Einzigartige Informatiker-Pflichtveranstaltung:

KEYSIGNINGPARTY 17. Juli 2008

16 bis 18 Uhr, G325, Hauptgebäude (Fachgebiet SE)

Organisiert mit dem KeysignOrg-Softwareprojekt

STELL DIR VOR, DU SCHREIBST E-MAILS UND KEINER LIEST MIT.

Genau das bietet dir die Verschlüsselungssoftware GnuPG (oder das kompatible PGP): für private Mails angenehm, für Passwörter oder andere vertrauliche Daten unverzichtbar. Andersherum kannst du deine Mails auch signieren und damit verhindern, dass sich jemand anders als du ausgibt.

Voraussetzung dafür ist allerdings die Sicherheit, dass E-Mail-Adresse und Schlüssel des Empfängers wirklich der Person gehören, der du schreiben willst — andersherum kann eine Person deiner signierten Mail nur vertrauen, wenn sie zusätzlich weiß, dass der verwendete Schlüssel deiner ist. Um das Vertrauen in einen Schlüssel auszudrücken, kann man ihn signieren. Vertrauen ist transitiv: Ist ein Schlüssel von jemandem signiert worden, dem du vertraust, kannst du auch der ersteren Person vertrauen. So lässt sich ein Web of Trust aufbauen — und genau das ist das Ziel von Keysigning Partys.

Um den Prozess so einfach wie möglich zu gestalten, entstand im Rahmen des Softwareprojekts 2007 das Programm „KeysignOrg“. Es liegt als Java-Anwendung für alle Plattformen vor und leitet sowohl den Organisator, als auch die Teilnehmer komfortabel durch den Planungsprozess.

Entwicklergruppe: Tri-Thong Truong, Maximilian Szengel, Hendrik Richert, Alexander Post, Julian Raschke

#1: Du lädst dir GnuPG herunter, erstellst einen Schlüssel und liest dir in etwa das Konzept durch. Für dein Mailprogramm gibt es sicher ein Plug-In.
#2: Wir stellen die Party-Anmeldungsseite online. Du trägst dich mit deinem Key ein.
#3: Am 15. Juli um 24 Uhr wird dir eine Liste der anderen Teilnehmer zugesandt. Du lädst dir den KeysignOrg-Client herunter und druckst die Liste aus.
#4: Auf der Party am 17. Juli triffst du Leute und notierst, dass ihr Schlüssel wirklich ihnen gehört. Wen du nicht kennst, den lernst du kennen—und prüfst seine Identität anhand seines Personalausweises.
#5: Im KeysignOrg-Tool bestätigst du dies anschließend—und lässt das Programm den von dir signierten Schlüssel per Mail zustellen. Dadurch wird auch seine E-Mail-Adresse validiert. Er kann deine Signatur jetzt an den öffentlichen Keyserver senden und jedem zeigen, dass du ihm vertraust.

Fragen? julian@raschke.de oder daniel.luebke@inf.uni-hannover.de