Alle Schlüssel an einem Bund

Ein neuer Modus der Verteilung der PGP-Schlüssel der Roten Hilfe

> Wenn ihr eine verschlüsselte Mail an buxtehude@rote-hilfe.de schreibt, woher wisst ihr dann eigentlich, dass wirklich die Leute aus Buxtehude den Schlüssel haben und nicht, sagen wir, der Hamburger Staatsschutz? Realistisch ist die Antwort derzeit meistens: gar nicht, denn die Art, wie wir in der RH die Echtheit von Schlüsseln sicherstellen wollten, hat in den letzten Jahren immer schlechter funktioniert. In diesem Artikel wollen wir kurz erzählen, was passiert ist und dann einen neuen Plan für die zuverlässige Verteilung von Schlüsseln vorstellen.

Wer bisher mit der Roten Hilfe verschlüsselt Kontakt aufnehmen wollte, hat auf unserer Kontaktseite Instruktionen gefunden, unseren (den der Datenschutzgruppe) Schlüssel zu importieren, anhand des unten gedruckten Fingerprints nachzusehen, ob der auch in Ordnung ist, dann dem Schlüssel das Vertrauen auszusprechen und schließlich damit zu sehen, ob andere RH-Schlüssel damit richtig unterschrieben sind.

Das funktionierte, solange wir auf vertrauenswürdigen Kanälen Fingerabdrücke von Ortsgruppen oder anderen Stellen bekommen haben und dann die unterschriebenen Schlüssel auf die Schlüsselserver hochgeladen haben. Wir haben uns damit ganz gut vorbereitet gesehen auf den Tag, an dem die Staatsgewalt PGP angreift.

Mehr dazu ist in den ansonsten unserer bescheidenen Meinung nach immer noch lesenswerten PGP-Artikeln aus RHZ 3/09 und 4/09 zu erfahren – wenn euer Archiv nicht so weit zurückreicht, probiert https://datenschmutz.de/gc.

Das Ende eines Plans

Dreh- und Angelpunkt des Verfahrens ist, dass Menschen explizit Schlüssel prüfen, denn grundsätzlich fällt jede Verschlüsselung mit Vertraulichkeit und Echtheit der Schlüssel. Faustregel: Wenn ihr nie gefragt werdet, ob ihr einem Schlüssel vertraut, vertraut ihr die *gesamte* Verschlüsselung jemand anders an – im Fall von HTTPS, also eurem Webbrowser, sind das zum Beispiel ausgerechnet Polizeiausrüster wie T-Systems oder Atos.

Unser Plan, diese Verifikation über Unterschriften der Datenschutzgruppe hinzubekommen, war aber über die Jahre immer zweifelhafter geworden. Es verwenden nämlich die meisten weniger computeraffinen Menschen PGP durch den Mailclient Thunderbird und seine Erweiterung Enigmail. In dieser Kombination war es schon seit Jahren immer schwieriger geworden, die Vertrauensprüfung über diese Unterschriften zu machen – das hat inzwischen viele Klicks gebraucht, und mensch musste schon wissen, wo mensch hinschauen sollte. Insofern dürften sogar die, die das vor vielen Jahren mal gemacht haben, inzwischen damit aufgehört haben.

Der Plan starb engültig letztes Jahr, als irgendwelche Spaßvögel Schlüssel mit einer Unzahl von Unterschriften auf die Schlüsselserver legten. Das hat nicht nur diese belastet, sondern vor allem auch alle, die diese Schlüssel importieren wollten – im Effekt waren die PGP-Unterschriften zu einem Vehikel für Denial of Service-Angriffe geworden. Da es in dem alten Modell („Web of Trust") entscheidend darauf ankam, dass jede_r Unterschriften für jeden Schlüssel hochladen konnte, ist in diesem Rahmen kein dauerhaft wirksames Kraut gegen so einen Angriff gewachsen.

