Netzwerksicherheit [NetSec]

Dr.-Ing. Falko Dressler

Computer Networks and Communication Systems
Department of Computer Sciences
University of Erlangen-Nürnberg

http://www7.informatik.uni-erlangen.de/~dressler/
dressler@informatik.uni-erlangen.de
Course Overview

- **Network Security**
  Threats and security goals, basic mechanisms

- **Cryptography**
  Basics, symmetric cryptography, asymmetric cryptography

- **Cryptographic Techniques**
  Modification check values, random number generation, cryptographic protocols

- **Protocols for Network Security**
  Access control, integrating security services into communication architectures, security protocols at the link layer, IPSec architecture, security protocols at the transport layer

- **Applications**
  Firewalls, security aspects of mobile communications (WLAN, GSM/UMTS, Mobile IP)

- **Attack Detection and Countermeasures**
  Intrusion detection and prevention, countermeasures, IP traceback
Course Overview

- **Material**
  - …

- **News, updates, handouts, …**
  
  [Link](http://www7.informatik.uni-erlangen.de/~dressler/lectures/netzwerksicherheit-ws0506/)

- **Persons**
  - Dr.-Ing. Falko Dressler (lecture)
  - Jochen Kaiser (exercises)
Exercises

- Organization
  - Consolidation of course topics
  - Working groups of 2-3 students
  - Mix of theoretic and practical exercises

- Overview
  - Lab training
  - Network monitoring and analysis
  - Cryptographic algorithms
  - Security analysis
  - VPN, Firewalls (Linux, Cisco)
  - WLAN security (how to access secured WLANs)
  - Attack and intrusion detection
Course Organization

- Lecture
  - additional dates

- Exercises (3-4 groups)
  - Tuesday, 8:00-10:00, RZ 01.153 CIP-Pool
  - Tuesday, 10:00-12:00, RZ 01.153 CIP-Pool

- ... see web page for more up-to-date information
Course Organization

- **Examination**
  - Computer science: in combination with “Kommunikationssysteme”
  - Computational engineering: oral examination
  - Exercises are relevant!

- **“Schein”**
  - Oral examination at the end of the semester
  - “benoteter Schein”: successful processing of ALL exercises, the grade results form the oral examination
  - “unbenoteter Schein”: successful processing of ALL exercises, at least 50% must be achieved in the oral examination
Curses at Dept. of Computer Science 7

- Kommunikationssysteme +
  - Pervasive Computing,
  - Protokolle der
  - Hochgeschwindigkeits- und
  - Mobilkommunikation,
  - Netzwerksicherheit
    (systemorientiert)

- Dienstgüte von
  Kommunikationssystemen,
  Netzwerksicherheit
  Selbstorganisation in Autonomen Sensor-/Aktornetzen,
  Simulation and Modeling I
  (methodisch)

- Simulation and Modeling I+II
<table>
<thead>
<tr>
<th>Reference Code</th>
<th>Author(s)</th>
<th>Title and Edition Information</th>
</tr>
</thead>
</table>