Ende-zu-Ende-Krypto unter Beschuss - Verbot ist technisch aber Un...

Die Verfügbarkeit von Ende-zu-Ende-Verschlüsselungen steht immer wieder unter Beschuss. Erst kürzlich wurde ein neuer Vorstoß gestartet, die sichere Kommunikation insbesondere auf Messenger-Plattformen zu untergraben.

Zu diesem Thema gab es kürzlich einen Austausch zwischen Nutzern und den Anbietern des GoldBug Messenger Projektes. Dabei handelt es sich um einen Instant Messenger, der Ende-zu-Ende-Krypto nativ integriert und somit einfach nutzbar macht. Die Ausführungen dazu wollen wir an dieser Stelle dokumentieren:

Frage: Wie wären Verantwortlichkeiten geregelt, wenn es bei einem Ende-zu-Ende-Verschlüsselungsverbot sodann Zweitschlüssel gäbe?

GoldBug Messenger Projekt: Die Verantwortlichkeit für Klartexte sind an jede Kopie eines Schlüssels geknüpft. Auch wenn niemand die Absicht hat, Ciphertext in Klartext zu wandeln - außer ein oder die Schlüsselbesitzer - sind die Inhaber eines Schlüssels auch verantwortlich für den Inhalt einer Verschlüsselung. Sie sind auch verantwortlich für den Schutz des Schlüssels und damit des Inhalts der Verschlüsselung. Daten verantwortet also jeder, der sie speichert und einen Schlüssel dazu hat. Ende-zu-Ende Verschlüsselung wird sich nicht verbieten lassen.

Eine Ende-zu-Ende-Verschlüsselung ist heutzutage nicht nur mit einem geheimen Passwort (symmetrische Verschlüsselung), sondern auch schon mit a-symmetrischen Schlüsseln (also den bekannten Schlüsselpaaren des privaten und öffentlichen Schlüssels der PKI, Publik Key Infrastructure) vorhanden. Daher ist die Ende-zu-Ende-Verschlüsselung vielfältiger zu betrachten als derzeit in der politischen Debatte gedacht.

Datum: *Samstag, 28.11.2020 07:30 Uhr*
Mehr: *Datenschutz*
Autor: *Christian Kahle*

Die Vorstellung eines Generalschlüssels ist zudem vereinfacht: Ein Zweitschlüssel ist immer eine Kopie und Weitergabe eines definierten Schlüssels. Sodann kann ein sogenanntes REPLEO (Verschlüsselung des eigenen öffentlichen Schlüssels) einem Schlüssel vor einer Schlüsselübertragung zusätzlichen Schutz geben. So müsste ein Ende-zu-Ende-Verschlüsselungsverbot auch für das Verschlüsseln (und senden) von Schlüssel gelten. Wie soll ein Schlüssel gesichert werden, der durch eine Ende-zu-Ende-Verschlüsselung gesandt wird, um eine normale Verschlüsselung aufzubauen? Politik wackelt hier an den Grundfesten.

Eine Schein-Diskussion

Frage: Wenn vielfältige Technik die Ende-zu-Ende-Verschlüsselung schützt, warum ist sie dann so oft in der politischen Diskussion, ohne technische Aspekte und Antworten zu berücksichtigen?

GoldBug Messenger Projekt: Richtig, es ist eine Schein-Diskussion, die technisch längst beendet ist: Ende-zu-Ende-Verschlüsselung durch Cryptographisches Calling - das ist das Erneuern der Ende-zu-Ende-Verschlüsselung während der laufenden Sitzung durch zahlreiche Methoden - oder das Fiasco Forwarding mit Fiasco Keys (dabei werden für eine Nachricht gleich ein Dutzend an Ende-zu-Ende verschlüsselnden Schlüsseln gesandt) oder die Anwendung von Schlüsseln des McEliece Algorithmus (wie er schon in drei Chat-Applikationen eingebaut ist) ist sicher, wenn Ciphertext erst mal versandt ist oder mit Copy/Paste in einen Kommunikationskanal eingefügt wurde (vgl. ausführlich Nomenclatura 2019). Es müssen somit auch Softwareanbieter, Verschlüsselungsmethoden sowie Transport-Anbieter von Ciphertext bei der Ende-zu-Ende Verschlüsselung differenziert betrachtet werden.

Frage: Es geht um den staatlichen Eingriff in die Infrastruktur der Anbieter. Wenn im Gesetz steht, der Anbieter von Verschlüsselung hat diese aufzumachen, dann hat er Verschlüsselung aufzumachen.

