Privatsphäre ohne Zutun

pEp-Aktivist Hernâni Marques im Interview

Das über eine Stiftung finanzierte Projekt „pretty Easy privacy“ (pEp) soll verschlüsselter Kommunikation zum Durchbruch verhelfen. Die Integration ins beliebte Thunderbird-Add-on Enigmail könnte ein wichtiger Schritt dahin sein. Stiftungsrat Hernâni Marques spricht über das Konzept und weitere Pläne von pEp.

c’t: Herr Marques, Sie sind Vorstandsmitglied im Schweizer CCC. Wie hat es Sie in die pEp-Stiftung verschlagen?

Hernâni Marques: Die Ziele der pEp-Stiftung decken sich politisch und technisch mit den Aktivitäten des CCC in der Schweiz, sodass die Stiftung zum Beispiel ein Referendum gegen das Überwachungsgesetz BÜPF finanziell unterstützt hat. Ich wurde vom pEp-Chefentwickler Volker Birk, ebenfalls Aktivist des CCC-CH, angefragt und habe umgehend zugesagt, im Stiftungsrat aktiv zu sein.

Gerade leite ich auch Teile des Enigmail/pEp-Projekts. Am meisten allerdings bin ich mit Community-Arbeit und administrativen Aufgaben bei der Stiftung beschäftigt. Die Community-Arbeit umfasst Vorträge und Kommunikation zu pEp, doch auch Aktivitäten im Rahmen der Internet Engineering Task Force (IETF), um pEp als Internet-Standard zur Diskussion zu stellen.

c’t: pEp soll Ende-zu-Ende-Verschlüsselung massentauglich machen. Wie wollen Sie echtes Privacy-by-Default erreichen?

Marques: Im ersten Schritt soll E-Mail-Verschlüsselung nach dem IETF-Ansatz der opportunistischen Verschlüsselung (RFC 7435) automatisiert werden. Der User soll möglichst keine Fragen beantworten müssen. pEp hat die Aufgabe, sich darum zu kümmern, dass die Privatheit bestmöglich gesichert wird und dass die Kommunikationspartner automatisch in den Besitz der dafür nötigen Schlüssel kommen.

Bei E-Mail heißt dies dann auch, dass nicht nur der Inhalt, sondern auch die Metadaten geschützt werden sollen – wenn immer möglich. Anders als bei Ansätzen von Privacy-by-Design soll es nicht bloß *möglich* sein, die Privatsphäre zu schützen, sondern sie soll wann immer möglichst ohne Zutun automatisch geschützt werden; per Voreinstellung, was Privacy-by-Default ist. Beispielsweise verschlüsseln wir bei pEp automatisch Header, indem wir die eigentliche Mail mitsamt ihren Headern mit einem Outer-Envelope umschachteln. Zudem ist vorgesehen, dass wir den SMTP-Standard um ein Kommando erweitern, um Onion-Routing für E-Mail zu ermöglichen. Durch den Verschachtelungsansatz des pEp-Nachrichtenformats sind wir hierfür bereits vorbereitet. In einem weitergehenden Schritt möchten wir Textnachrichten durch das GNUnet verschicken – ein P2P-Framework für sichere und volldezentralisierte Netzwerke.

Hernâni Marques will den Privacy-per-Default-Ansatz durchsetzen.

c’t: Der pEp-Ansatz sieht allerdings einige Kompromisse vor, die absolute Vertraulichkeit unterminieren können. So verzichten Sie darauf, private Schlüssel mit einer Passphrase zu versehen: ist das Gerät kompromittiert, dann auch der Schlüssel.

Marques: Das pEp-Projekt richtet sich nicht gegen gezielte Angriffe. Mit genug Aufwand ist jedes Endgerät beliebig angreifbar. Wir sind nicht überzeugt, dass eine Passphrase die Sicherheit bei gezielten Angriffen erhöht. Der Angreifer braucht nur zu warten, dass die Passphrase eingegeben wird, um die zusätzliche Hürde zu überwinden. Zudem haben Passphrases einen entscheidenden Nachteil: Die Usability leidet massiv.

Wir wissen aus der Praxis der Crypto-Partys, die wir seit den Snowden-Enthüllungen in der Schweiz regelmäßig durchführen, dass Benutzer die Lust an der ständigen Eingabe einer Passphrase verlieren – und zuletzt das OpenPGP-Setup aufgeben. Wir sind der Ansicht, dass die Benutzer ihre Geräte selbst mit einer ausreichend langen Passphase oder einem Code absichern sollten, um ihre Operational Security zu erhöhen.

c’t: Das große Ziel von pEp ist, Ende-zu-Ende-Verschlüsselung auf vielen Kommunikationskanälen mit pEp zu vereinfachen. Wie ist da derzeit der Entwicklungsstand?

Marques: Beim pEp-Projekt wird zurzeit an vier Lösungen für Endbenutzer-Software gearbeitet: pEp für Android (im Google Play Store und in f-droid), Outlook (im Digitalcourage-Shop), iOS und Enigmail/pEp. Ein wichtiges Feature bei pEp, das so rasch wie möglich aktiviert wird, ist Schlüsselsynchronisation (KeySync) zwischen mehreren Geräten, damit ein Benutzer seine E-Mails über mehrere Geräte lesen kann. Auch Browser-Add-ons möchten wir entwickeln und weitere weniger beachtete Plattformen abdecken, wofür wir eigens eine neue Entität auf der re:publica im Mai vorstellen: die pEp-Genossenschaft. Diese wird vorher unter anderen von Sibylle Berg, Marc-Uwe Kling, Meinhard Starostik und Juli Zeh begründet. *(hob@ct.de)* c't