

# Übungen zu Systemsicherheit

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

## F.1 Besprechung der Aufgabe 'OverlayFS'

- Probleme?

## F.2 Ausnutzen von Anwendungsfehlern

- Anwendungen mit anderen Privilegien werden dazu gebracht, eigenen Code auszuführen
- Je nach Zugriffsmöglichkeit auf die Anwendung (Netzwerk/Lokal) sind unterschiedliche Angriffsmöglichkeiten vorhanden

## F.3 Einige Angriffsmöglichkeiten

- Ungeprüfte Übergabe von Benutzerdaten an kritische Bibliotheksfunktionen (z.B.: `system`, `exec`)
- Falsche Benutzung von Bibliotheksfunktionen (z.B.: `printf` ohne Formatstring, Formatstringattacken)
- Pufferüberläufe mit ersetzen der Rücksprungadresse
- Pufferüberläufe mit Shellcode-Einschleusung auf dem Stack
- Pufferüberläufe mit Shellcode-Einschleusung auf dem Heap

## F.4 Demonstration Pufferüberlauf/Stackaufbau

- Live-Demonstration „Pufferüberlauf“
- Aufbau des X86-Stacks
  - ◆ Siehe auch „`/proj/i4syssec/a5/showstack/showstack2.c`“

## F.5 Finden von ausnutzbaren Anwendungsfehlern

- Quellcode nach Lücken durchsuchen
  - ◆ Manuell
  - ◆ Mit Hilfsprogrammen wie „splint“
  - ◆ Wenn Binary vorliegt, „nm“ für Adressen der Funktionen
- Disassemblierung der Binaries
  - ◆ Debug-Symbole sind hilfreich
- Fuzzing
  - ◆ Zufällige Eingabedaten erzeugen und „Reaktion“ des Programms beobachten

## F.6 Aufgabe 6

- Vorgabe: sbit-Programm `/proj/syssec/bin/abgabe` mit Quellcode in `/proj/syssec/bin/abgabe.c`
- Ziel: Erzeugung der Datei `/proj/i4syssec/a5/exploited/user1_user2`
- Exploit des Programms auf sovielen Wegen wie möglich