GoldBug Messenger Projekt: Wie genannt: Anbieter sind oft nur ein Kanal für Ciphertext. Ein E-Mail-Provider kann eingehenden Ciphertext nicht konvertieren. Somit muss man Anbieter für die Erstellung von Ciphertext von den Transporteuren und den (Zwischen-)Speichernden (Hostern) von Ciphertext trennen. Und dabei gilt: Ciphertext bei diesen Akteuren kann heute voraussichtlich nicht gebrochen werden, wenn der Verschlüsselungsalgorithmus jenseits von RSA und ECDSA ist - d.h. der Klartext besser mit den Algorithmen NTRU oder McEliece verschlüsselt wurde (vgl. a. Lexikon Nomenclatura 2019). Es ist also entscheidend, ob der Anwender verschlüsselt oder ein App-Anbieter oder ein Kanal- bzw. Cache-Anbieter davon betroffen ist. Ein Gesetz, dass Kanal-Anbieter Ciphertext nicht weiterleiten dürfen, wird es nie geben, wenn es Banking, Shopping und E-Mail weiterhin geben soll.

Frage: Es geht um die Problematik der politischen Diskussion, eine Ende-zu-Ende-Verschlüsselung einzuschränken. Im Falle, dass man auf die Hersteller von Verschlüsselungssoftware abstellt, könnten sie einer Export- bzw. Distributionskontrolle unterliegen, die für jeden Hersteller im Inland bzw. in Europa dann gelte?

GoldBug Messenger Projekt: Mathematik unterliegt weder der Exportkontrolle noch einer Distributionskontrolle. Software kann quelloffen sein oder im Internet jenseits lokaler und regionaler Rechtsprechung bezogen werden. Ciphertext zu erstellen erfolgt täglich wie Brot backen - und ist dabei kein Geld-Drucken. Wenn jeder Kommunikations-Laut eines Menschen wie jedes Datenpacket inspiziert werden soll, in welcher Gesellschaft leben wir dann? Das, was vertraulich - also nicht für Dritte bestimmt - unseren Mund verlässt, kann in einer freien Gesellschaft keiner Exportkontrolle unterliegen. Denn: wer illegal handeln will, wird auch illegale Werkzeuge nutzen, aber die Sicherheit allen zu nehmen, bedeutet größeres Unheil, als Verschlüsselung in der Hand aller zu belassen.

Wie die Probleme in der Praxis aussehen, erfahren Sie auf der kommenden Seite.

1 2 ***nächste Seite ›***

Frage: Nähmen wir an, die politische Phantasie des Verbotes von Ende-zu-Ende-Verschlüsselung würde doch real: Wie käme sichere Ende-zu-Ende Verschlüsselung dann doch auf ein mobiles Endgerät des normalen Nutzers, der nur Apps aus dem Appstore installieren kann, wenn kein Hersteller mehr Verschlüsselungssoftware vertreiben darf?

GoldBug Messenger Projekt: Mit Copy/Paste des Ciphertexts! Dieser ist immer und überall für jeden Verfügbar und auf zahlreichen Maschinen mit zahlreichen Programmen erzeugbar. Eine App im Appstore ließe sich sicherlich verhindern, aber das Copy und Paste von Ciphertext niemals. Daher ist dieses politische Unterfangen des Verbotes von Ciphertext-Verschlüsselung und deren Applikationen sinnlos und wäre auch nicht zielgerichtet.

Frage: Copy/Paste ist ein zusätzlicher Schritt, den man bewusst gehen muss. Wie kann diese komplexe Verschlüsselung für alle gefördert werden und nicht nur für die Wissenden und Eingeweihten bestehen?

GoldBug Messenger Projekt: Es wird immer eine öffentliche und zugänglich Lehre über Verschlüsselung geben und Open Source Programme wie auch Linux Maschinen werden auch immer zur Verfügung stehen. So schwierig ist es nicht, einen Chipertext irgendwo zu generieren und auszukopieren, und im gewünschten Kanal einzufügen.

Es geht dezentral

Frage: Die fehlende Bequemlichkeit wird manuelle Prozesse killen. Muss passende Software nicht zentral angeboten werden, damit Nutzer diese beziehen, denn auch die Funktionalität benötigt zentrale Prozesse?

GoldBug Messenger Projekt: Weder symmetrische noch asymmetrische Verschlüsselung benötigt Zentralität. Copy/Paste von Ciphertext ist ein einfacher Vorgang, den jeder bequem in der Praxis durchführen kann. Zudem wird quelloffene Software jederzeit installierbar sein - wie genannt auch auf jederzeit quelloffenen Linux-Systemen.

Frage: Ist PGP/GPG nicht das beste Beispiel, dass fehlende Zentralität und Usability den Einsatz zum großflächigen Scheitern brachte?

GoldBug Messenger Projekt: Das POPTASTIC-Protokoll - das verschlüsselten Chat über E-Mail-Server abbildet - wächst beispielsweise durch die Applikation Delta-Chat grossflächig. Auch zuvor haben diese Chatform schon andere Applikationen entwickelt (vgl. Adams 2016). GPG ist also nicht tot, sondern ein Standard.

Frage: Dennoch, wären Anbieter von Software und deren Webseiten nicht verschwunden, wenn sie den Ciphertext nicht öffnen könnten, wenn es ein Ende-zu-Ende Verschlüsselungsverbot gäbe?

