c't magazin für computer technik

Krypto-Kampagne

(PGP/GnuPG-Schlüssel-Zertifizierung auf Messen)

Was ist PGP?

Pretty Good Privacy (PGP/GnuPG) ist ein anerkannter und sicherer De-facto-Standard für authentische und vertrauliche E-Mails. Elektronische Nachrichten sind auf dem Weg durchs Netz neugierigen Blicken und Manipulationsversuchen ungeschützt ausgeliefert. Außerdem lassen sich Absenderangaben beliebig verfälschen, sodass über die Identität des Urhebers zunächst keine gesicherte Information vorliegt. Abhilfe schafft Krypto-Software wie PGP oder GnuPG.

PGP benutzt so genannte Public-Key-Verschlüsselung. Dabei besitzt jeder Anwender ein zusammengehöriges Schlüsselpaar aus einem geheimen und einem öffentlichen Schlüssel. Daten, die mit dem öffentlichen Schlüssel chiffriert sind, lassen sich ausschließlich mit dem geheimen Gegenstück wieder dechiffrieren. Umgekehrt kann ein Anwender beispielsweise für einen Text mit seinem geheimen Schlüssel eine digitale Signatur erstellen. Deren Überprüfung durch einen Empfänger fällt nur bei Verwendung des zugehörigen öffentlichen Schlüssels und des unveränderten Textes positiv aus. So können zweifelsfrei der Urheber einer Signatur bestimmt und Manipulationen an unterschriebenen Daten erkannt werden.

Wozu braucht man eine Zertifizierung?

Bei der Erzeugung eines Schlüsselpaares gibt der PGP/GnuPG-Anwender Name und E-Mail-Adresse an, die in einer so genannten User-ID (UID) im öffentlichen Schlüssel abgelegt werden. Die angegebenen Daten sind jedoch beliebig. Deshalb muss man sich vor der Benutzung eines Public Keys davon überzeugen, dass er auch wirklich zu seinem vorgeblichen Inhaber gehört. Dies ist jedoch besonders schwierig, wenn man sich (noch) nicht persönlich kennt.

Die Echtheit eines Schlüssels kann auch durch die digitale Signatur einer vertrauenswürdigen dritten Partei bestätigt werden, der man die gewissenhafte Überprüfung der gemachten Angaben überlässt. Mit unserer Signatur zertifizieren wir die Korrektheit der Daten in den UIDs eines PGP-Schlüssels. Die Authentizität unserer Signatur-Schlüssel lässt sich anhand der im Heft abgedruckten PGP-Fingerprints leicht überprüfen.

Warum eine Krypto-Kampagne?

Anlass zum Start der Krypto-Kampagne im Frühjahr 1997 waren die damals aufkommenden Bestrebungen zur Einschränkung von Verschlüsselungstechnologien zu Gunsten einer einfacheren Strafverfolgung. Entsprechende Pläne wurden nicht umgesetzt, kommen aber immer wieder in die Diskussion. Seit 1997 hat die Krypto-Kampagne mehr als 20 000 PGP-Schlüssel signiert, was einen erheblichen Beitrag zur Verbreitung des offen PGP-Standards leisten konnte.

Die nun eingeführte Überprüfung der E-Mail-Adressen soll helfen, die Qualität von Signaturen im PGP-Vertrauensnetz zu verbessern. Die Krypto-Kampagne will dadurch die Vertrauenswürdigkeit von signierten PGP-Schlüsseln stärken und ein stärkeres Bewusstsein für den Umgang mit Identitäten, Signaturen und Verschlüsselung in einer digitalen Informations-Umwelt schaffen.

Heise Zeitschriften Verlag GmbH & Co. KG | Redaktion c't | Helstorfer Straße 7 | 30625 Hannover

Key-ID DAFFB000 | Fingerprint A3B5 24C2 01A0 D0F2 355E 5D1F 2BAE 3CF6 DAFF B000