Holger Bleich, Bernhard Münkel

Vertrauen auf den ersten Blick

Automatische E-Mail-Verschlüsselung mit Steed

Ein neues Projekt soll auch bei Privatleuten die Akzeptanz von E-Mail-Verschlüsselung fördern. Ziel ist es, die Technik in den Hintergrund treten zu lassen und alle Vorgänge zu automatisieren. Doch zur Realisierung von „Steed“ sind noch viele Hürden zu nehmen.

Nur wenige Nutzer nehmen die Mühe auf sich, zur E-Mail-Verschlüsselung ein Vertrauensnetzwerk aufzubauen oder alternativ Geld in ein CA-Zertifikat zu investieren. Diesem Problem wollen Werner Koch und Marcus Brinkmann mit einem neuen Projekt begegnen. Werner Koch ist Mitbegründer der Free Software Foundation Europe und Hauptentwickler von GnuPG, der Implementierung des offenen Verschlüsselungsstandards OpenPGP. Sein Partner Marcus Brinkmann entwickelt seit vielen Jahren an Debian und GNU/Hurd.

Sie kennen also das Problem zu gut, dass S/MIME und OpenPGP zwar sicher sind, aber dem Wunsch eines durchschnittlichen Benutzers nach einfacher Bedienung und vor allem nach Kompatibilität nicht nachkommen [1]. Im Oktober 2011 haben sie ein Konzeptpapier vorgelegt, in dem sie Veränderungen an Mail-Clients, -Servern und Verschlüsselungsmodulen vorschlagen. Mit möglichst minimalem Zutun des Anwenders soll die zugrundeliegende Technik dafür sorgen, dass alle Nachrichten per Voreinstellung verschlüsselt werden.

Das „Steed“ (Secure Transmission of Encrypted Electronic Data) genannte Projekt soll wesentliche Prozesse bei der Mail-Verschlüsselung ändern [2]. Es sieht vor, dass Schlüssel automatisch generiert, geprüft und via DNS verteilt werden. Den Erfindern zufolge liegt der Clou darin, dass die Methode vollständig kompatibel zu den beiden Verschlüsselungsstandards PGP und S/MIME ist.

Schlüssel DNS

Gemäß Steed prüft der Mailclient bereits bei seiner Installation in einem öffentlichen Verzeichnis, ob für das frisch angelegte Mail-Konto ein öffentlicher Schlüssel existiert. Ist dies der Fall, fragt die Anwendung den Nutzer nach seinem privaten Schlüssel, um Mail-Inhalte dechiffrieren zu können. Existiert noch kein Schlüssel, so erzeugt der Client entweder ein OpenPGP-Schlüsselpaar oder einen selbstzertifizierten S/MIME-konformen Schlüssel.

Der Anwender wird lediglich nach seinem Einverständnis und der obligaten Passphrase gefragt. Das S/MIME-Zertifikat und/oder den selbstsignierten öffentlichen OpenPGP-Schlüssel schickt der Mailclient ohne Zutun des Anwenders dann in das Verzeichnis, wo sie für jedermann auffindbar sind.

Laut Koch und Brinkmann leiden insbesondere die bestehenden OpenPGP-Schlüssel-Datenbanken unter dem Problem, dass sie weder skalierbar noch jederzeit, etwa durch Firewalls hindurch, automatisch zu erreichen sind. Diese Unsicherheit überträgt sich demnach auf die Nutzer, die deshalb lieber gleich auf Verschlüsselung verzichten.

Die beiden Entwickler suchten einen anderen Speicherort und wurden im Domain Name Service (DNS) fündig: Die DNS-Infrastruktur ist zwingend von jedem Rechner mit Internetzugang aus erreichbar. Außerdem ist sie dezentral, skalierbar und ausfallsicher aufgebaut und mit DNSSEC sogar gegen Mithören abgesichert.

Bindeglied

Seit geraumer Zeit schon wird das DNS in ähnlicher Weise bereits für DomainKeys Identified Mail (DKIM) genutzt, um Phishing und Spam zu begegnen: Zu jeder Domain gehört ein öffentlicher Schlüssel, der im DNS hinterlegt ist. Die Domaininhaber können Mails mit ihrem privaten Schlüssel signieren. Der Empfänger kann mit dem öffentlichen Gegenstück prüfen, ob die Mail tatsächlich von der Domain kommt, die im Mailheader steht.

