzliche Bestimmungen und allgemeine Grundsätze machen Hochsicherheit zu einem Profifeature für Firmen, Regierungen und Verwaltungen. Das dazu nötige Fachwissen wird eher in IT-Abteilungen zu finden sein. |
| Einfache Begriffe und Erklärungen | notwendig | Einer der schwersten Fehler der Vergangenheit |

| | | |
|---|---|---|
| | | darf nicht wiederholt werden. Alleine die Dokumentation erfordert das Vorhandensein einer Organisation, die Wildwuchs in Quelltexten und Beschreibungen eindämmt. |
| Nutzermitwirkung | notwendig | Eine Eigenverantwortung des Nutzers für die Sicherheit seiner Daten ist zwingend notwendig, das Bewusstsein ist aber gerade auf dem Gebiet der elektronischen Kommunikation wenig bis gar nicht ausgeprägt. Statt wie bisher Unternehmen bei Pannen die Schuld zuzuweisen, ist vorzugsweise der Nutzer in die Pflicht zu nehmen (nur Rechte geht nicht). |

## Organisation:

| Eigenschaft | Wichtigkeit | Kommentar |
|---|---|---|
| Non-profit Organisation, die nicht aufgekauft werden darf. | notwendig | Der Kauf von PGP durch McAfee im Jahre 1997 hat gezeigt, dass man nicht lange auf „Ableger“ warten muss. Aus der Vergangenheit muss gelernt werden. |
| Open Source | notwendig | Die API, welche das Schlüsselmanagement übernimmt, muss quelloffen sein. Es ist nicht zu erwarten, dass alle Mailclients, Telefone und Messenger quelloffen sein werden. Erfolg ist nur durch Unterstützung quelloffener, als auch geschlossener Anwendungen möglich. |
| Finanzierung durch Crowd Funding und Spenden | sinnvoll | Als Incentive bei Crowd Funding könnte beispielsweise die Verfügbarkeit von Profifeatures dienen. Spendenfinanzierung durch die Industrie und durch Privatleute ist bei adequater Visibilität wahrscheinlich. |
| Sitz der Organisation in einem politisch stabilen Land | notwendig | Die Schweiz als stabile Demokratie, aktuell auch der Kernbereich der EU, sind geeignet. |
| Politische Unabhängigkeit | notwendig | Ein derartiges Projekt darf niemals Sklave einer Regierung sein. |
| Legalität | sinnvoll | In China wird ein derartiges Projekt grundsätzlich vom Staat als illegal angesehen. Als Massstab kann aktuell beispielsweise der Kernbereich der EU angesehen werden. |
| Einschränkungen der Sicherheit für freie Versionen | notwendig | Allgemein gilt in der EU, den USA, Kanada und der Schweiz die Grenze von 56 Bit für symmetrische Verschlüsselung, sofern der asymmetrische Teil sicherer als 512 Bit (für DH und RSA) ist. Diese Grenze ist in Anbetracht der politischen Lage seit dem 11. September 2001 zwar ärgerlich, jedoch durchaus zu verstehen. Die breite Masse von Menschen lässt sich mit 56 Bit symmetrisch durchaus schützen.<br>Hinweis: für kommerzielle Lösungen, die eine Kontrolle der Verbreitung erlauben, besteht diese Einschränkung nicht. |
| Abwehr böswilliger Kommentare | notwendig | Meist sind Kommentare frei von belastbaren Inhalten. Schlecht organisierte Projekte scheitern häufig daran. Eine der zentralen Aufgaben der Organisation ist es, Verbesserungsvorschläge von Bashing zu trennen und auf Bashing fachgerecht |

| | | |
|---|---|---|
| | | zu antworten. Damit lässt sich erfahrungsgemäß jedes böswillige Argument entkräften. |
| Abwehr von Klagen durch Staaten und durch Behörden | notwendig | Massenhaftes Abhören ist bei Erreichen einer bestimmten Größe nicht mehr möglich. Eine Fülle von Behörden aus aller Herren Länder werden die Organisation mit hoher Sicherheit schikanieren und gegebenenfalls verklagen. |

## Technische Details

Eine grundlegende technische Lösung erfordert die Verfügbarkeit einer Reihe von Verschlüsselungsverfahren. Es ist jedoch möglich, die Komplexität gering und – besonders wichtig – vom Nutzer fern zu halten. Der Nutzer muss sich nur dafür interessieren, wenn seine Wissbegierde das erfordert, aber nicht, um die Techniken einzusetzen.

Technisch basieren Verschlüsselungsverfahren auf folgenden Methoden:

a) Asymmetrische Verfahren zur öffentlichen Vereinbarung geheimer Schlüssel. Asymmetrische Verfahren verwenden für Ver- und Entschlüsselung verschiedene Schlüssel, so dass ein Schlüssel veröffentlicht werden kann und nur der zweite geheim gehalten werden muss.

b) Symmetrische Verfahren zur Verschlüsselung der Daten. Symmetrische Verfahren verwenden für beide Richtungen den gleichen Schlüssel, der folglich geheim bleiben muss.

c) Hashverfahren zur Sicherung der Integrität der Daten. Hashverfahren verwenden keine Schlüssel. Für einen Datensatz kann ein eindeutiger Hashwert von jedem berechnet werden, aus einem Hashwert lässt sich der Datensatz aber nicht rekonstruieren.

d) Signaturverfahren – eine Kombination aus a) und c) – zum Echtheitsnachweis der Nachricht. Ein Hashwert wird mit dem privaten Schlüssel verschlüsselt und kann mit dem öffentlichen Schlüssel entschlüsselt werden. Eine Signatur kann daher nur vom Inhaber des Geheimschlüssels erstellt werden.

e) Zertifikate als signierte Ausweise für eine Person oder eine Maschine. Die Signatur erfolgt in der Regel durch weitere Teilnehmer, denen implizit zu vertrauen ist.

