

# Übungen zu Systemsicherheit

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

## C.1 Besprechung der Aufgabe 'genpw'

- BIO\_flush() erzeugt ein '\n' auf dem Terminal
  - ◆ Besser mit Puffern arbeiten

**BIO\_s\_mem(3)**

- Weitere Probleme?

## C.2 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

## C.3 Aufwandsabschätzungen

- 8 Stellen und 95 Zeichen Alphabet (viele Sonderzeichen)

$$95^8 = 6.6 \cdot 10^{15}$$

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

$$62^8 = 2.2 \cdot 10^{14} \text{ (30 mal schlechter)}$$

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

|                            |                             |
|----------------------------|-----------------------------|
| $26^8 = 2.1 \cdot 10^{11}$ | (31.000 mal schlechter)     |
| $26^7 = 8.0 \cdot 10^9$    | (825.000 mal schlechter)    |
| $26^6 = 3.1 \cdot 10^8$    | (21.000.000 mal schlechter) |
| ...                        |                             |

- Weiter Einschränkungsmöglichkeiten
  - ◆ Wörterbücher
  - ◆ Wortlisten mit Wortfragmenten, Silben, etc,

## C.4 Weiterhin zu berücksichtigen

- Die Rechenleistung verdoppelt sich alle eineinhalb Jahre (bzw. die Kosten halbieren sich alle eineinhalb Jahre).
- 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.

## C.5 Aufgabe: findpw

- Gesucht ist das Passwort zu folgendem Hash

```
$ ./genpw
Enter Password: FINDME!
$syssec1$U8K0An3Z$HIfthwWSFmtQ4GVTDfcDmQ
```

- 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 probierten Passwörter anzeigen!
- Schnelle Rechner im CIP
  - ◆ faui01
  - ◆ faui05