Koch hält die Umsetzung von DKIM aber für „überflüssig und fehlerhaft“. Wie man seiner Ansicht nach das DNS besser für eine Public-Key-Infrastruktur (PKI) nutzen kann, beschrieb er bereits 2006 in seinem Konzept „Public Key Association“ (PKA) [3]. Darin definierte er das DNS als Verbindung zwischen Absenderangabe und zugehörigem öffentlichem Schlüssel und nannte das Ganze „ein vereinfachtes Vertrauensmodell für OpenPGP und selbstsignierte X.509-Zertifikate“.

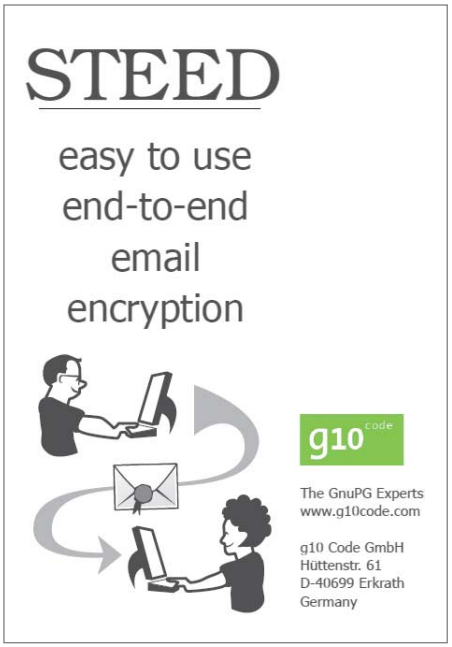
Nun soll PKA bei Steed zum Einsatz kommen. Weitgehend unbekannt ist, dass das DNS bereits heute einen eigenen Record-Typ zum Abspeichern von Zertifikatsinformationen vorsieht. Diese CERT-Ressource-Records sollen gemäß Steed künftig zu jeder E-Mail-Adresse einen Fingerprint entweder eines S/MIME-Zertifikats oder eines selbstsignierten OpenPGP-Schlüssels enthalten. Hinzu kommt der Verweis in Form eines URI, wo Zertifikat und/oder öffentlicher Schlüssel komplett herunterzuladen sind.

Erhält der Steed-vorbereitete Mailclient nun eine signierte Mail einer unbekannten Person, etwa von alice@example.net, kann er im DNS mit alice._pka.example.net nach dem öffentlichen Schlüssel suchen. Eine manuelle Abfrage im DNS nach Infos zur unterschriebenen Mailadresse würde so aussehen:

```
$ host -t cert alice._pka.example.net
alice._pka.example.net text "v=pka1;fpr=47[...]A907;
                uri=http://example.net/alice.pubkey.txt"
```

Den hier angegebenen Fingerprint („fpr“) kann der Mailclient nun mit dem vom Schlüssel in der Mailsignatur generierten Hash abgleichen. Damit lässt sich immerhin schon einmal sicher sagen, dass derjenige, der die Mail geschickt hat, auch Gewalt über die DNS-Records zur Absende-Domain hat. Sollte der Fingerprint nicht passen, ist die Absenderangabe gefälscht.

In diesem Konzept kommt den Mailprovidern folglich eine wichtige Rolle zu: Sie herrschen über die Domains, fungieren also als Schnittstelle zwischen Mailclient und DNS. Sie müssen es ihren Anwendern ermöglichen, den CERT-Record zur Mail-Adresse zu verwalten. Im Steed-Konzeptpapier heißt es dazu: „Ein Protokoll zwischen Mailclient und dem Provider-Backend für die Schlüsselverwaltung ist nötig, um die nötige Interaktion zwischen Nutzer und Mailprovider unsichtbar zu machen.“ Die Entwickler schlagen vor, dazu IMAP entsprechend zu erweitern.



Ein Flyer soll Steed Besuchern von Fachkongressen schmackhaft machen.

Gegenüber c't betonte Koch, dass der Mailprovider zwar das Bindeglied zwischen seinen Kunden und dem DNS als Verzeichnis darstellt, aber nicht als Vertrauen gebende Instanz fungieren kann. Wie soll der Sender dann Schlüsseln über den Weg trauen, wenn er weder auf ein Web-of-Trust (OpenPGP) noch auf ein CA-Zertifikat (S/MIME) setzen kann?