Es wollte auch niemand mehr ein wirkliches Kraut finden, denn seit der Markt den kommerziellen (und repressiven) Wert von sozialen Graphen entdeckt hat (also: wer macht was mit wem?), ist eigentlich klar, dass die alte Utopie des Web of Trust vom Kapitalismus aufgefressen ist. Wenn ihr so wollt: Ölpest des 21. Jahrhunderts.

Jedenfalls: Unterschriften von den Schlüsselservern

gehen nicht mehr, und die Prüfung von Unterschriften aus anderen Quellen ist ein obskures Ritual geworden. Wir brauchen also etwas anderes, wenn wir Leuten, die mit der RH in Kontakt treten wollen, weiter eine glaubhafte Verschlüsselung anbieten wollen.

Alle Schlüssel an einem Bund

Grundidee unseres Ersatzverfahrens ist: Alle PGP-fähigen Mail-Clients können gut die Unterschrift unter Mails prüfen und zeigen das auch sehr klar an.

Das nutzen wir jetzt, indem wir einfach alle Schlüssel, mit denen Organisationsfremde kommunizieren wollen könnten (also die der Ortsgruppen, diverser Gremien, des BuVo) in einer einzigen unterschriebenen Mail verschicken. Stimmt die Unterschrift, könnt ihr die Schlüssel importieren und habt zumindest auch die in gewissem Sinn verifizierten Schlüssel in eurem Schlüsselbund. Diese Mail mit den Schlüssel könnt ihr per Web-Formular bestellen (oder bei Bedarf auch irgendwie anders; rührt euch, wenn ihr so einen Bedarf habt).

Allerdings tut sich wieder das Problem mit der Echtheit der Unterschrift auf. Die Lösung dafür ähnelt der bei unserer alten Lösung: Der Fingerabdruck des einen Schlüssels, der die Mail mit dem Schlüsselbund unterschreibt, ist zum Beispiel in der RHZ zu finden (nämlich ab jetzt auf Seite FIXME: Redaktion, baut das doch bitte ein). Damit das ganze Verfahren des Einsammelns von Schlüsseln aber nicht zwingend an der Datenschutzgruppe hängt, gibt es dafür einen Schlüssel, der schluessel@rote-hilfe.de gehört (das sieht nur aus wie eine Mailadresse – es hat keinen Sinn, Mail dorthin zu schicken, und ihr könnt mit dem öffentlichen Schlüssel davon auch nicht verschlüsseln).

Wenn ihr mit dem Fingerprint den Schlüssel verifiziert habt, bekommt ihr bei unserer Schlüsselbundmail ein klares Ja oder Nein im Hinblick auf die Echtheit der Mail. Solltet ihr je ein Nein bekommen, *kann* es sein, dass euch jemand falsche Schlüssel unterschieben will – und davon wüssten wir dann gerne.

Auf https://rote-hilfe.de/ueber-uns/adressen (genauer einer Seite, die von dort verlinkt ist) haben wir eine schrittweise Anleitung, wie das mit Thunderbird und Enigmail geht – probiert das Rezept gerne aus, und wenn es (einmal) nicht (mehr) funktionieren sollte, sagt bitte gleich Bescheid

Unterdessen gilt weiter, was wir vor über zehn Jahren in RHZ 4/09 geschrieben haben: „Solange [die Behörden selbst mit Verschlüsselung und Verifizierung von Schlüsseln kämpfen], sind allzu viele Gedanken zu dem Thema vermutlich übertriebene Paranoia. [...] Doch] wenn die Gegenseite anfängt, unsere Verschlüsselung anzugreifen, schadet es bestimmt nicht, wenn wenigstens wir in der Roten Hilfe einen kühlen Kopf bewahren (können)."

Kontakt und Artikel-Archiv: https://datenschmutz.de

PGP Fingerprint: 4FD3 B3EE 7FCE 9FFD EC75 CAF9 4847 5F52 5C0C 5DB1