EMail's ver- und entschlüsseln (Praxisarbeit)

Kennenlernen von zwei Methoden zur Ver- und Entschlüsselung von EMails mit PGP.
Dauer: 2 Lektionen. Dies ist eine Arbeit für 2-er Gruppen!

Dokumentieren sie alle Installations- und Konfigurationsschritte!

Einführung
OpenPGP und S/MIME sind die beiden wichtigsten Standards für E-Mail-Verschlüsselung. Das S/MIME-Protokoll verwendet dabei X.509-Zertifikate und ist deshalb nicht kompatibel zu OpenPGP, das ein "Web of Trust" mit öffentlichen OpenPGP Schlüsselservern ist, auch wenn es dieselben kryptografischen Verfahren (Asymmetrische Verschlüsselung mit privaten und öffentlichen Schlüsseln für Schlüsseltausch und Textverschlüsselung mit symmetrischem Verfahren) verwendet. (PGP = Pretty Good Privacy; S/MIME = Secure Multipurpose Internet Mail Extensions)

Hauptanwendungen von OpenPGP sind die Signierung und die Verschlüsselung von E-Mails. Dafür gibt es zwei Formate:

- **PGP/INLINE** (z.B. für Webmail)
  Die E-Mail wird dabei von ihrer Struktur her als gewöhnliche Textmail erzeugt, die verschlüsselten Text als kodierten Text enthält.
  Nicht für HTML-Mails!
  Dateianhänge können vorab verschlüsselt und/oder signiert werden (im Fall von Webmail muss man das ohne entsprechendes Browser-AddOn selber machen). Allerdings garantieren die Signaturen dann nicht die Integrität der Mail insgesamt. Signierte Teile können unbemerkt entfernt werden, in anderem Zusammenhang signierte Daten können hinzugefügt werden (was nur auffiele, wenn man sich die Mühe machte, die Zeitstempel der einzelnen Signaturen zu vergleichen). Nachteile von PGP/Inline: Mailprogramme, die OpenPGP nicht verstehen, zeigen die Signatur im Text an, was verwirrend sein kann.

- **PGP/MIME**
  Dieses Verfahren deckt auch Dateianhänge und HTML-Mails ab. Für den Mailbody und alle Anhänge kann jeweils einzeln festgelegt werden, ob sie verschlüsselt und/oder signiert werden sollen. Auch dieses Verfahren schützt aber nur den Inhalt der Mail, nicht ihre Kopfdaten (Absender, Empfänger, Betreff, Datum).

Das OpenPGP-Protokoll wird von vielen Produkten unterstützt. Zum Beispiel das kommerzielle PGP und das freie Open-Source-Programm GnuPG.

Ein zentrales Thema ist die Schlüsselbeglaubigung (Schlüsseltausch!). Dies soll aber nicht Gegenstand dieser Übung sein!

Info zur 1. Aufgabe
In dieser Aufgabe verschlüsseln wir die EMails mit Mailvelope. Dies ist ein Verschlüsselungs-AddOn mit OpenPGP für Webmail. Anhänge können damit nicht verschlüsselt werden. Dieses AddOn macht von JavaScript Gebrauch und kann darum ein gewisses Sicherheitsrisiko darstellen. Darum nur als Notlösung für z.B. Webmail verwenden! Das Mailvelope-AddOn ist für verschiedene Webbrowser verfügbar. Wir werden es in dieser Übung innerhalb Firefox verwenden.

Info zur 2. Aufgabe
Unter Verwendung von dem frei verfügbaren GnuPG (PGP wäre die kommerzielle Variante) bzw. der Windows-Variante Gpg4win werden wir innerhalb eines EMail-Clients (Thunderbird) EMails mit dem AddOn Enigmail ver- und entschlüsseln.

Vorarbeiten

Bevor sie loslegen, lesen sie bitte den ganzen Text einmal sorgfältig durch!

Die folgenden Arbeiten erledigen sie auf ihrem Laptop. Entweder auf dem Laptop selbst oder in einer virtuellen vmware-WIN7/8/10-Maschine.