Diesem Einwand begegnen die Steed-Erfinder mit dem Vertrauensmodell „Trust upon first contact" (TUFC): Beim Schlüsselabruf wird ein Zertifikat übertragen, das der Client anschließend prüfen und akzeptieren kann. Verläuft dieser Check erfolgreich, entscheidet allein der Nutzer beim ersten Kontakt, ob er die Adresse in seine Liste vertrauenswürdiger Mailpartner aufnimmt (Whitelist) oder ihn künftig blockiert (Blacklist). Künftig entfallen weitere Nachfragen, es sei denn, der Nutzer ändert in einem „Expertenmodus" manuell den Status.

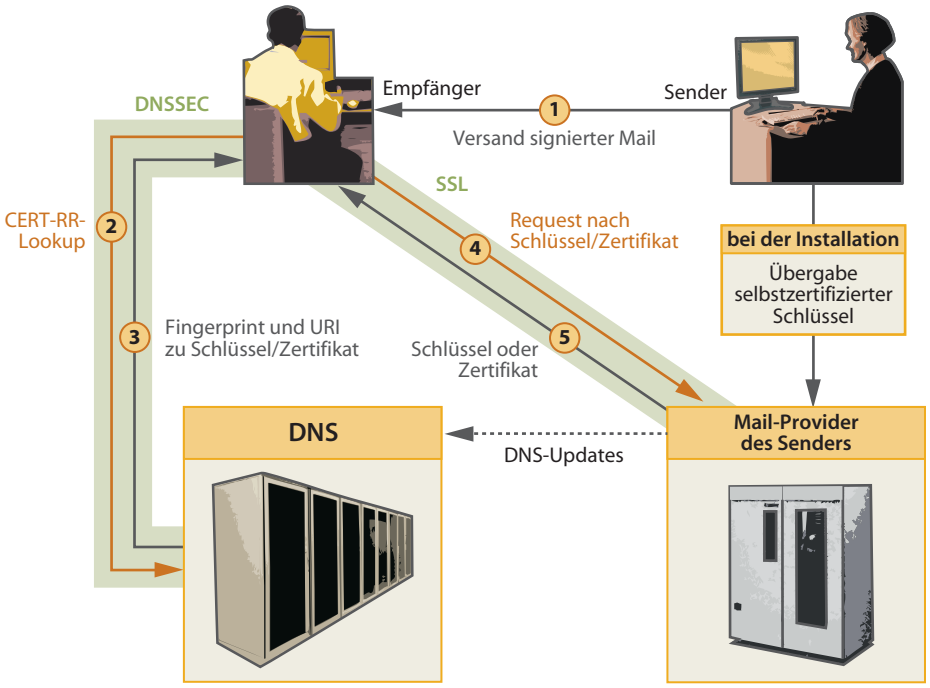
Vertrauen bei Kontakt

Bei Steed heißt diese dauerhafte Verbindung „persistency of preudonym" (POP). Sie wird stärker, je länger sie hält. TUFC, so erklären die beiden Erfinder, sei deshalb so gut geeignet, weil es im Unterschied etwa zum gängigen S/MIME-Modell „menschliche Vertrauensentscheidungen ermöglicht und unterstützt, anstatt sie zu ersetzen".

Auf diese Form des Vertrauensmodells trifft übrigens jeder Internetnutzer, der eine verschlüsselte Verbindung zu einem Mail- oder Webserver aufruft: Beim Erstkontakt muss er den angebotenen SSL-Schlüssel und das zugehörige unbekannte Zertifikat manuell bestätigen, sofern das Zertifikat nicht von einer bekannten Authority ausgestellt wurde und damit extern als vertrauenswürdig eingestuft wurde.

TUFC ist nicht prinzipiell neu, weicht aber von den bei E-Mail eingesetzten Vertrauensinfrastrukturen ab. Hinter einem Zertifikat steht nicht mehr zwingend eine vertrauenswürdige Instanz. Der Anwender ist noch mehr in der Verantwortung, ob er einem Zertifikat vertraut oder nicht. Die Autoren weisen darauf hin, dass dieses Verfahren bereits heute bei Administratoren gängige Praxis ist, etwa bei Verbindungen mit Root-Shells: Erst nach der ersten Kontaktaufnahme wird der Schlüssel übertragen und bleibt erhalten, bis eine Veränderung gemeldet wird.

