Hacker-Lexikon:

Was ist die End-to-End Verschlüsselung?

Von Andy Greenberg

11.25.14 | 09:00 |

Getty Images

TL; DR:

End-to-End Verschlüsselung ist ein System der Kommunikation, wo sind die einzigen Menschen, die Nachrichten zu lesen, können, die Menschen kommunizieren. Kein Lauscher greifen die kryptografischen Schlüssel benötigt, um das Gespräch zu entschlüsseln – nicht einmal ein Unternehmen, das den messaging-Dienst ausgeführt wird.

Viele Unternehmen prahlen, dass ihre Kommunikation-app verschlüsselt werden. Aber das marketing Anspruch eine Followup-Frage verlangt: Wer hat den Schlüssel? In vielen Fällen hält das Unternehmen selbst die kryptografischen Schlüsseldaten, mit dem sie Ihre Nachrichten entschlüsseln können — und tut daher alle Hacker, das Firma oder Regierung offizielle ansehen über seine Schulter gefährdet.

Aber zunehmend sind Privatsphäre-bewusste Kommunikationstools Roll-out eines Features namens "End-to-End-Verschlüsselung". Dieses Versprechen "End-to-End" bedeutet, dass Nachrichten in einer Weise, die nur den einzigartigen Empfänger einer Nachricht verschlüsselt werden, es, und nicht jemand dazwischen zu entschlüsseln kann. Mit anderen Worten, nur die Endpunkt-Computer halten die kryptografischen Schlüssel, und dem Server der Firma fungiert als einen Analphabeten Messenger, vorbei an Nachrichten, die diese selbst entschlüsseln kann nicht.

Diese Vorstellung des Entschlüsselungsschlüssels nie verlassen das Gerät des Benutzers mag wie ein Paradox. Wenn dem Server der Firma nie den Schlüssel sehen kann, dann wie es auf das Gerät bekommt, wenn der Benutzer in erster Linie die app installiert?

Die Antwort wird durch eine andere Krypto-Trick bekannt als Public-Key-Verschlüsselung möglich. In öffentliche Schlüsselsysteme Krypto wird ein Programm auf Ihrem Computer mathematisch ein Schlüsselpaar generiert. Einerseits den privaten Schlüssel oder geheimer Schlüssel, genannt dient zum Entschlüsseln von Nachrichten, die an Sie gesendet und nie verlässt Ihr Gerät. Andererseits den öffentlichen Schlüssel dient zum Verschlüsseln von Nachrichten, die an Sie gesendet werden, und es ist so konzipiert, dass diese Nachrichten nur der entsprechende private Schlüssel entschlüsselt werden kann. Diesen Schlüssel kann an Dritte weitergegeben werden, möchte eine Nachricht an Sie verschlüsseln. Denken Sie an das System wie eine Lockbox vor der Haustür für den UPS-Lieferung-Mann: kann jeder mit Ihren öffentlichen Schlüssel setzen etwas in das Feld ein und aktivieren sie den Schreibschutz, aber Sie haben nur den privaten Schlüssel zu entsperren.

Die erste freie, weit verbreitete End-to-End verschlüsselte messaging Software war PGP Pretty Good Privacy, ein Programm von Phil Zimmermann codiert und veröffentlichte 1991. Es ist jedoch Jahrzehnte, dass vollständige Verschlüsselung-Tunnel, um die Massen zu erreichen. Programme wie das "Off The Record"-Plugin für Jabber Instant messaging-Anwendungen und TextSecure Textnachrichten machten End-to-End Verschlüsselung weit einfacher zu bedienen. Apple verwendet eine Form der End-to-End Verschlüsselung in seiner iMessage-ca. (obwohl einige Sicherheitsexperten auf Mängel bei der Umsetzung, die seine Nachrichten entschlüsselt werden können, könnte,darauf hingewiesen haben.) Google ist das Experimentieren mit einer End-to-End Verschlüsselung e-Mail Plugin für Chrome. Und gerade letzte Woche Smartphone messaging-app Whatsapp TextSecure integriert seine Android Software, End-to-End Verschlüsselung für Hunderte von Millionen von Nutzern einschalten.

Auch End-to-End-Verschlüsselung ist nicht unbedingt unempfindlich aus schnüffeln. Anstatt zu versuchen, tatsächlich die Verschlüsselung zu brechen, kann zum Beispiel ein Lauscher versuchen Empfänger einer Nachricht anzunehmen, so dass Nachrichten auf ihren öffentlichen Schlüssel statt diejenige der Absender bestimmt verschlüsselt werden. Nach dem Entschlüsseln der Nachricht, Snoop dann zum eigentlichen öffentlichen Schlüssel des Empfängers verschlüsselt und schicken Sie es auf einmal eine Erkennung zu vermeiden; Dies ist, was ist bekannt als ein Man-in-the-Middle-Angriff. Um diese Taktik zu bekämpfen, erzeugen einige Programme von End-to-End Verschlüsselung einzigartige einmalige Zeichenfolgen anhand der beiden Nutzer öffentlicher Schlüssel. Die beiden Menschen Kommunikation ausgelesen die Passphrase zueinander vor Beginn ihres Gespräches. Wenn die Zeichen übereinstimmen, können sie beruhigt sein es gibt keinen Mann in der Mitte.

Natürlich gibt es noch zwei Schwachpunkte verließ auch perfekte End-to-End Verschlüsselungssysteme: die enden. Jeder Benutzer Computer kann noch gehackt werden,

um seinen kryptografischen Schlüssel zu stehlen oder einfach die Empfänger entschlüsselt Nachrichten lesen. Sogar die meisten perfekt verschlüsselte Kommunikation-Leitung ist nur so sicher wie das Postfach am anderen Ende.

Hacker-Lexikon ist die WIRED-Erklärer-Serie, die Jargon der Informationssicherheit, Überwachung und Datenschutz de verwirren soll.

http://www.wired.com/2014/11/hacker-lexicon-end-to-end-encryption/