Die aktuellen Verfahren besitzen über die mangelnde Teilnahme privater Nutzer hinaus ein Reihe weiterer Mängel, die zu Unsicherheiten führen.

1. Es wird das Falsche verschlüsselt. Beispielsweise sind Strecken zwischen Mailagent und Mailserver verschlüsselt, die Mail selbst jedoch nicht. Auf dem Server kann nach wie vor die Nachricht mitgelesen werden. Eine Sicherheit besteht trotz Verschlüsselung und Sicherheitsversprechen der Provider de fakto nicht.

2. Es sind mehrere Verfahrensmodelle in Betrieb, die auf der Nutzung von Zertifikaten beruhen. Dies führt zu Inkompatibilitäten verschiedener Anwendungen und zu einem hohen Aufwand, der vom Nutzer für die Einrichtung und für den Betrieb aufzuwenden ist. Nutzer sind dazu – verständlicher Weise – nicht bereit.

3. Die am häufigsten eingesetzten Modelle sehen vor, dass von bestimmten Organisationen ausgestellten Zertifikaten zu trauen ist. Das Vertrauen bezieht sich hierbei nicht nur auf die korrekt eingerichtete Verschlüsselung, sondern auch auf die Identität des Zertifikatinhabers. Es sind allerdings eine Viel-

zahl von Agenturen auf dem Markt, die jeweils aufgrund verschiedene Sicherheitsrichtlinien Zertifikate erstellen. Ein grünes Symbol im Browser sagt deshalb erst dann etwas aus, wenn der Nutzer den Aussteller und dessen Richtlinien überprüft hat. Da Zertifikate nur online geprüft, aber nicht beim Nutzer hinterlegt werden, spiegelt das Verfahren Sicherheit vor, ohne wirklich sicher zu sein.

4. Zertifikate sind mit wiederkehrenden Kosten verbunden, ohne dass für Kommunikationspartner in jedem Fall echte Sicherheit entsteht. Nutzer lehnen daher den Erwerb von Zertifikaten – verständlicher Weise – in der Regel ab.

Für einen breiten Einsatz der Verschlüsselung ist notwendig, dass

- sie transparent erfolgt, d.h. der Nutzer muss sich im Betrieb nicht mit ihr auseinander setzen,
- sie automatisch erfolgt, d.h. der Nutzer kann sicher sein, dass verschlüsselt wird,
- keine zusätzlichen Kosten entstehen,
- dass sie legal ist oder durch gesellschaftliches Verhalten legalisiert wird,
- der Nutzer, wie bisher auch, selbst seinen Partnern vertraut und sich nicht auf anonyme Zertifikatausteller verlassen soll,
- das System nur bei einem möglichen Fehlerfall dem Nutzer den Vorfall meldet und dieser nur in diesem Fall prüfen muss, ob alles korrekt ist (darüber hinaus gehende Prüfungen bleiben davon unberührt).

Für die Konstruktion eines sicheren Verfahrensmodells stehen die notwendigen Verschlüsselungsalgorithmen a) – c) zur Verfügung. Signaturverfahren als permanente Kennung eines Datensatzes stehen nicht für alle Verfahren zur Verfügung: ein kürzlich entwickeltes Verfahren, dass den Trommlern der Quantencomputergefahr die Stöcke aus der Hand schlägt, leistet das beispielsweise nicht. Es ist jedoch immer möglich, sich durch eine Kommunikation abzusichern, d.h. für die Kommunikationssicherung stellt das nur eine unwesentliche Einschränkung dar, während der Nutzer die Möglichkeit erhält, die ihm wichtigen Gesichtspunkte berücksichtigt zu wissen.

## Das allgemeine Modell

Der Inhalt dieses Abschnitts und auch der folgenden ist nur eine recht grobe Skizzierung und auch den Nichttechnikern eine Orientierung erlauben sowie eine allgemeine Diskussion anheizen. Unsere Konzepte gehen natürlich deutlich mehr ins Detail als wir hier andeuten können. Wer das hier verdaut und als Diskussionsgrundlage akzeptiert hat, kann in den Folgeartikeln tiefer in das Konzept einsteigen.

Das Verschlüsselungsmodell beruht auf dem Zero-Trust Konzept und besitzt zwei Grundprinzipien:

1. Es werden grundsätzlich alle Verbindungen verschlüsselt. Unverschlüsselte Kommunikation ist nicht mehr präsent (ausgenommen Router, die Daten auf einem ohnehin aus den Internetprotokollen hervorgehenden Quelle-Ziel-Weg rangieren und i.d.R. aus Effizienzgründen nicht verschlüsselt werden).
2. Die Information wird darüber hinaus grundsätzlich end-2-end verschlüsselt. Wenn eine Information über mehrere Verbindungen zugestellt wird, wie beispielsweise E-Mails, bedeutet dies in Verbindung mit 1. automatisch eine Mehrfachverschlüsselung.

