Übungsblatt zur Vorlesung
Ausgewählte Themen zur Computersicherheit im WS 2017/18
Dozent: PD Dr. Reinhard Bündgen

Aufgabe A -- Softwareinstallation
Installieren Sie ein Mailprogramm, dass GPG unterstützt bzw. ein Plug-in für GPG erlaubt (letzteres ist der Fall für Thunderbird, MS Outlook, Apple Mail). Installieren Sie GPG.

Falls Sie Ihre Mailkonfiguration auf Ihrem Rechner nicht ändern wollen, können Sie gerne eine virtuelle Maschine für diesen Zweck installieren (z. B. mit Virtual Box, KVM/Qemu oder VMware).

Aufgabe B -- Schlüsselerzeugung
Lesen Sie sich ein GPG-Tutorial durch und erzeugen dann mit den GPG-Werkzeugen ein Schlüsselpaar für die e-mail Adresse, die Sie bei der Vorlesungsanmeldung angegeben haben und über die Sie Ihr Klausurergebnis erhalten wollen.
Der Schlüssel soll mindestens 2048 Bit lang und mindestens 6 Monate gültig sein.

- Testen Sie Ihr Mailprogramm zusammen mit GPG. Testen Sie, ob z. B. das Versenden von signierten Mails funktioniert.
- Senden Sie Ihren öffentlichen Schlüssel an GPG Schlüsselserver, alternativ können sie Ihren öffentlichen Schlüssel exportieren und an mich und einige Kurteilnehmer direkt schicken.

Aufgabe C – Vorbereitung KeySigning Party (bis zum 12.12.2017)
Schicken Sie bis zum 12.12.2017 eine Mail an buendgen@de.ibm.com mit dem Betreff/Subject:
Sicherheitsvorlesung WS17: KeySigning Party

Der Inhalt der Mail sollte eine einzige Zeile enthalten, die die Daten Ihres Schlüssels enthält und folgendes Format hat (Felder werden durch einen Doppelpunkt getrennt):

> Schlüssel ID : Schlüssellänge : Verschlüsselungsalgorithmus : Vorname Nachname : e-mail-Adresse : Fingerabdruck des Schlüssels : Bereitschaft, Ihre Daten zu teilen
>
> Wobei im letzten Feld ja steht, wenn Sie bereit sind, Ihre Daten mit allen anderen Teilnehmern im Kurs zu teilen und nein sonst.

Beispiel: für meinen Schlüssel sähe die Zeile wie folgt aus:

> B501DD00:4096:RSA: Reinhard Buendgen:buendgen@linux.vnet.ibm.com:70E9 725C 886B 38C9 DDCD 39F9 0D85 98B5 D8C4 6188:ja

Aufgabe D – Teilnahme bei der Key Signing Party

Kommen Sie am 15.12. zur Vorlesung und bringen Sie Folgendes mit:

- Ihren Studierendenausweis
- einen weiteren Ausweis mit Lichtbild (Perso, Führerschein, Pass, ...)
- Ihre Schlüsseldaten (, die Sie verschickt haben)
- etwas zu schreiben
- *keinen* Computer