Aktueller Stand der E-Mail-Verschlüsselung

Vorteile von E-Mail als Kommunikationsmedium

- dezentrales Protokoll ohne Besitzer
- große Auswahl an Clients
- große Auswahl an Server-Anbietern
- hohe Verbreitung und Akzeptanz
- fehlende Funktionalität kann durch Formatierung des Inhalts nachgerüstet werden (z.B. HTML-Formatierung, Verschlüsselung, ...)

Sinn und Zweck von E-Mail-Verschlüsselung

Vorteile

- Privatheit und Vertraulichkeit von Kommunikation
- Verschlüsseln von Dateianhängen
- Authentifizierung durch Signierung

Nachteile

- Einrichtungsaufwand
- Notwendigkeit der Schlüsselverwaltung (Sammeln und Vorhalten von fremden öffentlichen Schlüsseln sowie Sichern der eigenen privaten Schlüssel) oder der Beschaffung eines Zertifikats
- alle Arten von Scans (z.B. nach Malware) müssen vor dem Verschlüsseln erfolgen
- erhöhter Prozessoraufwand sowie größere Datenmenge

E-Mail-Verschlüsselungssysteme

PGP

- Ende-zu-Ende-Verschlüsselung
- zum Verschlüsseln sowie Signieren geeignet
- Schlüssel können lokal erzeugt werden, jedoch muss der Public Key verteilt werden
- Forward Secrecy nicht vorgesehen
- nicht nur für E-Mail-Verkehr, sondern auch für Verschlüsselung von Dateien geeignet
- wird generell als die sicherste offene Verschlüsselungsmethode angesehen

S/MIME

- Ende-zu-Ende-Verschlüsselung
- zum Verschlüsseln sowie Signieren geeignet
- benötigt Zertifikats-Aussteller-Authorität (CA)
- Forward Secrecy nicht vorgesehen
- nur für den Austausch von E-Mail-Nachrichten vorgesehen

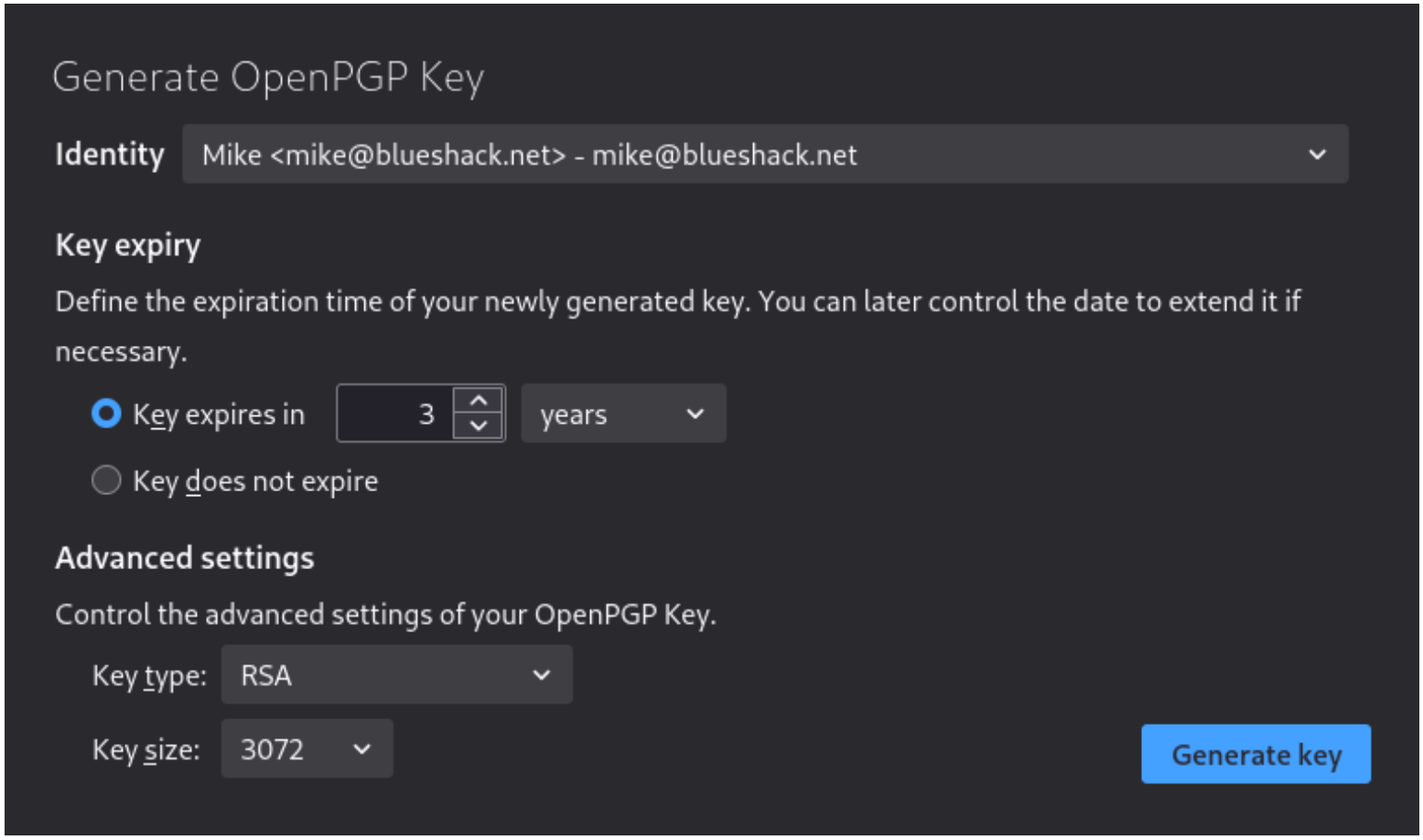
TLS (SSL)