Die Verschlüsselung erfolgt mittels sicherer Verschlüsselungsalgorithmen der Typen a) – c). „Sicher“ bedeutet, dass Angriffe auch mit hohem Aufwand in akzeptabler Zeit nicht einen Einbruch führen. Signaturverfahren werden für die Kommunikationssicherung nicht zwingend vorausgesetzt.–Verfahrenstechnisch können aber durchaus Vorteile entstehen, wenn sie existieren. Dokumentsignaturen außerhalb der online-Kommunikation sind nicht Gegenstand dieses Modells.

Wesentliches Kriterium ist eine grundsätzliche Verschlüsselung, die von den Systemen ohne Beteiligung der Nutzer durchgeführt wird. Diese Verschlüsselung kann aufgrund der angesprochenen gesetzlichen Beschränkungen durchaus eine beschränkte Qualität aufweisen. Bei einer generellen Verschlüsselung wird auch bei geringer Verschlüsselungsqualität ein Massenausspähen wirkungsvoll unterbunden. Nutzer mit höherem Sicherheitsbewusstsein können darüber hinaus kommerzielle sichere Lösungen einsetzen.

Teilnehmer am Verfahren sind netzwerkfähige Geräte und Nutzer. Nutzer führen die Kommunikation über eine nicht festgelegte Anzahl netzwerkfähiger Geräte. Für die Teilnehmer gilt:

a) Die Teilnehmer verfügen über ein langzeitgültige elektronische Identität (EI). Die EI eines Gerätes wird bei Inbetriebnahme zwangserstellt. Die EI eines Nutzers wird auf mindestens einem Gerät zwangserstellt, kann bei weiteren vom Nutzer genutzten Geräte aber auch importiert werden.

   Die elektronische Identität besteht aus einer menschenlesbaren Kennung sowie den öffentlichen Schlüsseln eines asymmetrischen Verfahrens. Die geheimen Schlüssel werden abgesichert verwaltet. Die EI entspricht damit im Aufbau dem heutigen Zertifikat, wobei eine Signatur nicht zwingend notwendig ist und ein Wechsel in der Regel im allgemeinen Modell nicht erfolgt.

b) Die Geräte verfügen über eine Datenbank zur Speicherung von elektronische Identitäten von Kommunikationspartnern und Kontrollinformationen zu den Kommunikationsvorgängen. Damit wird das heutige Zertifikatsystem abgelöst. Ziel ist eine erhöhte Sicherheit bei gleichzeitig einfacherer Handhabung.

**Nutzer**. Die Interessen des Nutzers, sich nicht mit komplizierten Vorgängen beschäftigen zu müssen, im laufenden Betrieb keinen zusätzlichen Aufwand zu haben und bei möglichen Angriffen rechtzeitig informiert zu werden, werden in folgender Weise erfüllt:

- Die Inbetriebnahme eines Gerätes nebst der Eingaben bestimmter Daten für die EI erfolgt durch den Nutzer. Dies ist ein einmaliger Vorgang, der durch eine ausführliche Benutzerführung unterstützt werden kann.

  Das Vorgehen entspricht der üblichen Inbetriebnahmepraxis; mit einer ablehnenden Haltung der Nutzer ist nicht zu rechnen.

- Im normalen Betrieb ist die Verschlüsselung für den Nutzer vollständig transparent. Er muss keine zusätzlichen Handgriffe gegenüber einem unverschlüsselten Verkehr ausführen, er muss nichts kontrollieren.

  Die primären Sicherungsmechanismen, mit dem gewünschten Kommunikationspartner verbunden zu sein, entsprechen den heutigen: der normale Nutzer verlässt sich auf Bekanntes und vertraut diesem. Die elektronische Hilfe durch Zertifikate spielt nur eine unwesentliche Rolle und trägt somit nur bedingt zur Sicherheit bei.

- Während die Erstellung einer EI im Rahmen einer Inbetriebnahme eine unwesentliche Erweiterung der Inbetriebnahmeprozeduren ist, bedarf die Verwaltung jedoch wesentlich nutzerfreundlicherer Mechanismen als dies heute der Fall mit Zertifikaten ist.

Die Sicherheit für den Nutzer wird durch zwei Mechanismen hergestellt:

- Bei jeder Verbindung wird zunächst die eigene EI gesendet und die EI des Ziels angefordert. Mit diesen wird eine verschlüsselte Verbindung hergestellt. Verbindungen sind somit immer verschlüsselt (Mechanismus 1)
- Eine neue EI des Partners wird in der Datenbank gespeichert, aber nicht überprüft. Die Sicherheit, mit dem korrekten Partner zu kommunizieren, liegt im Vertrauen des Nutzers (primäre Sicherheitsstufe).
- Bei einer erneuten Kommunikation wird die Anzahl der Verbindungen mit diesem Partner erhöht. Jede Kommunikation mit der gleichen EI erhöht die Sicherheit, tatsächlich mit dem gewünschten Partner zu kommunizieren. Dies ist die sekundäre Sicherungsmaßnahme.

  Die Sicherheit besteht in der Speicherung der individuellen Daten auf Geräten des Nutzers und nicht durch wiederkehrende Prüfung einer Signatur durch einen Dritten, ohne selbst eine Buchführung zu besitzen.

**Störungsfall**. Wird für die Kommunikation mit einem bekannten Partner eine andere EI präsentiert, liegt ein Störfall vor. Mögliche Ursachen für einen Störfall sind

a) Der Partner hat die elektronische Identität aus irgendwelchen Gründen ausgewechselt. Diese Störung ist unkritisch, muss aber behoben werden.

b) Ein Angreifer versucht, die Identität des Partners vorzutäuschen, und wird erkannt. Die Störung ist kritisch, sofern der Nutzer falsch reagiert.

c) Ein Angreifer hat bislang die Identität vorgetäuscht, fehlt aber nun in der Kommunikationskette. Die bisherige Kommunikation wurde abgehört, die Störung ist sehr kritisch.

