TRANSFORMATION

DER KRYPTOGRAPHIE

[Deutschsprachiges E-Buch]

Bertram & van Dooble

Transformation der Kryptographie

Transformation der Kryptographie

Grundlegende Konzepte zur Verschlüsselung, Meilensteine, Megatrends und nachhaltiger Wandel in Bezug auf verschlüsselte Kommunikation und ihre Nomenklatura

von Linda A. Bertram & Gunther van Dooble

Mathematiker und Informatiker
haben durch die Berechnung der Wahrheit
das Menschenrecht auf Privatsphäre in der Hand.

Bisher waren die Erstellung, Anwendung und Erforschung der Kryptographie und ihrer Algorithmen und Prozesse sowie die Programmierung entsprechender Software staatlichen Institutionen, Sachverständigen und dem Militär vorbehalten.

In der jüngeren Vergangenheit wurde neben der jahrhundertealten Verschlüsselung mit einem geheimen Schlüssel die Verschlüsselung mit einem Schlüsselpaar - bestehend aus einem öffentlichen und einem privaten Schlüssel - etabliert.

In diesem Fall kann mittels mathematischer Berechnung (Primfaktorzerlegung) mit dem öffentlichen Schlüssel des Kommunikationspartners und den eigenen Schlüsseln eine

Nachricht entsprechend ver- und wieder entschlüsselt werden.

Es ist eine Verschlüsselung nicht mit einem gemeinsamen Geheimnis, sondern mit einer sogenannten "Public Key Infrastructure (PKI)" (↗[02][16][25][44][39]): Nur das Schlüsselpaar, eines von denen kann öffentlich sein - und die andere, die privat ist.

Seitdem existieren diese beiden Verschlüsselungsmethoden: Die Methode zur Verwendung eines geheimen Schlüssels wird als symmetrische Verschlüsselung bezeichnet (↗[54][21][15][04][01]) (beide Kommunikationspartner müssen das Passwort kennen).

Die PKI-Verschlüsselung mit einem öffentlichen und einem privaten Schlüssel wird als asymmetrische Verschlüsselung bezeichnet.

Die Beschreibung der Übertragung eines symmetrischen Zugangsschlüssels bei der asymmetrischen Verschlüsselung - ohne größere Sicherheitsbedenken - war ein Meilenstein in der Kryptographie.

Seitdem hat sich die moderne Kryptographie stetig weiterentwickelt.

Heute hat sich das mathematische Wissen im Bereich der Kryptographie stark erweitert.

Es wurden auch prozessorientierte, atemberaubende Konzepte und Erfindungen entdeckt, die den Schutz von Texten - unsere schriftliche Kommunikation - weiter vorangebracht und sicherer gemacht haben.

Im Folgenden möchten wir mehr als zwei Dutzend grundlegende Konzepte, Meilensteine, Megatrends und nachhaltige Veränderungen für eine sichere Online-Kommunikation und Verschlüsselung hervorheben und zusammenfassen, die auch die Grundlage für die Veröffentlichung einer modernen Enzyklopädie bilden.

Die Blütezeit der "Ende-zu-Ende“-Verschlüsselung (1)

Die Umstellung auf eine entsprechende Ergänzung der Punkt-zu-Punkt-Verschlüsselung durch eine Ende-zu-Ende-Verschlüsselung (↗[24]) wurde nicht nur technisch, sondern auch in der gebräuchlichen Sprache durchgeführt: Beide Verschlüsselungswege (Punkt-zu-Punkt wie auch Ende-zu-Ende) waren strukturell immer präsent.

In jedem Fall hat das Bewusstsein für die Ende-zu-Ende-Verschlüsselung jedoch zunehmend an Bedeutung gewonnen, da das Internet und die mobile Kommunikation zu Beginn des 21. Jahrhunderts zunehmend überwacht und abgefangen wurden.

Jeder spricht heute von Ende-zu-Ende-Verschlüsselung. Ja, "Ende-zu-Ende-Verschlüsselung" wird von vielen Bürgern sogar als Begriff für "Verschlüsselung" selbst verwendet.

Wir fragen uns heute, ob die Verbindung zwischen Dir und mir auch durchgängig verschlüsselt ist, also von meinem Ende zu Deinem Ende und damit ohne Lücken sei.Denn eine Punkt-zu-Punkt-Verschlüsselung in E-Mail und Chat - wie beim bekannten XMPP-Chat (↗[61][32]) - bedeutet, dass der Benutzer zum Server eine Transportverschlüsselung hat.

Der Server kann die Daten lesen und dann verschlüsseln, bevor er sie erneut Punkt-zu-Punkt (Transport)-verschlüsselt sendet.

Dies zeigt auch, dass zu dieser Zeit alte Chat-Protokolle oder Transportverschlüsselungen entwickelt wurden und dass die entsprechenden Anwendungen heutzutage aufgrund fehlender Programmierung von (kontinuierlicher) Ende-zu-Ende-Verschlüsselung architektonische Probleme haben - oder zumindest Anstrengungen unternehmen sollten, um diese Lücken zu füllen.

Die Ende-zu-Ende-Verschlüsselung muss häufig angefordert oder vorgeschrieben und später installiert werden.Beispielsweise hat XMPP ein Manifest für die Verschlüsselung veröffentlicht (↗[61]), aber nur wenige Clients und Server haben ihren Inhalt und Code bisher verbessert.

Es bleiben Fragen zu einer fragmentierten IT-Architektur sowie zum inhaltlichen Qualitätsstandard offen: ob alle modernen Möglichkeiten im kleinsten gemeinsamen Nenner erarbeitet werden können.

Das bedeutet, dass die neueren Entwicklungen - zum einen, die auf dem Algorithmus RSA basierenden Clients (↗[12] [52]) mit alternativen Algorithmen wie NTRU (↗[36][67] [11][23]) und McEliece (↗[50][06][20][51]) auszustatten und zweitens, die Möglichkeit eines schnellen und häufigen Austausches der Schlüssel für eine Ende-zu-Ende-Verschlüsselung - durch das Manifest in eine undefinierte Zukunft verschoben wurden.

Dies erfordert in einer IT-Landschaft mit zahlreichen Klienten und Servern einen erheblichen Programmieraufwand bzw. den Ausschluss von Klartext auf jedem Weiterleitungsserver: Wenn wir alle XMPP-Messenger mit RSA-Verschlüsselung deaktivieren und alle Server sperren möchten, die Klartexte weiterleiten - sie also konsequent dem Ende-zu-Ende-Paradigma folgen -