



Inst. für Angew. Informationsverarbeitung

Prof. Dr. Franz Schweiggert

Michaela Weiss  
Wolfgang Kaifler

08.02.2011

Lösung 13

# Systemnahe Software I (WS 2010/2011)

**Ausgabetermin: 08.02.2011**

## 1 Fragen:

**Nennen und erklären Sie einige Neuerungen, die mit dem Standard C-99 eingeführt wurden!**

- In FOR-Schleifen können nun Initialisierungen vorgenommen werden, ohne diese vorher explizit zu definieren.
- Es wurde ein neuer Datentyp 'Bool' eingeführt.
- Das Schlüsselwort *inline* wurde eingeführt, um die Funktions- Implementierung an der Stelle des Aufrufes einzusetzen.

**Welche Bedeutung und welche Auswirkungen hat das sogenannte setuid-Bit bei einem ausführbaren Programm?**

- Wenn ein solches Programm ausgeführt wird ist es mit den Rechten des Users ausgestattet, dem das ausführbare Programm gehört.

**Was führt beim Umgang mit Strings unter C häufig zu Sicherheitslücken? Was kann dagegen unternommen werden?**

- Eine der größten Sicherheitslücken in C in Verbindung mit Strings ist die fehlende Überprüfung der Länge. Sogenannte Overruns sind oft schwer, teilweise nur zur Laufzeit zu finden.
- Abhilfe dagegen schafft die Verwendung alternativer Bibliotheken, beispielsweise der *stralloc*-Bibliothek.

**Beim Lesen aus Dateien wird oft auf das Dateiende abgeprüft. Woher weiß Unix wann eine Datei zu Ende ist?**

- Unix kennt die Größe jeder Datei, welche in der Inode steht.
- Beim Lesen dieser Datei verwaltet Unix einen Offsetpointer, an welcher Position innerhalb der Datei sich der Leesezeiger befindet.
- Ist die Differenz zwischen Dateigröße und Offset-Pointer null, so kann Unix nichts mehr aus dieser Datei lesen, und gibt dies an die entsprechenden System-Calls zurück.