Freie Universität Berlin, Institut für Informatik, Arbeitsgruppe Software Engineering
Prof. Dr. L. Prechelt, S. Salinger, J. Schenk, Ute Neise, Alexander Pepper, Sebastian Ziller

Übungsblatt 12 WS 2009/2010 zum 10.3.2010

Aufgabe 12-1: (Fälschungssicherheit von Emails)

1) Viele Spam-Mails kommen von scheinbar bekannten Personen und Institutionen. Wie kann es passieren, dass Sie scheinbar eine Email von einem Freund oder einer Firma bekommen (erkennbar an der Email-Adresse im Absenderfeld), die diese aber nicht abgeschickt haben?
2) Lesen Sie das Gerichtsurteil unter http://www.jurpc.de/rechtspr/20020125.htm genau durch. Ist damit dem Betrug nun Tür und Tor geöffnet?
3) Wie wehren sich Mailinglistenbetreiber dagegen, dass Emailadressen angemeldet werden, obwohl deren Inhaber dies gar nicht veranlasst haben?
4) Wie können Sie als Sender einer Email einigermaßen sicherstellen, dass der Empfänger Ihrer Urheberschaft auch trauen kann?

Aufgabe 12-2: (Why Johnny Can't Encrypt)

1) Recherchieren Sie: Was ist PGP? Wie funktioniert es?
2) Lesen Sie die Studie *Why Johnny Can't Encrypt: A Usability Evaluation of PGP 5.0* (http://www.gaudior.net/alma/johnny.pdf) zumindest soweit, dass Sie die nachstehenden Fragen beantworten können[1]. Geben Sie bei jeder Ihrer Antworten die Textstelle (Seite, Spalte, Absatz) an, auf die Sie sich beziehen!
    a. Welche Annahmen/Hypothesen wollen die Autoren des Artikels belegen?
    b. Welche empirischen Verfahren haben die Autoren verwendet, um Ihre Hypothesen zu belegen? Warum wurde dabei PGP 5.0 als „Untersuchungsgegenstand" ausgewählt?
    c. Welche Einsichten und Fähigkeiten sollte (laut den Autoren!) PGP bzw. dessen Benutzeroberfläche einem durchschnittlichen Benutzer vermitteln?
    d. Wie definieren die Autoren ihre Anforderungen an die Benutzbarkeit von „Sicherheitssoftware" (*security software*)?
    e. Welches sind die Hauptschlussfolgerungen die die Autoren aus den Ergebnissen ihrer empirischen Studien ziehen? Wie werden diese Schlussfolgerungen begründet?
    f. Was ist Ihr persönlicher Eindruck von der Studie? Und: Liefert sie Erklärungen, warum PGP von vielen Email-Nutzern nicht verwendet wird?

[1] Dokumentation zu PGP finden Sie z.B. unter http://www.pgpi.org/ oder http://www.pgp.com/de/index.html, Informationen zu OpenPGP/GnuPG z.B. unter http://www.gnupg.org/index.en.html.