Anwendungssysteme – Übung 12

T. Bullmann, N. Lehmann, S. Rolfs, S. Reim, M. Höhne, J. Cwojdzinski

1. Aufgabe: Fälschungssicherheit von E-Mails

1) eMails werden vom Mailserver ohne eine Sicherheitsprüfung an den vom Sender gewünschten Ort versendet. (reine Funktion)

2) Nein. Letztendlich unterliegen Willenserklärungen der Auslegung, ihre Anfechtung ist möglich und sie können widerrufen werden. → Einzelfallprüfung

3) Sie senden dem „Anmelder“ eine eMail mit einem Bestätigungscode zu. Erst wenn dieser Code aktiviert wird, ist die Anmeldung gültig.

4) Durch eine Art digitale (nicht fälschbare) Signatur.

2. Aufgabe: Why Johnny Can’t Encrypt

1) **Was ist PGP?**

- Pretty Good Privacy ist ein von Phil Zimmermann entwickeltes Programm zur Verschlüsselung und zum Unterschreiben von Daten.

Wie funktioniert es?

Man kann mit PGP wahlweise eine Nachricht signieren, verschlüsseln oder signieren und verschlüsseln. Die Signatur dient dazu, die Echtheit der Nachricht zu garantieren. In der Praxis wird man Nachrichten, wenn man sie verschlüsselt, immer auch signieren. Hingegen sind signierte unverschlüsselte Nachrichten nicht sehr verbreitet.

- Erzeugen einer digitalen Signatur
- Verschlüsselung

2) Text (http://www.gaudior.net/alma/johnny.pdf)

a) User-Interface-Design bleibt für eine effektive Sicherheit ein offenes Problem

b) Weil u.a. eine Marketing-Literatur darauf hingewiesen hat, dass PGP 5.0 eine grafische Benutzeroberfläche hat, die komplexe mathematische Kryptographie für Computer-Einsteiger zugänglich macht.

c) Der Benutzer sollte in die Lage versetzt werden eine eMail zu signieren/zertifizieren und zu verschlüsseln

d) Die Autoren definieren ihre Anforderungen in 4 Punkten:

1) Der Benutzer wird zuverlässig sensibilisiert für die Sicherheitsaufgabe.

2) Der Benutzer ist in der Lage herauszufinden, wie er die Aufgabe erfolgreich erfüllen kann.

3) Der Benutzer macht keine Gefährlichen Fehler.

4) Der Benutzer ist „ausreichend“ zufrieden mit dem Interface um es weiterhin zu benutzen.

e) User-Interface-Design bleibt für eine effektive Sicherheit ein offenes Problem.

Keine der 4 Anforderungen wurde von den Benutzern zufriedenstellend erfüllt.

f) Man könnte den Eindruck gewinnen, dass die Studie einen Beleg für die gewünschte These liefern soll.

Es wird keine ernstzunehmende Aussage über einen Grund für das nicht verwenden von PGP 5.0 getroffen.