- Thunderbird als MailClient installieren (https://www.mozilla.org/de/thunderbird/)
- Wir benötigen einen EMail-Account, denn man über einen Mailclient wie Thunderbird, Outlook etc. aber auch über ein Webmail-Interface bewirtschaften kann. Es werden ihnen dazu für die Dauer der Übung folgende EMail-Accounts zur Verfügung gestellt:
  a@noldar.ch / b@noldar.ch / c@noldar.ch / d@noldar.ch / e@noldar.ch / f@noldar.ch
  Sie sprechen sich innerhalb der Klasse ab, welche Gruppe welche noldar-EMail-Adresse verwendet!
  Richten sie den EMail-Account auf Thunderbird ein! Details dazu siehe im Anhang!
- Firefox installieren (https://www.mozilla.org/de/firefox/new/)

Bei der ersten Übung werden wir EMail's in Firefox bzw. über das Webmail erstellen und empfangen.
Bei der zweiten Übung werden wir im Mailclient Thunderbird EMail's erstellen und empfangen.

Zur Kontrolle werden sie mir je einmal (Aufgabe B und Aufgabe C) eine verschlüsselte EMail zukommen lassen: EMail-Adresse: master@noldar.ch. Der Public-Key entnehmen sie der Webseiten-Info unter www.noldar.ch/contact/ (Siehe ganz unten: Somethin‘ to hide? Pretty good!)

Sie werden im Folgenden mehrere Möglichkeiten haben, ein OpenPGP-Schlüsselpaar zu erzeugen. In allen Fällen sehen die beiden Schlüssel aber immer so aus: (Also z.B. Datei: FelixMuster.asc / asc steht für ASCII)

Der öffentliche Schlüssel:

```
-----BEGIN PGP PUBLIC KEY BLOCK-----
Version: GnuPG v2

mHjzBFYjc.
...
...
...
Gw==

-----END PGP PUBLIC KEY BLOCK-----
```

Der private Schlüssel:

```
-----BEGIN PGP PRIVATE KEY BLOCK-----
Version: Mailvelope v1.2.0
Comment: https://www.mailvelope.com

wqdsf
...
...
...
fAp77rQ

-----END PGP PRIVATE KEY BLOCK-----
```

