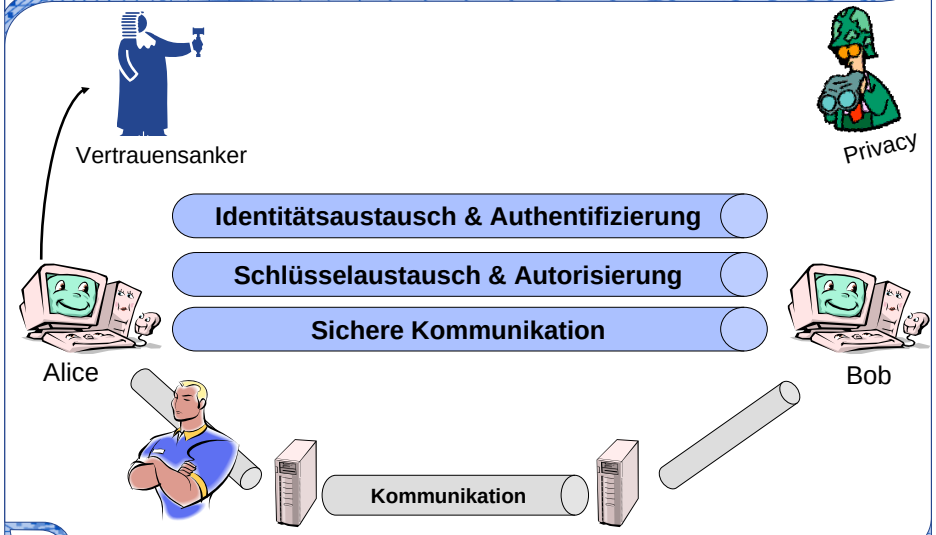
Die Vorlesung im Überblick

TeleMatics

Netzsicherheit:
Architekturen und Protokolle

Die Vorlesung im Überblick

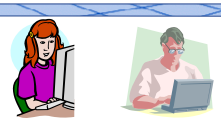


Ablauf der Vorlesung

14.04.10	Einführung
21.04.10	*Krypto-Grundlagen 15:45, -102*
21.04.10	Kerberos, Teil 1
28.04.10	Kerberos, Teil 2
05.05.10	Grundlagen PKI/PMI Vertrauensmodelle
12.05.10	X.509/PKIX
19.05.10	PMI
26.05.10	PGP/SPAM
02.06.10	DNSsec
09.06.10	Grundlagen Schlüsselaustausch IKE
16.06.10	Grundlagen sicherer Datentransport IPsec
23.06.10	TLS
30.06.10	Infrastrukturschutz 1
07.07.10	Infrastrukturschutz 2
14.07.10	Routing-Sicherheit

Kryptogrundlagen

- Darf ich vorstellen, Alice und Bob



- Einführung in die Grundlagen der Kryptographie
  - Mittwoch, 21.04., 15:45, -102
  - Freiwillig!
- Was kann man erwarten?
  - nur die notwendigsten Konzepte
    - z.B. Verschlüsselung, Hash, Signatur, …
  - keine Details zu Algorithmen
  - keine Mathematik/Algebra

Zusatztermin: Kryptogrundlagen
Montag 21.04. 15:45, -102

Für das Verständnis der Vorlesung sehr gut!
Wissen wird in Prüfung vorausgesetzt!

Organisatorisches

- Vorlesungsunterlagen
  - http://www.tm.kit.edu/itm
  - Vorlesungsfolien
    - mit Anmerkungen
    - Platz für eigene Notizen
  - Abkürzungsliste
  - Weitere Materialien