Eine Störung kann nur durch den Nutzer beurteilt und beseitigt werden. Hilfeführungen sind gleichwohl möglich und sinnvoll. Eine Akzeptanz durch den Nutzer ist gewährleistet, so lange der Anteil an „false positives“, also Störungsmeldungen, die keine sind, klein bleibt. „False positives“ entstehen insbesondere durch a); ihre Vermeidung wird unten diskutiert.

**Geräte**. Die Kommunikation zwischen Geräten erfolgt nach den beim Nutzermodell genannten Prinzipien. In geschlossenen Netzwerksegmenten werden die EI der möglichen Partner auf den Geräten im Rahmen der Inbetriebnahme vorgegeben. Eine Kommunikation erfolgt nur mit diesen Geräten; Verbindungen mit Geräten unbekannte EI werden abgelehnt (das entspricht dem heutigen IPsec bzw. VPN-Prinzip). Bei offenen Netzwerken können die EI in der Datenbank zu Sicherheitsüberprüfungen abgelegt werden.

## Sicherheit des allgemeinen Modells

Im allgemeinen Modell erfolgen keine Kontrollen, ob die übertragene elektronische Identität echt oder gefälscht ist. Wir gehen dennoch von einer sehr hohen Sicherheit bereits im allgemeinen Modell aus.

**Knacken des privaten Schlüssels.** Die Fähigkeiten der Angreifer zum Einbruch in die Verschlüsselung werden in der Regel überschätzt. Bei fast allen Verfahren liegen die notwendigen Zeiten selbst bei hohem gerätetechnischen Aufwand bei tausenden von Jahren. Einbrüche werden durch Manipulation der Hardware, der Betriebssysteme, der Anwendungen oder durch Ermittlung zu einfach gewählter Kennworte erzielt, nicht aber durch Brechen der Algorithmen.

Gehen wir dennoch davon aus, dass ein Angreifer in der Lage ist, den geheimen Schlüssel eines Verfahren in 5 h zu ermitteln, gleich auf welche Weise dies nur erfolgt. Wenn das Modell einer allgemeinen Zwangsverschlüsselung umgesetzt wird, führt das auf eine Gesamtanzahl von $10^{10}$ oder mehr existierende elektronischer Identitäten. Für die Ermittlung der Geheimschlüssel sind somit ca. 5,6 Mio Jahre notwendig. Aus Sicht der Nutzer wäre pro Jahr weniger als jeder Millionste Nutzer von einem Bruch betroffen. Aus rein praktischen Gründen wird daher kein Angriff stattfinden, der wie heute in die Breite geht und alle Nutzer betrifft, da sich im Verhältnis zum Aufwand kein nennenswerter Gewinn erzielen lässt.

**Man-in-the-Middle.** Aufgrund der fehlenden Verifizierung der elektronischen Identität besteht die Möglichkeit, dass ein Angreifer sich zwischen Initiator und Ziel schaltet, ohne dass dies bemerkt wird. Der beide Seiten den Angreifer für den jeweils anderen Partner halten würden, kann dieser die Information jeweils entschlüsseln und damit mitlesen und mit dem Schlüssel des anderen Teilnehmers wieder verschlüsselt weiter senden.

Erfolg hat der Angreifer aber nur, wenn er bei der ersten und bei jeder folgenden Kommunikation in der MITM-Position ist. Fehlt er, würden die Partner andere elektronische Identitäten erhalten und den Nutzer über einen möglichen Einbruch informieren. Da der Einbruch in Echtzeit erfolgen muss, wären aufgrund der Menge der Kommunikationsvorgänge damit selbst Angreifer überfordert, die heute die Kommunikation weitgehend abgreifen und auswerten. Da ein Angreifer in den meisten Fällen ohnehin keine brauchbaren Informationen erhält und bei Bekanntwerden des Einbruchs mit größerer Vorsicht der Nutzer und schlechter Presse rechnen muss, ein Bekanntwerden aber ungleich wahrscheinlicher ist als heute, ist auch MITM keine Angriffsoption.

Die Sicherheit der Nutzer steigt mit der Anzahl der Kommunikationsvorgänge. Bei häufigeren Kommunikationsvorgängen kann ein Nutzer sicher sein, mit dem korrekten Teilnehmer verbunden zu sein, ohne dass die Verschlüsselungsparameter jemals überprüft worden wären.

## Spezielle Modelle

Das allgemeine Modell liefert nur einen Rahmen. Für die verschiedenen Einsatzfälle sind weitere Spezifikationen notwendig.

**Einschränkungen des allgemeinen Modells**. Die Sicherheit des allgemeinen Modell kann für den Nutzer unzureichend sein, wenn

- sehr kritische Informationen übertragen werden, die eine echte Authentifizierung erfordern,
- der Nutzer den Verdacht hat, gezielt überwacht zu werden (bei gezielter Überwachung greifen die auf der Masse der EI und Verbindungen beruhenden Mechanismen des allgemeinen Modells nicht).

Die gewünschte Sicherheit kann durch beliebige existierende Standardmethoden oder spezielle Methoden hergestellt werden, beispielsweise durch Verifizierung der elektronischen Identität auf einem Weg, der eine

Manipulation durch den vermuteten Angreifer ausschließt. Derart geprüfte EI werden in der Datenbank speziell markiert. Dies entspricht der heutigen Vorgehensweise im Rahmen des PGP-Modells.