Und die verschlüsselte Botschaft:

```
-----BEGIN PGP MESSAGE-----
Charset: utf-8
Version: GnuPG v2

Qqvms5xQ160
...
...
...
xeyXD

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

1. **Aufgabe A: Schlüsselpaar erzeugen**
   Installieren sie Gpg4win, ab V2.2.6. (http://gpg4win.org/download.html) Dies ist die Free-Windows-Variante von GnuPG bzw. OpenPGP! Alles installieren!
   Erzeugen sie in Kleopatra (gehört zum Lieferumfang von Gpg4win) unter "Datei/Neues Zertifikat/Persönliches OpenPGP-Schlüsselpaar erzeugen" ihr eigenes Schlüsselpaar. Alternativ können sie das Schlüsselpaar auch im Mailvelope (siehe nächste Aufgabe) erstellen!
   Hinweis: Beim Erzeugen eines Schlüsselpaars wird von ihnen eine sog. Passphrase verlangt. Dies ist ein Passwort, das sie später beim Erstellen und Öffnen einer verschlüsselten Nachricht eingeben müssen. Die Passphrase also nicht vergessen und unter keinen Umständen weitergeben!
   Kleopatra ist der Zertifikatsmanager von GnuPG. Damit können sie die Schlüssel verwalten. Öffentliche Schlüssel, die sie von ihren Kommunikationspartner erhalten, müssen sie zuerst in das System einpflegen.
   Deponieren sie ihren öffentlichen Schlüssel als asc-Datei auf dem BSCW im M114-Ordner/Public-Keys.

2. **Aufgabe B: Sichere EMail mit Mailvelope**
   Öffnen sie Firefox und gehen sie auf die Mailvelope-Webseite www.mailvelope.com (https://www.mailvelope.com/de/)
   Installieren sie das Firefox-AddOn Mailvelope. Neben der Firefox-URL-Eingabezeile ist neu das Mailvelope-Symbol hinzugekommen, das man anklicken muss, um weitere Einstellungen zu tätigen. Hier könnte man auch ein Schlüsselpaar erzeugen!
   Öffnen sie ihr Webmail und erstellen sie darin verschlüsselte Emails:
   a. Suchen sie sich Kommunikationspartner in der Klasse aus (die öffentlichen Schlüssel liegen ja auf dem BSCW) und und tauschen sie gegenseitig verschlüsselte EMails aus.
   b. Als Arbeitskontrolle verschicken sie eine an mich verschlüsselte EMail, die als Text ihren öffentlichen Schlüssel (in Textform eingefügt) enthält! EMail-Adresse: master@noldar.ch. Der Public-Key entnehmen sie der Webseiten-Info unter www.noldar.ch/contact/ (Siehe ganz unten: Somethin‘ to hide? Pretty good!) Nach Erhalt ihrer EMail werde ich ihnen eine mit ihrem öffentlichen Schlüssel verschlüsselte Botschaft zurückschicken.
   Hinweis: Das AddOn Mailvelope tritt dann in Erscheinung, wenn sie den EMail-Text eingeben. Am rechten Fensterrand erscheint ein Schreibblock-Symbol. Wenn sie dies anklicken, öffnet sich der Mailvelope-Editor. Nach Eingabe ihres Textes wählen sie Verschlüsseln und geben an, für wen sie diesen Text verschlüsseln wollen. Dazu muss der öffentliche Schlüssel ihres Adressaten zuerst in Mailvelope eingetragen worden sein. Dies können sie über die Mailvelope-Optionen (Mailvelope-Symbol rechts oben anklicken) unter "Schlüssel importieren" erledigen. Nachdem sie ihren Text verschlüsselt haben, erscheint er im Webmail-Fenster chiffriert und mit dem PHP-Header `-----BEGIN PGP MESSAGE-----` versehen.

3. **Aufgabe C: Sichere EMail mit Enigmail**
   Installieren sie in Thunderbird das AddOn Enigmail V1.8.2 (oder neuer) (https://www.enigmail.net/download/)
   Erstellen sie nun in Thunderbird verschlüsselte Emails:
   a. Suchen sie sich Kommunikationspartner in der Klasse aus (die öffentlichen Schlüssel liegen ja auf dem BSCW) und und tauschen sie gegenseitig verschlüsselte EMails aus.
   b. Als Arbeitskontrolle verschicken sie eine an mich verschlüsselte EMail, die als Text ihren öffentlichen Schlüssel (in Textform eingefügt) enthält! EMail-Adresse: master@noldar.ch. Der Public-Key entnehmen sie der Webseiten-Info unter www.noldar.ch/contact/ (Siehe ganz unten: Somethin‘ to hide? Pretty good!) Nach Erhalt ihrer EMail werde ich ihnen eine mit ihrem öffentlichen Schlüssel verschlüsselte Botschaft zurückschicken.
   Hinweis: Nach der Instrallation von Enigmail erhalten sie in der oberen Menuezeile den Eintrag "Enigmail". Hier können sie die Schlüssel importieren. Wenn sie eine EMail verfassen, erscheint in der oberen Menuezeile ebenfalls der Eintrag "Enigmail". Dort haben sie die Möglichkeit mit "Verschlüsselung ein" die Verschlüsselung zu bewirken. Alternativ haben sie auch ein Enigmail-Schloss-Symbol links, unterhalb des Senden-Symbols! Eine erhaltene verschlüsselte EMail wird durch anklicken automatisch entschlüsselt, wenn man vorher seine Passphrase richtig eingegeben hatte.

Ich habe bewusst verzichtet, die nötigen Schritte mit detaillierten Printscreens und präzisen Teilschritten zu erklären. Damit will ich erreichen, dass sie auch noch selber etwas mitdenken und recherchieren ;-)

Viel Erfolg!

Anhang

Es werden die Einstellungen für a@noldar.ch gezeigt! Für alle weiteren Accounts gilt Analoges. Das Passwort ist immer dasselbe! Richten sie den Email-Client immer verschlüsselt ein, damit ihre Kollegen mit Sniffer-SW nicht ihrer Email-Kommunikation lauschen können ;-)

Einstellungen MAIL	
E-Mail Konto	
Benutzername	a@noldar.ch
Passwort	**Pa$$w0rd**
DOMAIN	noldar.ch
Konfiguration ohne SSL/TLS (unverschlüsselt)	
Eingangsserver POP / IMAP	pop.noldar.ch / imap.noldar.ch
Port POP / IMAP	110 / 143
Ausgangsserver	smtp.noldar.ch
Port	25, 587
Konfiguration mit SSL/TLS (verschlüsselt)	
Eingangsserver POP / IMAP	pop.mail-ch.ch / imap.mail-ch.ch
Port POP / IMAP	995 / 993
Ausgangsserver	smtp.mail-ch.ch
Port	465

Zugang zum Webmail: https://owa.mail-ch.ch/ Einloggen mit Benutzername und Passwort!

URL und Mailaccounts werden privat von Jürg Arnold betrieben. Die Schüler werden gebeten, diese Accounts nicht zu missbrauchen und ausschliesslich für die vorliegende Lehrübungen zu verwenden.
Die Accounts werden nach der Übung restlos entfernt!