- Transportverschlüsselung
- meist zu Marketing-Zwecken ohne explizite Abgrenzung von e2e-Verschlüsselungsmethoden erwähnt
- Forward Secrecy möglich
- der Abruf von E-Mails sollte unabhängig anderer Verschlüsselungsmethoden immer über TLS statt über eine nicht transportverschlüsselte Verbindung erfolgen

Funktionsweise am Beispiel von PGP

- Erzeugen eines Schlüsselpaars (privater und öffentlicher Schlüssel)
- Import von fremden öffentlichen Schlüsseln
- optionales Verschlüsseln bei jedem Mailversand, sofern öffentliche Schlüssel für alle Empfänger vorhanden sind
- optionales Signieren bei jedem Mailversand
- Versenden von unverschlüsselten und unsignierten Mails ist weiterhin möglich

Erstellen eines Schlüsselpaars



Beim Erstellen eines Schlüsselpaars kann ein automatisches Ablaufdatum eingestellt sowie die Verschlüsselungsmethode und die Größe des Schlüssels eingestellt werden.

Das Ergebnis sind zwei Dateien, die in der Schlüsselverwaltung angezeigt und von dort aus exportiert werden können. Ist ein Wiederrufs-Schlüssel gewünscht, muss dieser explizit generiert werden.

Schlüsselpaar beim Public Key-Verfahren

privater Schlüssel

- zum Entschlüsseln von eingehenden Nachrichten
- zum Signieren von ausgehenden Nachrichten
- muss unter allen Umständen privat bleiben

öffentlicher Schlüssel

- für andere Personen, zum Verschlüsseln von Nachrichten an die eigene Adresse
- für andere Personen, zum Überprüfen von mit dem privaten Schlüssel erstellten Signaturen
- kann beliebig öffentlich geteilt werden

Inhalt einer verschlüsselten E-Mail

unverschlüsselter Text

```
Test
```

verschlüsselter Text (gekürzt)

```
-----BEGIN PGP MESSAGE-----

wcFMA3h2FVxexNWlAQ/8CZ7h6T7D3WaMQioyac

j3ig+9LE+hNJxnJvOqe5ybadpx22Pi6ExmGVcy

hvi25y6PFq8hwIgtarHrSgv2t/nSt9FHSN+INR

K/pet1cXbCH2QNckohFX0H5thsUa6j3NL08rSY

-----END PGP MESSAGE-----
```

