Übungen zu Systemsicherheit

Jürgen Kleinöder,
Michael Gernoth, Reinhard Tartler
Universität Erlangen-Nürnberg, Informatik 4

SYSSEC

F.12 Schwächen passwortbasierter Authentifizierung

- Hauptproblem: Der Hashalgorithmus ist zu schnell berechenbar
- Grobe Einteilung
  - Sekunden: LM Hash
  - Stunden/Wochen: NT Hash
  - Monate/Jahre: unix crypt
  - Jahre: MD5Crypt = bsd algorithm1
  - Jahrzehnte: PBKDF2

Reproduktion jeder Art oder Verwendung dieser Unterlage, außer zu Lehrzwecken an der Universität Erlangen-Nürnberg, bedarf der Zustimmung des Autors.

F.13 Aufwandsabschätzungen

- 8 Stellen und 95 Zeichen Alphabet (viele Sonderzeichen)

95 ^ 8 = 6.6 * 10^15

- 8 Stellen und 62 Zeichen Alphabet (gross, klein) und Zahlen):

62 ^ 8 = 2.2* 10^14 (30 mal schlechter)

- 8 Stellen und 26 Zeichen Alphabet (nur kleine Buchstaben):

26 ^ 8 = 2.1 * 10 ^ 11 (31.000 mal schlechter)
26 ^ 7 = 8.0 * 10 ^ 9 (825.000 mal sclechter)
26 ^ 6 = 3.1 * 10 ^ 8 (21.000.000 mal schlechter)
...

- Weitere Einschränkungsmöglichkeiten:
  - Wörterbücher
  - Wortlisten mit Wortfragmenten, Silben, etc,

F.14 Weiterhin zu berücksichtigen

- Die Rechenleistung verdoppelt sich alle eineinhalb Jahre (bzw. die Kosten halbieren sich alle eineinhalb Jahre (Amdahls Law)).
- Geschickte Auswahl des Suchraumes findet Passwörter deutlich früher wenn sie nicht wirklich REIN zufällig sind (Zeichen wie ^{}~‘ werden kaum verwendet).
- Passwörter aus Wörterbüchern und Variationen davon sind ebenfalls deutlich leichter zu finden.

Reproduktion jeder Art oder Verwendung dieser Unterlage, außer zu Lehrzwecken an der Universität Erlangen-Nürnberg, bedarf der Zustimmung des Autors.

F.15 Aufgabe: findpw

- Gesucht ist das Passwort zu folgendem Hash

```
$ ./genpw
Enter Password: FINDME!
$syssec1$iCTRKl6I$IVbdHY6ELEG6dhIjakmFHQ
```

- Nachzulesen in der Datei

```
/proj/i4syssec/aufgabe1b/passwd
```

- Randbedingungen
  - Es wurden nur Grossbuchstaben und Zahlen verwendet
  - Es ist 6 Zeichen lang
  - Bitte die Rate der getesteten Passwörter anzeigen!
- Schnelle Rechner im CIP
  - faui0sr0, faui0sr1
  - faui06* und faui08*

Reproduktion jeder Art oder Verwendung dieser Unterlage, außer zu Lehrzwecken an der Universität Erlangen-Nürnberg, bedarf der Zustimmung des Autors.