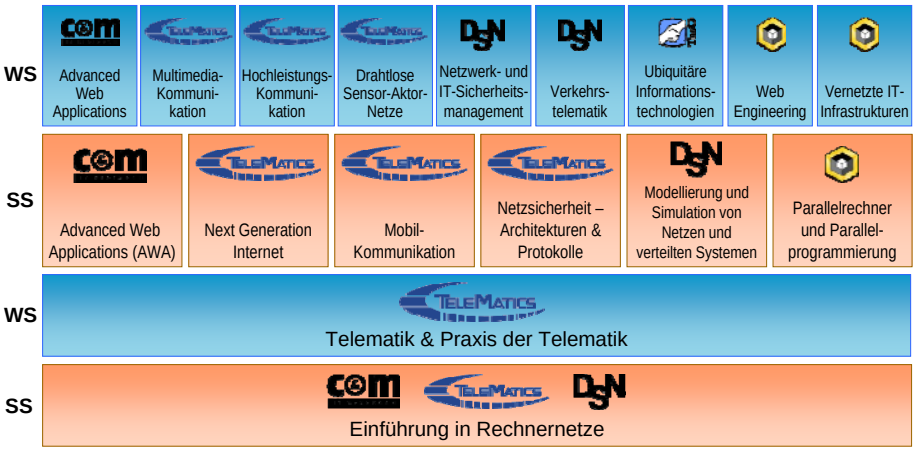
Verwenden Sie zur Prüfungsvorbereitung bitte unbedingt die Folien mit Anmerkungen!!!

Fragen, Wünsche, Anregungen?
Mail an marcus.schoeller@neclab.eu

Organisatorisches

- **Überblick über das Institut für Telematik**
  - **Professoren**
    - Prof. Dr. Martina Zitterbart (seit 2001)
    - Prof. Dr. Sebastian Abeck (seit 1996)
    - Prof. Dr. Wilfried Juling (seit 1998)
    - Prof. Dr. Hannes Hartenstein (seit 2003)
    - Prof. Dr. Michael Beigl (seit 2010)
    - em. Prof. Dr. Gerhard Krüger (seit 1971)
  - **Mitarbeiter**
    - Ca. 45 wissenschaftliche Mitarbeiter
    - Technische Mitarbeiter
    - Sekretärinnen/Verwaltungsangestellte
  - **Studierende**
    - Ca. 35 Hiwis
    - Über 2000 mündliche Prüfungen
    - Über 40 Diplomarbeiten pro Jahr

Überblick: Lehrveranstaltungen

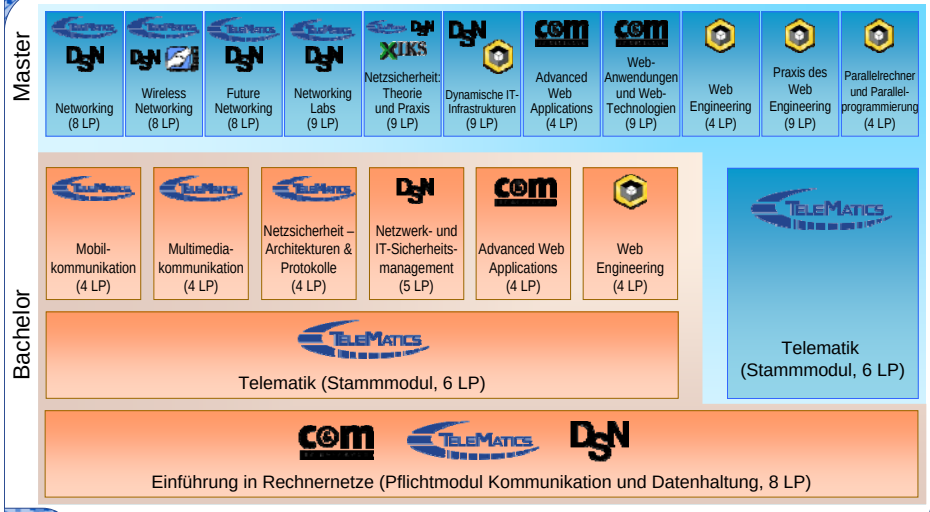


Angaben ohne Gewähr. Es gelten die Regelungen des jeweils gültigen Modulhandbuchs und der Prüfungsordnung.