Spezielle Methoden erfordern eine Mitwirkung des Nutzers:

- ✔ Sind einmalige Maßnahmen für bestimmte Ziele (z.B. Bank) für einen größeren Nutzerkreis notwendig/sinnvoll, können sie in einem Setup-Verfahren (z.B. Kontoeröffnung) durchgeführt werden. Aufgrund der Einmaligkeit bestehen keine Akzeptanzprobleme beim Nutzer.
- ✔ Sind häufiger spezielle Maßnahmen notwendig, erfordert dies eine größere Mitarbeit des Nutzers. Wir gehen allerdings davon aus, dass Nutzer betroffen sind, die bereits heute speziellere Absicherungsmaßnahmen unternehmen und diese Mitarbeit akzeptieren. Akzeptanzprobleme entstehen auch hier nicht.

**Wechsel der EI**. Wechselt ein Nutzer die EI, kann dies zu Störungsmeldungen führen. Der Wechsel aufgrund des Verlusts der privaten Schlüssel, eines Einbruchs in das Schlüsselsystem oder aufgrund einer Sicherheitsüberlegung des Nutzers erfolgen. Eine automatische Behandlung ist ohne Ausschluss eines Angriffs nicht möglich, so dass resultierende Störungsmeldungen behandelt werden müssen.

Im Verkehr mit Servern kann die EI eines Nutzers im Rahmen des Name/Kennwort-Logins auf dem Server beglaubigt installiert werden. Bei zukünftigen Besuchen des Nutzers entfällt das Login, da es mit der EI automatisch erfolgt (Vereinfachung der Situation heute bei gleichzeitig höherer Sicherheit gegenüber dem Cookie-Verfahren). Ein Wechsel der EI ist mit dem Name/Kennwort-Login möglich.

**Geräte-Vermittlung**. Geschlossene Netzsegmente können zu viele Nutzer enthalten, um in den Datenbanken der Geräte verwaltet zu werden. Ein Beispiel ist der vermutlich kaum noch aufzuhaltende autonome Automobilverkehr, der Kommunikation der Fahrzeuge untereinander und mit Leitsystemen erfordert. Aus Sicherheitsgründen muss dies ein streng abgeschottetes System sein, da ansonsten Terroristen oder Hacker Chaos auf den Straßen mit Verletzten und Toten erzeugen könnten. Die Problematik kann durch eine zentrale Datenbank beseitigt werden, in der alle EI in einem abgesicherten Verfahren registriert werden. Im Verkehrsbeispiel wären das die Server der zentralen Zulassungsstellen.

Alle Teilnehmer besitzen eine beglaubigte EI des Zentralservers. Bei Kommunikation mit einem der lokalen Datenbank unbekannten Teilnehmer wird die übertragene elektronische Identität durch gesicherte Kommunikation mit dem Zentralserver verifiziert. Dies entspricht dem heute möglichen Verfahren der Prüfung der Certificate Revocation List.

**Nutzer-Vermittlung**. Nutzer können unterschiedliche Geräte benutzen, die eigene Datenbanken haben. Dies würde zu unterschiedlichen Absicherungsgraden führen. Das Problem kann wiederum durch eine zentrale nutzerspezifische Datenbank, die jederzeit erreichbar ist beseitigt werden (Cloudlösung). Die EI der Datenbank ist verifiziert in den lokalen Datenbanken vorhanden. Die Mitwirkung des Nutzers wieder einmalig bei Inbetriebnahme erforderlich, so dass Akzeptanzprobleme nicht entstehen.

Die Verschlüsselung ist doppelt durchzuführen: die Kommunikation mit dem Server erfolgt verschlüsselt und authentifiziert. Abfragen und Updates erfolgen jeweils bei Kommunikation. Die Daten auf dem Server sind zusätzlich verschlüsselt, sofern es sich um einen Cloudserver handelt.

**Surfen im Internet.** Internetanwendungen können in zwei Kategorien unterteilt werden:

1. Gelegenheitsbesuche bei Webseiten, die sicherheitstechnisch unbedenklich sind,
2. sicherheitsrelevante Verbindungen wie Banking oder Shopping.

Die allgemeinen Prinzipien können bei beiden Kategorien angewandt werden, wobei eine strenge Kontrolle aber nur dann erfolgt, wenn der Nutzer dies dem System durch einen „Security"-Button angibt. EI dieser Server werden speziell geprüft, der Nutzer kann sie in seiner Datenbank als sicher markieren. Umgekehrt können auch Server einen Nutzer an seiner EI erkennen. Diese kann dem Server im Rahmen der Konteneinrichtung bekannt gemacht werden. Sichere Verbindungen sind dann sicher, weil **Nutzer** und **Server** die EI persönlich bestätigt haben und nicht aufgrund eines fragwürdigen Vertrauensmodells wie X.509-Zertifikate.

Da Geräte-EI und Nutzer-EI im Spiel sind, können während einer Kommunikation 2-4 EI zur Absicherung herangezogen werden. Aus Nutzersicht ist das kein Problem, da alles durch die Maschinen transparent abgewickelt werden kann.

**Telefonie**. Telefonate werden mit wechselnden Teilnehmern und wechselnden Geräten geführt, so dass mit hoher Wahrscheinlichkeit das elektronische Identitätmodell aus praktischen Gründen nicht durchgehalten werden kann. So kann die Anzahl der gespeicherten elektronische Identitäte begrenzt sein, außerdem sind Telefonate von anderen als zuvor verwendeten Geräten vom elektronische Identitätstandpunkt her neue Verbindungen.