Dieses „Vertrauen bis zur Änderung" wirft die Frage auf, was passiert, wenn Schlüssel oder Zertifikate kompromittiert sind oder ihre Gültigkeit verlieren. Dazu findet sich im Steed-Konzept nicht viel. Eine Rollover-Prozedur müsse geschaffen werden für den Fall, dass Zertifikate ungültig werden oder sich die Mailadresse ändert. Ein neues Zertifikat müsse automatisch mit dem alten überschrieben werden, bevor es verteilt werde. Ein Mechanismus müsse dafür sorgen, dass kompromittierte und zurückgezogene Zertifikate aus dem Verzeichnis verschwinden. Für die Portabilität der Krypto-Identität soll bei Steed ein eigens zu entwerfender PIM-Service sorgen. Ein Tool also, das es ermöglicht, den privaten und öffentlichen Schlüssel, ein eventuell vorhandenes X.509-Zertifikat sowie die vertrauenswürdigen Kontakte zu einem Paket zu sichern und transportfähig zu machen. So soll es möglich sein, dieselbe Mailadresse auf mehreren Rechnern oder mobilen Geräten wie Pads oder Telefonen zu nutzen.



Nach dem Steed-Konzept holt sich der Mailclient des Empfängers die nötigen Infos zum Absender aus dem DNS.

Viele Änderungen

Der Tatsache, dass die bisherigen Vertrauensmodelle Web-of-Trust und CA-Zertifikate sich nicht an breiter Front durchgesetzt haben, begegnen Koch und Brinkmann also nun mit Steed. Im Kern postulieren sie drei Dinge, die gegeben sein müssen: Die automatische Schlüsselerstellung, die automatische Schlüsselverteilung via DNS sowie Verschlüsselung per Voreinstellung („security-by-default").

Werner Koch wirft derzeit auf vielen Spezialisten-Veranstaltungen seinen Namen in den Ring und möchte Mitglieder von Standardisierungsgremien, aber auch Administratoren auf den Steed-Geschmack bringen. Das White Paper zum Projekt wird immerhin ausgiebig in der GnuPG-Mailingliste diskutiert.

Um Steed – insbesondere die Idee der Default-Verschlüsselung – zu realisieren, wären technische Änderungen an den beteiligten Komponenten notwendig. Mailclients müssten lernen, im DNS nach öffentlichen Schlüsseln zu suchen sowie lokale Schlüssel zu generieren, zu signieren und zu speichern.

Die beiden Entwickler haben nach eigenen Angaben zunächst drei Mail-Programme ins Auge gefasst, bei denen sie die Erweiterung realisieren wollen: Mutt, Claws-Mail und Thunderbird, „da dieser wahrscheinlich die am häufigsten benutzte Open-Source-Mailsoftware ist", erläutert Koch. „Outlook wollen wir auch gerne unterstützen", so der Entwickler. Dazu habe bislang aber lediglich ein ergebnisoffenes Gespräch mit dem Bundesamt für Sicherheit in der Informationstechnik (BSI) und dem zuständigen Microsoft-Entwicklungschef stattgefunden.

Genauso wichtig ist es, die Mailprovider mit ins Boot zu holen, da sie ja die Änderungen am DNS durchreichen müssen. „Ich habe einige informelle Gespräche geführt, aber kein Interesse gefunden", konstatiert Koch. Das Geschäftsmodell fehle, teilte man ihm demnach mit, und: „Wir machen jetzt sowieso De-Mail". Die Steed-Entwickler erwägen, zunächst als „Proof of concept" eigene DNS-Proxies bereitzustellen.

Doch die technischen Änderungen in der Infrastruktur sind nicht das größte Problem des Konzepts. Seine Akzeptanz hängt von Unternehmen ab, deren primäres Ziel ist, mit der Dienstleistung E-Mail Geld zu verdienen. Erst wenn diese einen Vorteil darin sähen, die Kommunikationssicherheit ihrer Kunden zum Teil des Geschäftsmodells zu erheben, stünden die Chancen für eine Realisierung von Steed besser. Doch das ist nicht in Sicht. (hob)

Literatur

[1] Holger Bleich, Schlüsselfragen, Vertrauenswürdige E-Mail-Kommunikation, c't 18/12, S. 132
[2] Projekt-Homepage und White Paper: http://g10code.com/steed.html
[3] Whitepaper zum PKA-Konzept: http://g10code.com/docs/pka-intro.de.pdf