Prüfungsregelung Studiengang Informatik (Diplom)

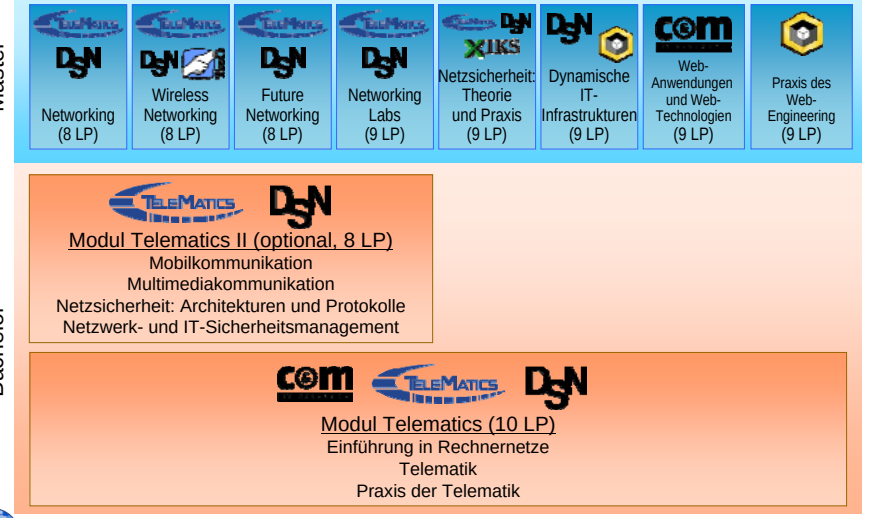
- **Kombinierbare Vorlesungen (Prof. Dr. Martina Zitterbart)**
  - Telematik (verpflichtend)
  - Hochleistungskommunikation
  - Mobilkommunikation
  - Multimediakommunikation
  - Netzsicherheit - Architekturen und Protokolle
  - Next Generation Internet
  - Drahtlose Sensor-Aktor-Netze
  - Ubiquitäre Informationstechnologien
  - Praktikum aus der Telematik
- Der Stoff des Kommunikationsteils der Vorlesung „Kommunikation und Datenhaltung“ bzw. der Vorlesung „Einführung in Rechnernetze“ wird vorausgesetzt (nicht die Klausur!)

Überblick: Module Bachelor/Master Informatik



Angaben ohne Gewähr. Es gelten die Regelungen des jeweils gültigen Modulhandbuchs und der Prüfungsordnung.

Überblick: Module Bachelor / Master Informationswirtschaft



Angaben ohne Gewähr. Es gelten die Regelungen des jeweils gültigen Modulhandbuchs und der Prüfungsordnung.

Modulzusammensetzung Master

Networking (8 LP)
Telematik
Hochleistungskommunikation
Next Generation Internet
Multimediakommunikation
Modellierung und Simulation von Netzen und verteilten Systemen
Netzsicherheit: Architekturen & Protokolle

Wireless Networking (8 LP)
Telematik
Mobilkommunikation
Drahtlose Sensor-Aktor-Netze
Verkehrstelematik (Traffic Telematics)
Ubiquitäre Informationstechnologien
Modellierung und Simulation von Netzen und verteilten Systemen
Netzsicherheit: Architekturen & Protokolle

Networking Labs (9 LP)
Next Generation Internet + Praktikum
Drahtlose Sensor-Aktor-Netze + Praktikum
Modellierung und Simulation von Netzen und verteilten Systemen + Praktikum
Netzsicherheit: Architekturen & Protokolle + Netzwerk- und IT-Sicherheitsmanagement
Mobilkommunikation + Praktikum

Future Networking (8 LP)
Telematik
Next Generation Internet
Multimediakommunikation
Mobilkommunikation
Drahtlose Sensor-Aktor-Netze
Verkehrstelematik (Traffic Telematics)

Netzsicherheit: Theorie und Praxis (9 LP)
Netzsicherheit: Architekturen & Protokolle
Netzwerk- und IT-Sicherheitsmanagment
Public Key Kryptographie
Symmetrische Verschlüsselungsverfahren
Seminar aus der Kryptographie