Aus den genannten Gründen muss trotzdem in den meisten Fällen keine weitere Kontrolle erfolgen, sofern man wiederkehrende Verbindungen mit den gleichen Geräten führt. Neue Verbindungen können durch ein Ampelsystem angezeigt werden. In der Regel besteht keine Notwendigkeit für den Nutzer, sich darum zu kümmern. Bei kritischen Informationen

- hat sich der Nutzer i.d.R. durch nichtmaschinelle Mechanismen versichert, mit dem richtigen Gesprächspartner verbunden zu sein,
- können die Nutzer sich den Fingerprint des Sitzungsschlüssels (Short Authentication String) vorlesen, was durch Angreifer i.d.R. nicht gefälscht werden kann.

**Private Geräte.** Immer mehr Geräte im Haushalt kommunizieren untereinander und können aufgrund der Durchlässigkeit der Netzwerke auch von Außen angesprochen werden. Solche Geräte bilden im allgemeinen Modell eine geschlossenen Kommunikationsgruppe (was heute nur bedingt gilt). Bei Inbetriebnahme eines Gerätes ist dieses in die geschlossene Gruppe im Rahmen eines sicheren Inbetriebnahmeverfahrens aufzunehmen. Aufgrund der Einmaligkeit der Inbetriebnahmeprozedur für jedes Gerät bestehen keine Akzeptanzprobleme beim Nutzer.

Die Kommunikation geschlossener Netzwerke mit der übrigen Welt erfolgt ausschließlich über Komponenten mit Gateway-Funktionen.

**E-Mail.** Gegenüber dem heutigen Verfahren sind für den Austausch einer E-Mail mehrere Nachrichten auszutauschen:

1. Automatischer Abruf der elektronischen Identität des Ziels, wenn nicht bekannt (optional; die erste Kommunikation kann auch unverschlüsselt erfolgen).
2. Senden der verschlüsselten Nachricht unter Einschluss der eigenen EI.
3. Optional, sofern die EI nicht signaturfähig ist: Challenge-Response-Nachrichten zur Bestätigung der Urheberschaft.

Sofern die Optionen aktiviert sind, ändert sich für den Nutzer gegenüber dem heutigen Stand lediglich die Bearbeitungszeit: der Abruf der EI des Ziels erfordert, dass der Zielrechner in Betrieb ist; gleiches gilt für eine Challenge-Response-Signatur. Ggf. bleiben E-Mails in der Sendewarteschlange, bis die Zielseite geant-

wortet hat, oder ändern ihren Status nach Abschluss des Challenge-Resonse-Verfahrens. Akzeptanzprobleme dürften kaum entstehen, da die Verschlüsselung für den Nutzer keinen Zusatzaufwand bedeutet.

Im speziellen Fall können die EI auf Servern hinterlegt oder auf anderem Weg verifiziert werden.

## Verstärkungsprinzip

Das allgemeine Modell führt mit relativ hoher Wahrscheinlichkeit zum Auffallen von Angriffen. Es genügen dazu schon automatische, dann aber lautstarke Warnungen der Geräte. Publicity ist aber das, was Angreifer am Meisten fürchten: Nachrichtendienste gelangen in die öffentliche Diskussion, Unternehmen ebenfalls, wenn sie sich nicht gegen Angriffe von Kriminellen hinreichend absichern. Öffentliche Diskussion und Gerätewarnungen führen aber auch zu einer gesteigerten Bereitschaft der Nutzer, sich mit dem Thema auseinander zu setzen und beispielsweise durch zusätzliche Mausclicks weitere Absicherungsmaßnahmen vorzunehmen. Das Modell sorgt somit eine sehr hohe Absicherung gegen einen Überwachungsstaat oder Kriminelle, ohne dass die Nutzer wirklich viel tun müssen.

## Akzeptanz durch Firmen/Privatpersonen und Legalität

Privatpersonen und insbesondere Firmen sind sehr darauf bedacht, keine illegalen Aktionen zu unternehmen. Die Verschlüsselung von Telefonaten und von Textnachrichten ist innerhalb der EU völlig legal. Voice-over-IP-Telefonate lässt sich durch die sogenannte Quellen-TKÜ auf richterliche Anordnung auf dem Endgerät des abzuhörenden Nutzers durchführen und Textnachrichten liegen bei den meisten Nutzern auf deren Endgeräten im Klartext vor. Diejenigen, die ihre E-Mails verschlüsselt speichern, können dies auch mit der derzeit verfügbaren Technik durchführen.

Die Legalität ist somit vollständig gewährleistet und vor allem erfüllen Firmen durch das in den Grundzügen vorgestellte Verfahren die gesetzlichen Anforderungen an den Datenschutz und die Firmengeheimnisse werden besser geschützt.

Die Ausfuhr kryptografischer Software (Nummer 5D002) EU-weit geregelt [2]. Software, die von jedermann überall auf der Welt von einem Server heruntergeladen werden kann, muss derart „schwach“ Daten verschlüsseln, dass sie nicht als „Dual-Use“ (zivil/militärisch nutzbares Gut) angesehen werden kann. Dazu ist neben der freien Verfügbarkeit entscheidend, dass:

- symmetrische Verschlüsselungsalgorithmen nicht mit Schlüssellängen größer 56 Bit arbeiten
- **oder** dass asymmetrische Algorithmen wie RSA und Diffie-Hellman nicht mit Schlüssellängen größer 512 Bit arbeiten (112 Bit bei elliptischen Kurven).

