



# Netzwerksicherheit

## Übung 1

Tobias Limmer / Christoph Sommer

Computer Networks and Communication Systems  
Dept. of Computer Sciences, University of Erlangen-Nuremberg, Germany

05. – 09.11.2007

# Die Übung

- erstmal: Willkommen!
  - falls ihr es noch nicht gemacht habt:  
Bitte auf Website registrieren!

```
http://www7.informatik.uni-erlangen.de/~dressler/lectures/  
netzwerksicherheit-ws0708/
```

- Voraussetzungen
  - gültiger Benutzeraccount auf CIP-Pool-Rechnern der Informatik
  - Grundlagen in C/C++ Programmierung

# Die Übung

- Inhalte der Übung:
  - Wiederholung des Vorlesungsstoffs:  
Wenn ihr Fragen habt, einfach melden!
  - praxisnahe Ergänzungen
- Übungstermine:
  - Dienstag, 14:15 – 15:45 Uhr, 01.153 CIP-Pool
  - Dienstag, 16:15 – 17:45 Uhr, 01.153 CIP-Pool
  - Donnerstag, 16:15 – 17:45 Uhr, 01.153 CIP-Pool

# Hausaufgaben

- Aufgabenstellung
  - fast jede Woche
  - wird immer Dienstags über Mailingliste und in Übungen verteilt
- Bearbeitung
  - in 2er- oder 3er-Gruppen
  - Programmierung in C/C++, notfalls auch in Java (dafür gibts aber dann keinen Beispielcode)
- Abgabe
  - spätestens die darauffolgende Woche am Montag, 23:59 Uhr
  - per Mail an <tobias.limmer@informatik.uni-erlangen.de>
- in den Übungen
  - Besprechung der Hausaufgaben
  - Vorstellung eurer Lösungen

# Prüfungen

- Schein:
  - alle Hausaufgaben (außer einer) müssen erfolgreich abgegeben werden
  - mündliche Prüfung in erster Woche nach Ende der Vorlesungszeit
  - benotet oder unbenotet
- studienbegleitende Prüfung:
  - Abgabe der Hausaufgaben nicht nötig
  - aber nützlich, denn
- Übungen und Hausaufgaben sind Teil des Prüfungsstoffs!

# Themen der Übungen

- Sicherheitsziele, Angriffsbäume
- Enigma
- Betriebsmodi, RSA
- Schlüsselaustausch
- Zertifikate
- IPSec
- Spoofing (MAC, ARP, IP)
- Mix-Netze
- Angriffserkennung

# Einteilung der Übungsgruppen

# Sicherheitsziele

- Fünf (technische) Sicherheitsziele...

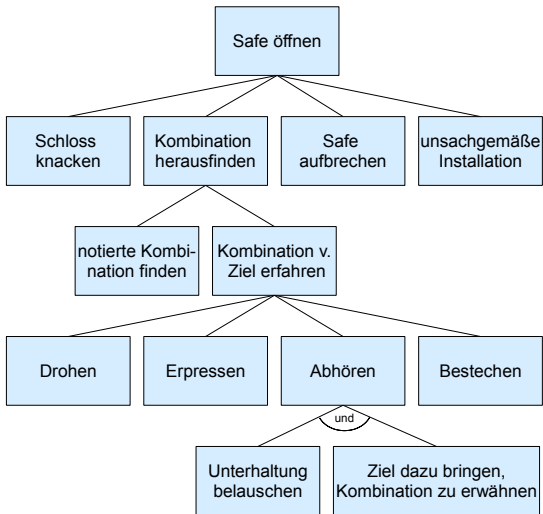
# Sicherheitsziele

- Vertraulichkeit (confidentiality)
- Datenintegrität (data integrity)
- Verbindlichkeit (accountability, non-repudiation)
- Verfügbarkeit (availability)
- kontrollierter Zugriff (controlled access)

# Angriffsbäume

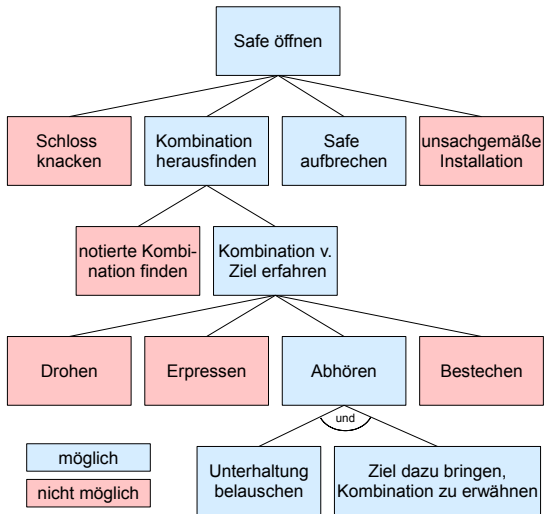
- formale und methodische Modellierung von Bedrohungen für ein (Computer-)System
- Angriffe gegen System werden baumbasiert dargestellt:
  - Wurzel stellt Ziel dar
  - restliche Knoten stellen Wege dar, das Ziel zu erreichen
- gut verwendbar für Sicherheitsanalysen:
  - Sicherheitsabschätzungen (Wie sicher ist mein System?)
  - „Was-wäre-wenn“ Fragestellungen
  - Kostenabschätzungen
  - ...

# Beispiel



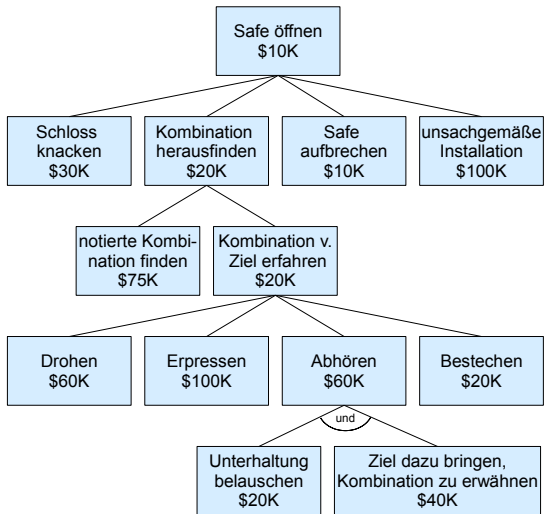
entnommen aus Bruce Schneier, „Attack Trees – Modeling security threats“. Dr. Dobbs Journal, Dezember 1999

# Beispiel – Markierung der unmöglichen Aktionen



entnommen aus Bruce Schneier, „Attack Trees – Modeling security threats“. Dr. Dobbs Journal, Dezember 1999

# Beispiel – Abschätzung der Kosten



entnommen aus Bruce Schneier, „Attack Trees – Modeling security threats“. Dr. Dobbs Journal, Dezember 1999