Vertrauen unter GenossInnen

PGP in der Praxis, Teil 2: Web of Trust

> In der letzten Ausgabe hatten wir ein wenig über PGP-Schlüssel und ihre Verwaltung sowie die digitale Signatur geplaudert. All das ist recht nett und auch sicher, solange sich die Gegenseite im Umgang mit der Technik so dämlich anstellt, wie sie das gegenwärtig tut (oder zu tun scheint). Wenn sie irgendwann mal geschickter wird, werden aber auch wir vorsichtiger sein müssen, und weil das nicht ganz trivial ist, lohnt sich schon jetzt ein Blick auf das Web of Trust.

Um kurz zu rekapitulieren: PGP funktioniert ein wenig wie eine große Wand von Briefkästen. Auf jedem Briefkasten steht mindestens eine Mailadresse. Der öffentliche Schlüssel entspricht in etwa einer Angabe wie „mein Briefkasten ist der 121. von links in der dreiundzwanzigsten Reihe“. Euer geheimer Schlüssel ist demgegenüber wie der reale Briefkastenschlüssel.

Mann in der Mitte

Nehmen wir jetzt an, ihr wolltet an konspa@anarcho.org schreiben. Ihr besorgt euch also wie im ersten Teil diskutiert ihren öffentlichen Schlüssel -- in der Briefkastenmetapher findet ihr raus, auf welchem Briefkasten „Konspa“ steht. Leider ist es für Joe den Staatsschützer im wirklichen Leben nicht schwer, „Konspa“ auf einen Briefkasten zu schreiben. Für PGP-Schlüssel kann das -- je nach dem, wie die Schlüssel so verbreitet werden -- schwieriger oder einfacher sein, möglich ist es auf jeden Fall.

Hat jetzt aber Joe euch seinen eigenen öffentlichen Schlüssel als Konspas untergeschoben, werft ihr den Brief in *seinen* Kasten, den er natürlich aufschließen kann. Ist er ordentlich perfide, wird er den gelesenen Brief nachher bei Konspa einwerfen (also mit Konspas wirklichem öffentlichen Schlüssel verschlüsseln), und niemand merkt, dass da was nicht stimmt.

Sowas heißt Man-in-the-Middle-Angriff und ist ein Einfallstor, um das sich alle Verschlüsselungssysteme kümmern müssen. Die Bundesregierung versucht sowas etwa gerade unter dem Titel „Bürgerportal“, wobei der Staatsapparat Schlüssel ausgibt, unterschreibt und -- vermutlich -- Nachschlüssel einbehält. Damit kann zwar jedeR leicht nachprüfen, ob der Staat glaubt, dass ein Schlüssel zu einer Person gehört, aber wir müssen wohl kaum erläutern, warum mensch das so wirklich nicht haben will.

Die soziale Lösung

Wenn im realen Leben Anna wissen möchte, ob Arthur wirklich Arthur von der Aargauer Antifa ist -- und exakt darum geht es hier --, wird sie (hoffentlich) nicht seinen Personalausweis prüfen. Stattdessen wird Arthur vielleicht von Barbara vom Baseler Bundschuh „vorgestellt“, und wenn Anna Barbara von ein paar Vernetzungstreffen kennt, würde sie danach wohl an Arthurs Identität glauben.

Das ist das Vorbild für das Web of Trust bei PGP-Schlüsseln. Die erste Basis dafür ist die Signatur. Anders als im ersten Teil, als es um die Signatur von Nachrichten ging, unterschreiben wir jetzt öffentliche Schlüssel. Eine solche Unterschrift unter einen Schlüssel entspräche im realen Sozialleben einer öffentlichen und dauernden Kundgebung von Barbara, dass Arthur eben Arthur ist.

Die zweite Basis ist eine Einschätzung der Vertrauenswürdigkeit von Menschen. Im PGP-Universum gibt es vier Niveaus von Vertrauen: niemals, kaum, vollständig und absolut. Die Bedeutung dieser Begriffe ist konfigurierbar, ist aber typischerweise etwa, dass eine Unterschrift

- von einer Person, der ihr niemals vertraut, ignoriert wird,

- von einer Person, der ihr kaum vertraut, ein Drittel zum Vertrauen in den unterschriebenen Schlüssel zählt,
- von einer Person, der ihr voll oder absolut vertraut, bereits ausreicht, um den Schlüssel für authentisch zu halten.