Es ist somit erlaubt, AES mit 128 Bit Schlüssellänge mit einem RSA 512 Bit oder einen AES mit auf 56 Bit verkürztem Schlüssel mit RSA 2048 Bit zu kombinieren.

Innerhalb der EU ist der Verkauf und die Nutzung von beliebig sicherer Verschlüsselung erlaubt. Es ist daher sinnvoll, starke Verschlüsselung grundsätzlich gegen eine Mindestgebühr zu verkaufen, um Nationalität und Identität des Anwenders zu ermitteln. Eine gut gesicherte Lizenzmaschine ist überdies eine Grundvoraussetzung, damit die frei herunterladbare Software nicht beliebig freigeschaltet werden kann.

Diese Gesetzgebung ist nur scheinbar sinnvoll. Man möchte angeblich keinesfalls Terroristen ein unknackbares Kommunikationsmittel in die Hand geben, jedoch die Kommunikation der eigenen Bürger mit Banken, Anwälten, Familienangehörigen und Kollegen in Firmen gegen Missbrauch schützen. Dazu bedient man sich der Definition einer Grenze, von der man unterstellt, dass sie für Hacker zu hoch und für Geheimdienste „gerade noch leistbar“ ist. Diese Grenze wurde mit der Zeit angehoben, um dem technischen Fortschritt auf Seite der Hacker zu folgen. Ende der 1990'er Jahre lag diese Grenze noch bei 40 Bit für symmetrische Verschlüsselungsverfahren.

Die Unsinnigkeit dieser Regelungen lässt sich an mehreren Fakten ablesen:

- Es ist weltweit kein Problem, durch kostenlosen Download an harte Verschlüsselungssoftware zu gelangen.
- Es ist auch kein Problem, harte Software in der EU legal zu erstehen und beispielsweise per Notebook weltweit zu verwenden. Die verschlüsselten Daten tragen keinerlei Kennung, mit welchem Produkt sie verschlüsselt sind, so dass ein Nachweis illegaler Verwendung nicht möglich ist.
- Terroristen und Kriminelle sind in Netzwerken organisiert, die medial bekannt über IT-Spezialisten verfügen, deren Kenntnisse sehr hoch angesetzt werden müssen. Es ist für diese Leute kein Problem, OpenSource-Code zu harter Verschlüsselungssoftware umzusetzen.
- Hacker oder IT-Kriminelle sind medial bekannt ebenfalls in der Regel in der Lage, die Minimalverschlüsselung zu knacken.
- „Gut gesicherte Lizenzmaschinen“ existieren nur in der Fantasie, wie die Erfahrungen der Medienbranchen zeigen. „Sichere Lizenzmaschinen“ beruhen auf einem Verschweigen aufgetretener Brüche oder eines mangelnden wirtschaftlichen Interesses, eine Maschine anzugreifen.

Eine solche Gesetzgebung richtet sich daher de fakto ausschließlich gegen die Kommunikationssicherheit des normalen Bürgers und schädigt die Innovativkraft der Wirtschaft. Da der vorgegeben Zweck keinesfalls erreicht werden kann, stellt sich die rechtliche Frage, ob solche Regelungen nicht gegen das Freiheitsprinzip und die Menschenrechte generell verstoßen.

## Kritische Masse

Anfänglich werden nur wenige Anwender das in den Grundzügen vorgestellte Verfahren nutzen. Aufgrund der Tatsache dass jeder Nutzer von VoIP-, Instant Messenger- oder e-Maildiensten derzeit ein Ziel darstellt, wird für Geheimdienste lediglich der Inhalt der Nachrichten und Gespräche zur Unbekannten. Verbindungsdaten und andere Metadaten (z.B. Standortinformationen) stehen jedoch in der gleichen Qualität wie zuvor zur Verfügung. Da Verschlüsselung auch heute bereits legal von einzelnen Nutzern ohne Konflikte mit den Behörden eingesetzt wird, wird die Teilnehmerzahl problemlos anwachsen können, insbesondere wenn die Verfahren in Betriebssysteme und Standardanwendungen übernommen werden. Da Massenphänomene schließlich schlecht per Gesetz verboten werden können, lassen sich auch unsinnige Regelungen wie die beschränkte Sicherheit beseitigen, wenn die breite Masse hochwertige Verschlüsselung einfach einsetzt.

## Einführungsphase

Ein sicheres System kann nur mit einer längeren Anlaufphase umgesetzt werden. In dieser Phase muss es mit bestehenden Systemen kooperieren können. Der Wirtschaft kommt bei Umsetzung des Konzepts eine Schlüsselrolle zu, da vom Nutzer kaum Bereitschaft zur Mitarbeit zu erwarten ist.

**Telefonie**. (Neue) Endgeräte werden grundsätzlich mit Verschlüsselungssoftware für die Sprachverschlüsselung sowie die notwendigen Anwendungen für EI-Generierung ausgestattet. Eine (schwache) Verschlüsselung wird durchgeführt, wann immer dies durch die beteiligten Geräte möglich ist. Ältere Geräte können auf Nutzerwunsch aufgerüstet werden. Eine Nutzermitwirkung ist nur notwendig, wenn besondere Anforderungen an die Verschlüsselungsqualität gestellt werden oder eine Aufrüstung älterer Geräte erfolgt.

**Webseiten**. Bei Neuinstallationen von Nutzerrechnern wird betriebssystemseitig grundsätzlich EI-Generierung vorgesehen. Dies können beispielsweise auch die bereits heute für SSH meist standardmäßig generierten klassischen Zertifikate sein. Die Verwaltungssoftware muss nutzerfreundlicher gestaltet werden, um Export auf anderen Geräte usw. zu erlauben.