Der oftmals gezogene Vergleich zu einem Briefumschlag hinkt: Weder kann eine verschlüsselte E-Mail durch geringsten Aufwand geöffnet werden, noch kann nach einer Entschlüsselung festgestellt werden, dass die E-Mail entschlüsselt wurde

Metadaten werden weitgehend (bis auf den Betreff) im Klartext transportiert

Komplexität der Einrichtung

- (Open)PGP ist mittlerweile in einigen E-Mail-Clients (z.B. Thunderbird) inkludiert und bedarf nur noch der Einrichtung und nicht mehr der Installation von Drittanbieter-Software. Die Vermittlung des Verständnisses der Technologie an sich ist jedoch nicht Teil dieser Programme.
- Einige Betriebssysteme (darunter fast alle Linux-Distributionen) werden bereits mit den Software-Komponenten für PGP-Verschlüsselung sowie dem systemweit nutzbaren Schlüsselbund ausgeliefert. In manchen dieser Distributionen ist Thunderbird ebenfalls bereits vorinstalliert; in allen anderen kann dieser oder ein anderer Client aus dem offiziellen Repository geladen werden.

Austausch von öffentlichen Schlüsseln

- wird der eigene Schlüssel auf einen Schlüsselserver geladen, sollte daran gedacht werden, diesen dort wieder zu invalidieren, sofern er nicht mehr verwendet werden soll
- verwendet man die Funktionen des Web of Trust, so sind die Verbindungen zu anderen Mailadressen und damit Personen und Unternehmen ersichtlich
- der Austausch eines Fingerprints in Person ist ratsam (mündlich/telefonisch oder per "Visitenkarte"); der Austausch des Schlüssels nur bedingt, weil dies meist die Verbindung von fremder mit eigener Hardware erfordert, was ein Sicherheitsrisiko an sich darstellt
- blinde Verschlüsselung allein ist kein Sicherheitsmerkmal - man sollte sicherstellen, dass man mit der richtigen Person kommuniziert

Zukunftstauglichkeit

...im Bezug auf andere Möglichkeiten zur Verschlüsselung

- Eine Vielzahl an Messengern bietet heute die Möglichkeit, mit deutlich geringerem Einrichtungsaufwand Ende-zu-Ende-verschlüsselt zu kommunizieren.
  Dabei liegen die Schlüssel jedoch fast immer beim Anbieter, womit nicht derselbe Grad an Vertraulichkeit gewährleistet ist. Zudem ist jeweils nur die Kommunikation mit Usern innerhalb desselben Netzwerks möglich.
- Die allgemeinen Vorteile des E-Mail-Protokolls können zu denen der E-Mail-Verschlüsselung hinzugezählt werden.

...im Bezug auf Sicherheit der Verschlüsselungsmethode

- Mit unendlich Zeit können sowohl PGP- wie S/MIME-verschlüsselte Nachrichten entschlüsselt werden, sodass nicht von einer unendlich währenden Verschlüsselung ausgegangen werden kann.
- Sobald ausreichend fähige Quantencomputer existieren, wird die Sicherheit von PGP- und S/MIME-verschlüsselten Nachrichten untauglich sein (und damit alle bis dahin versendete Nachrichten lesbar werden). Eine Lösung basierend auf asymmetrischen Public Key-Verfahren ist dann anzunehmenderweise überholt und muss symmetrischen oder nicht-digitalen Verfahren weichen.

Persönliche Meinung

Verschlüsselung ist nicht kinderleicht, und muss es auch nicht sein - der Fokus sollte auf dem Gewinn von Privatsphäre liegen, denn das ist der Sinn und Zweck.

Kommunikation im Allgemeinen sollte frei zugänglich, kostenlos und sicher sein.
Dass das heute Realität ist, ist nicht selbstverständlich, sondern durch die freiwillige und oft unentgeltliche Arbeit vieler fähiger Leute möglich.

Fragen & Diskussion

"Aktueller Stand der E-Mail-Verschlüsselung"

Manuel Kämpf

2022-04-23

https://cryptoparty-tuebingen.de/files/20220423/aktueller-stand-email-verschluesselung.zip