Information About This Course

Andreas Zeller/Stephan Neuhaus
Lehrstuhl für Softwaretechnik
Universität des Saarlandes, Saarbrücken

SS 2004/CVS Revision: 1.6

What Is This Course?

- Spezialvorlesung, 6 LP
- C.S. Master Students, Dipl.-Inform. Hauptstudium
- English

Important Dates

This lecture takes place on Thursdays, 1100–1300 c.t. in Bldg. 45, Lecture Hall 2.

The exercises take place on Wednesdays, 0900–1100 c.t. in 36/306.

Exercises are due on the Tuesday following the lecture, at 0900 s.t. in my office in 45/302.

Prerequisites

- Reasonably fluent in C (C++ is also OK)
- Basic cryptography ("plaintext", "ciphertext", "key", "encryption", "decryption", "hash function").
- Basic Operating Systems (threads, processes, file systems, race conditions, networking); Unix a plus.
- Basic mathematics: some sums, some integrals, some modulo operations, some vector operations, nothing really fancy.

How to Pass this Course

- Get at least 50% of the exercise points;
- demonstrate a solution to an exercise at least three times;
- pass the final exam at the end of the semester.

Collaboration on the exercises is allowed for teams of two (not more). However, you must *individually* demonstrate the solutions.

Depending on how many of you are left by the end of the semester, there might be oral exams (if there are just a few) or a written exam (if there are many).

First exercise is not graded!

Final Exam

- Closed-book exam
- No reference sheet allowed
- Reference solution and grades published some days after the exam
- Ungraded (only pass/fail)

Check Frequently!

Slides and exercises are available through the Web page at http://www.st.cs.uni-sb.de/edu/secdesign/

Slides available as PDF (for presentation) and postscript (for studying).

Here is some good advice, given away for free:

Recheck the lecture's web site frequently for updates. Material on this web page is prone to changes.

Again, the address is

http://www.st.cs.uni-sb.de/edu/secdesign.