Ferhat Topcu, Kai Raschke, Sebastian Lehninger, Olliver Wroblewski

Rechnersicherheit SoSe 16

Übung 2

Exercise 2

2.) What did Adobe do wrong?

Adobe hat den Fehler gemacht, dass sie die Zugangsdaten und die Passworthinweise in Klartext eingelagert haben. Zusätzlich, was wohl noch peinlicher bzw. der größere Fehler ist, dass Adobe die Passwörter mittels „3DES“ verschlüsselt hat, anstatt wie üblich mit Hilfe von Hashfunktionen einmalige und nicht zurück verfolgbaren Hashwerte zu generieren. „3DES“ ist eine symmetrisches Verschlüsselungsverfahren, aus dem sich die Klartext-Passwörter vergleichsweise leicht nach einer gewissen Zeit wieder generieren lassen. [0]

Exercise 3

1.) How are Passwords stored?

Passwörter werden mittels der BCrypt Hashfunktion crypt(const char *key, const char* setting) verschlüsselt - key ist das Klartext-Passwort und setting eine Hashingmethode
Der Inhalt von master.passwd ist eine Auflistung aller Nutzer auf dem System mit ihren Metadaten (getrennt durch ":"):

- name (Benutzername)
- password (Hashed Passwort)
- uid (Benutzer ID)
- gid (Group ID)
- class (Klassifikation)
- change (Letzte Passwort Änderung)
- expire (Ablaufdatum)
- gecos (Vollständiger Name)
- home_dir (Home Ordner)
- shell (Benutzer Shell) [1]

2.) Lösungen:

PIN Codes: Carol: 0668 Bob: 4012 Dave: 4415 Alice: 8531

Englisches Wort: Charlie: paleontology

Secret: Rand: correcthorsebatterystaple

Exercise 4

Man kann die announce Mailingliste unter lists.openbsd.org abonnieren oder regelmäßig auf http://openbsd.org/errata.html nach Patches schauen, dies sind jedoch nicht nur Securitypatches. Genau so für Debian: https://www.debian.org/MailingLists/

[0] - http://t3n.de/news/adobe-hack-noch-viel-schlimmer-506598/
[1] - http://man.openbsd.org/OpenBSD-current/man5/passwd.5