Der Rechner kann dazu noch „über Ecken“ gucken. Vertraut ihr etwa B, und hat B einen Schlüssel von C unterschrieben, die dann wieder einen von D unterschrieben hat, kann das das Vertrauen in den Schlüssel von D auch stärken, was aber nichts an den einfachen Grundkonzepten von Vertrauen und Beglaubigung ändert. Wichtig dabei ist, dass *ihr* entscheidet, wie vertrauenswürdig eine Person *für euch* ist.

Gewonnen ist mit dieser ganzen Prozedur, dass ihr auch Schlüssel von Menschen prüfen könnt, die ihr noch nie gesehen habt, sofern das Web of Trust dicht genug geknüpft ist, und das ohne jede Obrigkeit. Darin liegt vielleicht auch der Charme der Sache: Hier wird letztlich ein technisches Problem sozial gelöst, und das ist ein schöner Gegensatz zur gesellschaftlichen Norm des Versuches, soziale Probleme technisch (z.B. durch Kameraüberwachung) zu lösen.

Wie unterschreiben?

Die einfachen Kozepte können am Rechner natürlich immer noch eher konfus aussehen. Die im ersten Teil erwähnten Schlüsselverwaltungen bieten aber normalerweise relativ durchschaubare Schnittstellen für die Einstellung von Vertrauen und das Unterschreiben von Schlüsseln. In Thunderbird/Enigmails Schlüsselverwaltung finden sie sich im Kontextmenü (also nach einem Rechtsklick) der Schlüsselzeilen.

Ihr solltet Schlüssel nur dann unterschreiben, wenn ihr sicher seid, dass der Schlüssel wirklich zur „Identität“ passt, also zu der Person, die vernünftigerweise zu der/den E-Mail-Adresse/n gehört. Dazu müsst ihr einerseits sehen, ob ihr es mit der betreffenden Person zu tun habt -- was logischerweise nur geht, wenn ihr sie in der Realität kennt. Andererseits müsst ihr sehen, ob der öffentliche Schlüssel, den ihr habt, zum privaten Schlüssel dieser Person gehört.

Beim ersten Schritt kann euch PGP nicht helfen; der hat tatsächlich gar nichts mit Rechnern zu tun. Beim zweiten Schritt hingegen hilft die Mathematik. Ein PGP-Schlüssel ist nämlich eine sehr lange Zahl, die kein Mensch angucken will. Deshalb definiert der OpenPGP-Standard ein Verfahren, das aus diesen sehr langen Zahlen etwas kürzere Zahlen macht, die zwecks Romantik „Fingerabdruck“ genannt werden. Wenn die Fingerabdrücke von zwei Schlüsseln übereinstimmen, kann ziemlich sicher davon ausgegangen werden, dass sie auch wirklich identisch sind.

Wenn ihr nun einen Schlüssel beglaubigen wollt, könnt ihr euch von dem/der SchlüsselinhaberIn den Fingerabdruck vorlesen oder auf einem Zettel geben lassen oder etwas ähnliches. In der Schlüsselverwaltung von Thunderbird bekommt ihr den Fingerabdruck des fremden öffentlichen Schlüssels in der Dialogbox angezeigt, mit der ihr unterschreiben könnt. Experimentiert einfach mal -- wenn ihr es euch anders überlegt, könnt ihr Unterschriften immer noch zurückziehen.

Damit das Web of Trust funktioniert, müsst ihr dafür sorgen, dass andere Menschen eure Unterschrift an dem Schlüssel sehen. Der einfachste Weg dazu ist, den fremden öffentlichen Schlüssel zu exportieren und auf einen Keyserver hochzuladen (Enigmail hat einen Menüeintrag extra für diesen Zweck). Die Keyserver sind schlau genug, nur die neuen Unterschriften rauszuziehen und sich gegenseitig abzugleichen.

