ulm university universität
uulm

Inst. für Angew. Informationsverarbeitung
Prof. Dr. Franz Schweiggert
Michaela Weiss
Wolfgang Kaifler

01.02.2011
Blatt 13

Systemnahe Software I (WS 2010/2011)

Abgabetermin: 08.02.2011

Organisatorisches:

- Bitte melden Sie sich im Hochschulprotal zur Klausur an.

1 Fragen (4 Punkte)

- Nennen- und Erklären Sie einige Neuerungen, die mit dem Standart C-99 eingeführt wurden!
- Welche Bedeutung und welche Auswirkungen hat das sogenannte **setuid-Bit** bei einem ausführbaren Programm?
- Was führt beim Umgang mit Strings unter C häufig zu Sicherheitslücken? Was kann dagegen unternommen werden?
- Beim Lesen aus Dateien wird oft auf das Dateiende abgeprüft. Woher weiß Unix, wann eine Datei zu Ende ist?

2 Geheime Nachricht (15 Punkte)

Verschlüsselung ist ein Vorgang, bei dem ein klar lesbarer Text mit einem Verschlüsselungsverfahren in einen „Geheimtext“ umgewandelt wird.

Eine Art des Verschlüsselns ist das Scrambling-Verfahren, bei dem die Buchstaben „durcheinandergeworfen“ werden. Erst der Bustabe und die zugehörige Position machen den Text wieder lesbar.

Der codierte Text ist in Segmente unterteilt. Ein Segment besteht dabei aus zwei Komponenten: einem Integer, der relativ von der aktuellen Position auf das nächste Segment zeigt, und einem Zeichen. Beides wird nacheinander in einer Datei abgelegt.

Beispiel:
Der Text 'HALLO' könnte folgenderweise codiert sein:(**ohne Leerzeichen und Trennzeichen**)

| 4 # | 65000 # | -1 # | 65000 # | 3 H | 3 L | -4 O | -2 A | -2 L |

Das erste Segment beginnt mit einer (Integer) '4'. Wir springen also von der aktuellen Position aus vier Segmente weiter → 'H'. Diesen Buchstaben geben wir aus. Als nächste Positionsangabe in diesem Segment steht eine (Integer) 3. Also springen wir weitere drei Segmente nach hinten und geben das (Character) 'A' aus. Es folgt als Position eine (Integer) -2. In diesem Fall springen wir zwei Segmente nach vorne, usw. Das Textende wird durch das Zeichen '#' markiert.
Verwenden Sie zum Lesen ausschließlich System-Calls.

Da die Verschlüsselung aufgrund der Byte-Order architekturabhängig ist finden sie auf der Homepage zwei Dateien: *encrypted_sparc.txt* bzw. *encrypted_intel.txt*. Verwenden Sie die zu Ihrer Architektur passende Datei. Speichern Sie den entschlüsselten Text nun in der Datei *decrypted.txt* (Ohne Dateiumlenkung!).

Viel Erfolg beim Entschlüsseln!

Viel Erfolg!