GoldBug Messenger Projekt: Wir leben nicht mehr im Mittelalter: D.h. jeder hat einen Taschencomputer in der Jeans. Rechenoperationen oder Programme zur Erzeugung von Ciphertext sind säkularisiert für alle.

Auch für unerfahrene User

Frage: Nochmal zur Ausgangsfrage: Wie bekommt ein nicht technisch affiner Nutzer Ende-zu-Ende verschlüsselten Ciphertext ohne Software im Appstore auf sein mobiles Gerät?

GoldBug Messenger Projekt: Wie genannt: Mittels eines einfachen Sideloads des Ciphertextes: Copy/Paste.. Ciphertext wird immer auf einer Maschine erzeugbar sein und kann in jeden Kanal und jede Applikation einkopiert bzw. eingefügt werden. Weder Linux-Maschinen noch Chat-Server wie z.B. Echo-Chat-Server (Edwards 2019) kennen fehlende "Sideloads".

Frage: Ist das nicht ein Umweg? Dann sind die Ottonormalverbraucher bei mobilen Geräten schonmal außenvor. Wäre sodann sichere Verschlüsselung auf eine Elite beschränkt?

GoldBug Messenger Projekt: Umwege erhöhen die Ortskenntnis: Fdroid ist z.B. ein Appstore, aus dem quell-offene Applikationen jederzeit geladen werden können, wenn das Betriebssystem es erlaubt. Und Linux wird immer der Hoheit des Nutzers gehören. Ein Verbot von Ende-zu-Ende verschlüsselnder Software würde niemals zu einem Verschwinden von Ende-zu-Ende-Verschlüsselung führen und diese kann auch im Transport-Stream nicht erkannt werden. Der Einsatz von sicherem Ciphertext wird also niemals verdächtig, sondern ist ein Gehen der Extra-Meile, das zusätzliche Sicherheit verschafft. Wenn konsequent der Hauptteil der Kommunikation per default verschlüsselt wird, ist es zudem allein aufgrund von vorhandener Verschlüsselung unmöglich, auf potenziell schützenswerte Inhalte zu schließen. Treiben wir es auf die Spitze: Sollte Politik nicht folgerichtig auch Linux verbieten?

Frage: Banken und Shopping benötigen nicht zwingend uneinsehbare Ende-zu-Ende Verschlüsselung (sondern reguläre Ende-zu-Ende Verschlüsselung) und sind bereits jederzeit durch Aufsichten zugänglich. Hat dieses Auswirkungen auf die geschlossen-sichere Ende-zu-Ende-Verschlüsselung von zwei Nutzern beim Messenger?

GoldBug Messenger Projekt: Man kann Ciphertext aus dem Banking vom Ciphertext mit Ende-zu-Ende-Verschlüsselung aus einem Messenger nicht sofort unterscheiden. Ciphertext ist Ciphertext. Brechbarer (erlaubter) Ciphertext (z.B. mit Zweitschlüssel) kann nicht von unbrechbaren (dann ggf. unerlaubtem, Ende-zu-Ende-verschlüsseltem) Ciphertext in der Transportation identifiziert und getrennt werden. Ciphertext wird daher nicht elitär werden, sondern jeder nutzt zunehmend mehr Verschlüsselung, da die Infrastruktur es aus Sicherheitsgründen bieten muss und Nutzer darin geschult werden.

Frage: Wenn Ciphertext gleich Ciphertext gleich Ciphertext ist, könnte oder sollte man dann statt Ende-zu-Ende-Verschlüsselung nicht generell jeglichen Ciphertext verbieten?

GoldBug Messenger Projekt: Ein Bann von Ciphertext ist illusorisch. Code-Brecher wissen zudem nicht, in welcher Verschlüsselungsschicht sie sich befinden: Das ist die sogenannte Multiverschlüsselung, die sowohl Klartexte wie auch Ciphertexte (nochmals) zu Ciphertext wandelt. Es wird immer Lehre und offenes Informationsmaterial zur Verschlüsselung geben, das ist notwendig, wenn eine Nation Verschlüsselungsweltmeister oder auch Entschlüsselungsweltmeister werden will. Eines ist jedenfalls sicher wie die Rente: Einen Weltmeistertitel wird es ohne sichere Ende-zu-Ende Verschlüsselung nicht geben - im Gegenteil: wir müssen "mehr Verschlüsselung wagen" (Saskia Esken 2015), wenn wir "Verschlüsselungs-Standort Nr. 1 auf der Welt werden wollen".

Siehe auch:

- Zoom bietet jetzt allen Nutzern Ende-zu-Ende-Verschlüsselung an
- Google Messages: Android-App bekommt Ende-zu-Ende-Verschlüsselung
- Apple baut Ende-zu-Ende-Verschlüsselung deutlich aus

zurück 1 2