Wenn andere Menschen euren Schlüssel unterschreiben wollen, müsst ihr den Fingerabdruck eures eigenen Schlüssels herausfinden. Auch das geht in Schlüsselverwaltungen -- im Thunderbird/Enigmail etwa durch Rechtsklick auf euren eigenen Schlüssel und Auswahl von „Eigenschaften“. Vielleicht ist es keine schlechte Idee, immer ein paar Zettel mit diesem Fingerabdruck dabei zu haben.

Was unterschreiben?

Der technische Vorgang des Unterschreibens ist also eigentlich einfach. Viel schwieriger ist die soziale Frage, ob mensch wirklich öffentlich unterschreiben will[1]. Das Web of Trust kann nämlich auch die Gegenseite nachbauen. Aus den Unterschriften unter einem Schlüssel ist zumindest zu rekonstruieren, wer alles meint, den/die SchlüsselinhaberIn zu kennen. Manchmal ist das nicht schlimm -- etwa, wenn ihr ohnehin schon mit den Leuten telefoniert oder sie mit laufendem Mobiltelefon trefft und es nicht nötig ist, die

Beziehung vor Privatmenschen (sagen wir, Nazis) geheimzuhalten.

In anderen Fällen ist so eine Kundgebung richtig blöd. Wenn ihr z.B. eine klandestine Politgruppe habt, sonst nicht per PGP kommuniziert und dann, quasi als digitale Blutsbrüderschaft, alle gegenseitig ihre Schlüssel unterschreiben, könntet ihr die Mitgliedsliste auch gleich ans BKA geben. In so einem Szenario solltet ihr eure Schlüssel direkt austauschen und auf die Unterschreiberei verzichten.

Umgekehrt ist es sicher eine gute Idee, die Schlüssel von Ortsgruppen von „vertrauenswürdigen“ Schlüsseln unterschrieben zu haben. Bei der nächsten BDV könnte die Datenschutzgruppe einen entsprechenden Dienst anbieten (das müssen wir aber erst mit Leuten abstimmen, die die OGen wirklich kennen...). Dass wir die Schlüssel von Ortsgruppen und Ortsgruppen unseren Schlüssel unterschreiben, gibt der Gegenseite wenig Information über Offensichtliches („Die sind auf Zack!“) hinaus.

Eine allgemeingültige Regel, wann mensch zum Web of Trust beitragen will und wann nicht, ist kaum anzugeben. Je mehr aber eure Eltern, die Kumpels aus der Eckkneipe oder dem Ökocafe, befreundete HackerInnen und alle möglichen anderen Bekannten euren Schlüssel signieren (und ihr ihren), desto harmloser ist es, wenn auch Politleute unterschreiben; rauszukriegen, wer im Web of Trust Zecke ist und wer Bürger, wird unter diesen Umständen schon deutlich schwieriger.

Solange allerdings das BKA noch versucht, auf haarsträubende Weise externen Sachverstand zu PGP einzukaufen[2], sind allzu viele Gedanken zu dem Thema vermutlich übertriebene Paranoia. Vielleicht reicht es für die nächsten paar Jahre, die OG-Schlüssel signiert zu kriegen; mit dem Gedanken an das Web of Trust und späteren Umgang damit sollte mensch sich aber trotzdem vertraut machen, denn wenn die Gegenseite anfängt, unsere Verschlüsselung anzugreifen, schadet es bestimmt nicht, wenn wenigstens wir in der Roten Hilfe einen kühlen Kopf bewahren (können).

Datenschutzgruppe der Roten Hilfe Heidelberg

datenschutzgruppe@rotehilfe.de

PGP Fingerprint: a3d8 4454 2e04 6860 0a38 a35e d1ea ecce f2bd 132a

http://www.datenschmutz.de

[1] Ihr könnt Unterschriften auch so markieren, dass sie beim Export unterdrückt werden. Sowas kann sinnvoll sein, ist aber fürs Web of Trust natürlich irrelevant.

[2] http://annalist.noblogs.org/post/2009/01/04/bka-ratespielchen-rund-um-gnupg