Dynamische IT-Infrastrukturen (9 LP)
Web Engineering
Modellierung und Simulation von Netzen und verteilten Systemen + Praktikum
Ubiquitäre Informationstechnologien
Vernetze IT-Infrastrukturen
Netzwerk- und IT-Sicherheitsmanagement

Web-Anwendungen und Web-Technologien (9 LP)
Advanced Web Applications
Praktikum Web-Technologien

Praxis des Web Engineering (9 LP)
Web Engineering
Praktikum Web Engineering

Atomare Module (je 4 LP)
Advanced Web Applications
Web Engineering
Parallelrechner- und Parallelprogrammierung

Stammmodul Telematik (6 LP)
Telematik
Praxis der Telematik

Angaben ohne Gewähr. Es gelten die Regelungen des jeweils gültigen Modulhandbuchs und der Prüfungsordnung.

Modulzusammensetzung

Lehrveranstaltungen \ Module	Bachelor Pflichtmodul	Bachelor atomares Modul	Bachelor/Master Stammmodul Telematik	Master (atomares Modul)	Networking	Wireless Networking	Future Networking	Networking Labs	Netzsicherheit: Theorie und Praxis	Dynamische IT-Infrastrukturen	Web-Anwendungen & Web-Technologien	Praxis des Web Engineering
Einführung in Rechnernetze	X											
Telematik			X		X	X	X					
Praxis der Telematik			X									
Mobilkommunikation		X				X	X	X				
Multimediakommunikation		X			X		X					
Netzsicherheit: Architekturen und Protokolle		X			X	X		X	X			
Drahtlose Sensor-Aktor-Netze						X	X	X				
Hochleistungskommunikation					X							
Next Generation Internet					X		X	X				
Praktikum Future Internet (PrakATM)								X				
Projektpraktikum Sensornetze (PrakATM)								X				
Praktikum Modellierung und Simulation von…								X		X		
Modellierung und Simulation von Netzen und…					X	X		X		X		
Verkehrstelematik (Traffic Telematics)						X	X					
Netzwerk- und IT-Sicherheitsmanagement		X						X	X	X		
Ubiquitäre Informationstechnologien						X				X		
Vernetzte IT-Infrastrukturen										X		
Parallelrechner und Parallelprogrammierung				X								
Web Engineering		X		X						X		X
Praktikum Web Engieering												X
Advanced Web Applications		X		X							X	
Praktikum Web-Technologien											X	

Angaben ohne Gewähr. Es gelten die Regelungen des jeweils gültigen Modulhandbuchs und der Prüfungsordnung.

Prüfungsregelung Nebenfach

- Wirtschafts-Ingenieure (Diplomstudiengang) und andere müssen sowohl die Telematik-Vorlesung (2 SWS) als auch den Kommunikationsteil der Vorlesung „Kommunikation und Datenhaltung“ bzw. der Vorlesung „Einführung in Rechnernetze“ (2 SWS) in ihren Prüfungskatalog aufnehmen.
- Für die meisten Bachelor/Master-Studiengänge stehen die Nebenfachregelungen noch nicht endgültig fest. Bitte bei der jeweiligen Fakultät informieren.

Prüfungstermine

- Prüfungstermine werden jeweils einmal monatlich vergeben.
  - Gilt für Informatiker, Informationswirte, Elektrotechniker und Wirtschaftsingenieure
  - Konkrete Termine können im Sekretariat erfragt werden
  - Sollten v.a. in der Prüfungszeit keine freien Termine mehr vorhanden sein, werden nach Bedarf Zusatztermine angeboten
- **Anmeldung zu Prüfungen**
  - Im Sekretariat von Prof. Zitterbart bei Frau Wagner, Informatikgebäude am Schloss (Geb. 20.20), Raum 360, Tel.: 608-6411, Email: telematik@tm.uka.de
  - