Vertrauen im Nebel

Dr. Christian Grothoff
Professor für Informatik, BFH

Spätestens seit den Enthüllungen von Edward Snowden und dem neuen Bundesgesetz zur Überwachung des Post- und Fernmeldeverkehrs (BÜPF) ist jedem bewusst, dass private Kommunikation im Internet nicht a priori geschützt ist. Selbstschutz durch Verschlüsselung ist angesagt.

Eine notwendige Voraussetzung zum Verschlüsseln sind öffentliche Schlüssel, und diese sicher zu erlangen, ist schwierig. Nicht nur haben sich staatliche und privatwirtschaftliche Organisationen durch ihre Überwachungspartnerschaft diskreditiert und sind somit als Vertrauensanker für private Kommunikation untauglich. Nein, auch die Anforderungen im privaten Umfeld, wo pseudonyme Kommunikation wichtig sein kann, z. B. um berufliche und sexuelle Identitäten zu trennen, stehen im Zielkonflikt mit den üblichen Registrationssystemen. Diese versuchen, jedem Menschen genau eine Identität zuzuordnen. Wie können wir also an Schlüssel kommen, um unsere persönliche Kommunikation zu schützen?

Opportunistische Verschlüsselung

Wenn beide Parteien gleichzeitig online sind, ist die einfachste Methode dazu, das Schlüsselmaterial gleich am Anfang der Kommunikation zu senden. Diese Methode wird auch als opportunistische Verschlüsselung bezeichnet. Sie ist effektiv gegen passive Angreifer, die Nutzdaten nur durch Mitlesen der Kommunikation erlangen. Ein aktiver Angreifer, der in den Netzverkehr eingreifen kann, könnte jedoch die Schlüsseldaten beim Austausch ändern und die Teilnehmerschlüssel durch Angreiferschlüssel ersetzen. Danach könnte der Angreifer die Nutzdaten entschlüsseln und verändern.

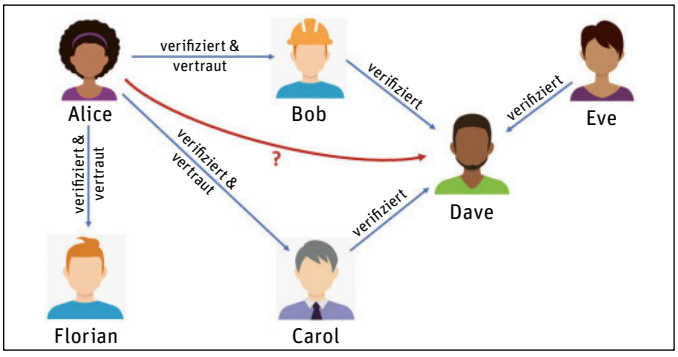

Abb. 1: Web of Trust

Trust on First Use

Eine Möglichkeit, dies zu verhindern, besteht darin, dass die Software sich den Schlüssel merkt. Sollte sich der Schlüssel der Gegenstelle ändern, wird der Benutzer alarmiert. Wenn ein Angreifer dann nicht jedes Mal bei der Kommunikation erfolgreich eingreift, ist der Benutzer zumindest gewarnt. Dieses Verfahren ist auch als Trust on First Use bekannt, da man der Netzwerkverbindung bei der ersten Benutzung vertrauen muss.

Trustwords

Es besteht natürlich die Möglichkeit, dass ein Angreifer schon beim ersten Kontakt aktiv in den Verbindungsaufbau eingreift. Dies kann entdeckt werden, indem man die Schlüssel unter Nutzung eines anderen Kommunikationskanals prüft, z. B. indem man sich die Schlüssel für E-Mails am Telefon vorliest. Leider sind die Schlüssel unhandlich lange Zahlen. Um daher das Vorlesen zu vereinfachen, verwendet z. B. die Schweizer pEp AG ein Verfahren, bei dem die Schlüssel auf sogenannte Trustwords abgebildet werden. Wer dann die Stimme des Kommunikationspartners am Telefon erkennt und die richtigen Trustwords vorgelesen bekommt, kann sich sicher sein, dass der richtige Schlüssel ausgetauscht wurde.

Web of Trust

Eine traditionelle dezentrale Alternative zur Schlüsselverifikation von Personen ist das sogenannte Web of Trust.

Hier wird das soziale Umfeld in die Verifikation mit einbezogen. Angenommen Alice hat bereits die Schlüssel von Bob, Carol und Florian verifiziert und möchte jetzt den Schlüssel von Dave verifizieren (Abb. 1). Wenn jetzt Dave bereits von Bob, Carol und Eve verifiziert wurde und Alice weiterhin Bob und Carol vertraut, dann reicht es, wenn Bob und Carol den Schlüssel von Dave zertifiziert haben. Beim Web of Trust werden solche Zertifikate gesammelt und auf sogenannten Keyservern gespeichert. Wenn dann Alice einen Schlüssel überprü-

fen will, sucht ihre Anwendung auf den Keyservern nach passenden Zertifikaten von Personen, die Alice bekannt sind und denen sie vertraut.

Metadaten

Um Schlüssel mit dem Web of Trust zu verifizieren, muss bekannt sein, wer welche Schlüssel zertifiziert hat. Da in der Regel diese Zertifikationen im Umfeld der Person stattfinden, kann man aus diesen Zertifikationsdaten das soziale Umfeld der Teilnehmer kartieren. Wer also das Web of Trust einsetzt, um seine Kommunikationsdaten zu schützen, exponiert seine Metadaten: Mit den öffentlichen Daten vom Web of Trust kann man ablesen, wer (wahrscheinlich) mit wem genügend Zeit verbracht hat, um den Schlüssel zu prüfen.

Solche Metadaten zu schützen, ist aber genauso wichtig wie der Schutz der eigentlichen Kommunikation. So bekannte Michael Hayden, der ehemalige Direktor sowohl der CIA als auch der NSA: «We kill people based on metadata» – d.h., Metadaten werden von den USA bereits als ausreichend aussagekräftig eingestuft, um die Entscheidung zu treffen, Leute zu ermorden.

Leider ist der Schutz von Metadaten technisch viel schwieriger als die Verschlüsselung des Inhalts eines Datenstroms.

Fog of Trust

An der Berner Fachhochschule arbeiten wir mit verschiedenen Partnern in Europa an einem Verfahren, welches das soziale Geflecht zur Prüfung von Schlüsseln nutzbar macht, ohne dieses zu exponieren. Wie beim Web of Trust müssen Teilnehmer Schlüssel zertifizieren. Statt dass alle Zertifikate auf einem Server im Web landen, werden diese beim Fog of Trust jedoch nur dem Schlüsselinhaber ausgehändigt. Wenn jetzt im obigen Beispiel Alice den Schlüssel von Dave prüfen möchte, schickt sie eine verschlüsselte Liste von Menschen, denen sie vertraut (also z. B. Bob, Carol und Florian). Wichtig ist, dass Dave nie erfährt, wem Alice vertraut. Dave erzeugt dann einen kryptografischen Beweis, der Alice zeigt, wie viele ihrer vertrauenswürdigen Personen den Schlüssel von Dave zertifiziert haben (im Beispiel sind das zwei). Sie erfährt jedoch nicht, welche Teilnehmer Dave zertifiziert haben.

Zukunftsfragen

Benutzbares Schlüsselmanagement ist eine zentrale Herausforderung für den Datenschutz. Jede Architektur zur Prüfung von Schlüsseln induziert gesellschaftliche Machtstrukturen, da sie die Regeln für digitale Partizipation festlegt. Diese Problematik sollte gerade auch in der Diskussion um die Privatisierung einer neuen Architektur für elektronische Identitätsdokumente (E-ID) eine Rolle spielen. Die BFH unterstützt die Diskussion mit ihrer Kompetenz in Forschung und Lehre.

Kontakt
– christian.grothoff@bfh.ch

Infos
– risis.bfh.ch
– ti.bfh.ch/informatik

Abb. 2: Fog of Trust – vertrauensvoll im schützenden Nebel