Browser sind mit EI-Verwaltungsanwendungen auszustatten. Als EI können auch die derzeit verwendeten Serverzertifikate verwendet werden, die nach der Erstprüfung auf dem Nutzerrechner verwaltet werden. Eine nutzerfreundliche Verwaltungsschnittstelle ist notwendig.

Bei Zertifikatwechsel der Server sind die Protokolle dahin gehend zu erweitern, abgelaufene Zertifikate mit den neuen im Verbund zu prüfen, um der Nutzer-EI-Verwaltung eine Übernahme zu ermöglichen. Eine Verbundprüfung besteht beispielsweise aus einem Challenge-Response-Verfahren, die den Server im Besitz beider privater Schlüssel ausweisen.

Im Kundenkontenbereich der Serverbetreiber können Installationsmöglichkeiten für die Nutzer-EI-vorgesehen werden, die eine automatische Anmeldung auf dem Server (ohne Name/Kennwort) oder verschlüsselte E-Mails erlaubt.

**E-Mails**. Es genügt eine Zwangs-EI-Erzeugung und deren Mitsenden in jeder E-Mail sowie eine automatische Übernahme eingehender EI in die Datenbank. Eine Verschlüsselung wird immer durchgeführt, wenn dies möglich ist. Die Einführung erfolgt ohne aktive Mitwirkung der Nutzer.

**Die Rolle der Wirtschaft**. Insbesondere bei der Anmeldung auf Servern bietet das System den Kunden Vorteile, mit denen Unternehmen werben können (einfachere Bedienung). Außerdem wäre das System sicherer als das Cookie-System, was auch im Interesse der Unternehmen selbst wäre. Verschlüsselte E-Mails würden den Unternehmen erlauben, kritische Informationen per E-Mail zu versenden. Die erhöhte Sicherheit ist ebenfalls ein deutliches Werbeargument. Unterstützen können Unternehmen den Systemaufbau ferner, indem sie ihre Werbung mit Sicherheit und Komfort durch ein Angebot kostenloser oder preisgünstiger Apps unterstützen.

**Sicherheit beim Nutzer.** Kritisch ist die Sicherheit der privaten Schlüssel beim Nutzer. Sie sind durch Name/Kennwort-Systeme zu sichern, die beim Hochfahren des Systems einzugeben sind. Kritisch ist der längere Betrieb eines Rechners, bei dem zu verhindern ist, dass in Abwesenheit des Nutzers mit Hilfe der EI Geschäfte getätigt werden. Störend ist die Eingabe des Kennwortes nach jeder längeren Pause. Eine Absicherung, die vermutlich nicht auf große Akzeptanzprobleme stößt, ist die Eingabe einer PIN (z.B. 4-stellig, alpha-

numerisch), die fest oder variabel vergeben werden kann und nur max. 3 Versuche erlaubt, bis doch auf das Hauptkennwort zurückgegriffen werden muss.

## Ausblick

Es liegen heute in ausreichendem Maße Erfahrungen mit Verschlüsselungssystemen zum Absichern von Kommunikationsverbindungen vor, so dass es möglich ist, präzise Vorhersagen zu machen, wie massentaugliche Lösungen aussehen werden.

Es kann als sicher angesehen werden, dass unabhängige Arbeiten zum gleichen Thema sehr ähnliche oder gar identische Lösungen postulieren.

Aufgrund der Erkenntnis, dass die graduelle Einführung einer derartigen Lösung frei von Nachteilen ist, regen die Autoren die Gründung einer gemeinnützigen Organisation an, deren Ziel die Bereitstellung einer einheitlichen, quelloffenen Bibliothek oder API ist, welche in kommerzielle, als auch nichtkommerzielle Software integriert werden kann und mit der Zeit einen einheitlichen Standard bildet. Die Lösung wird für Erweiterungen offen gehalten sein und das Höchstmaß an Einfachheit und Verständlichkeit bieten.

## Literatur

[1] Namenskürzel des Autors: jjc, Spiegel online, 2012, „Schlagwort-Fahndung: Geheimdienste überwachten mehr als 37 Millionen E-Mails“, http://www.spiegel.de/politik/deutschland/schlagwort-fahndung-geheimdienste-ueberwachten-mehr-als-37-millionen-E-Mails-a-817499.html

[2] Amtsblatt der Europäischen Union,

Kategorie 5, Teil 2, “INFORMATIONSSICHERHEIT“, 2015, http://www.ausfuhrkontrolle.info/ausfuhrkontrolle/de/gueterlisten/anhaenge_egdualusevo/anhang_1_kat_5_2.pdf

[3] Jürgen Schmidt, heise.de, „Lasst PGP sterben!“, 2015, http://www.heise.de/ct/ausgabe/2015-6-Editorial-Lasst-PGP-sterben-2551008.html

[4] Jürgen Schmidt, heise.de, „Kommentar: WhatsApp hat geliefert - jetzt sind wir dran“, 2016, http://www.heise.de/newsticker/meldung/Kommentar-WhatsApp-hat-geliefert-jetzt-sind-wir-dran-3163779.html

[5] Thomas Moßburger, focus.de, „Warum WhatsApps neueste Funktion Terroristen gelegen kommen dürfte“, 2016, http://www.focus.de/digital/handy/whatsapp-hilft-die-verschluesselung-terroristen-und-kriminellen_id_5418000.html