UNIVERSITÄT SIEGEN

Fakultät IV
Lehrstuhl für
Digitale Kommunikationssysteme

Praktikumsaufgabe 1
Kryptographische Verfahren und Anwendungen II
Sommersemester 2015

Aufgabe 1: Beschreiben Sie das grundlegende Konzept von OpenPGP.

a) Welche Sicherheitsdienste werden bereitgestellt?
b) Wo wird OpenPGP hauptsächlich eingesetzt?
c) Welche Schlüssel und/oder Zertifikate gibt es?
d) Wie werden diese Schlüssel/Zertifikate ausgetauscht?
e) Welche Algorithmen können eingesetzt werden? (Kurze Liste der wichtigsten, aktuell verwendeten Algorithmen.)
f) Bei der Generierung der Schlüssel werden Passwörter benötigt. Wie viele werden sinnvollerweise eingesetzt und wozu dienen sie?
g) Was bedeutet PGP/INLINE und PGP/MIME?
h) Welche Vor- und Nachteile hat OpenPGP aus Ihrer Sicht?

Aufgabe 2: Recherchieren Sie nach geeigneter Software, die Sie zum Erstellen und Verwalten von OpenPGP-Schlüsseln nutzen können, und weiterer Software, die Sie zum Austausch von Nachrichten benötigen. (Nutzen Sie ein Betriebssystem Ihrer Wahl. Auch Betriebssysteme für Smartphones können genutzt werden.)

a) Listen Sie die gefundene Software auf. Nutzen Sie die o.g. Kategorien zur Unterteilung.
b) Beschreiben Sie kurz Ihre gewählte Software (wenige Sätze genügen) und erstellen Sie eigene Screenshots, die die Benutzeroberfläche zeigen. (Bei Kommandozeilenanwendungen sollen die Screenshots sinnvolle Ausgaben anzeigen.)

Aufgabe 3: Erstellen Sie ein Schlüsselpaar für Ihre (studentische) Universitäts-E-Mail-Adresse. Erzeugen Sie auch Ihr Widerrufszertifikat.

a) Falls Sie bereits ein Schlüsselpaar für diese Adresse besitzen, laden Sie, falls noch nicht geschehen, Ihren öffentlichen Schlüssel auf einen Schlüsselserver (z.B. https://pgp.mit.edu/) hoch. Dokumentieren Sie Ihre KeyID und den Fingerabdruck. Erstellen Sie nun ein Schlüsselpaar für eine von Ihren anderen E-Mail-Adressen.
b) Protokollieren Sie die einzelnen Schritte der Schlüsselerzeugung (mit Screenshots).

c) Welche Länge sollte der Schlüssel heute mindestens haben? Welche Auswirkungen hat die Schlüssellänge? Sind sehr lange Schlüssel sinnvoll? Welche Schlüssellänge haben Sie genutzt?
d) Laden Sie Ihren öffentlichen Schlüssel auf einen Schlüsselserver (z.B. https://pgp.mit.edu/).
e) Dokumentieren Sie Ihre KeyID und den Fingerabdruck.

Aufgabe 4: Unterschrieben Sie die Schlüssel Ihrer Gruppenpartner nach sorgfältiger Prüfung der KeyID und des Fingerabdrucks und laden Sie dies auf den Schlüsselserver hoch. Jeder Schlüssel sollte von mindestens zwei Personen unterschrieben werden.
Beschrieben Sie die einzelnen Schritte, die hierfür notwendig sind und dokumentieren Sie, welche Schlüssel Sie unterschrieben haben.

Aufgabe 5: Schicken Sie Ihre das Protokoll als ZIP/tar-Archiv verschlüsselt mit PGP an thomas.koller@uni-siegen.de (KeyID: `3695ED66`, Fingerabdruck: `4E719EF64015F40013416DAC739EB27E3695ED66`) und robin.fay@uni-siegen.de (KeyID: `5900F665`, Fingerabdruck: `0EAE1B2C9DBAAAF28DE75D5E3FF08B2C5900F665`). Die notwendigen öffentlichen Schlüssel finden Sie auf dem Schlüsselserver https://pgp.mit.edu/ oder direkt auf der Webseite des Instituts. Prüfen Sie auch hier sehr sorgfältig die KeyID und den Fingerabdruck! (Was fällt Ihnen auf?)
Es werden nur korrekt verschlüsselte und im besten Fall signierte Lösungen akzeptiert ☺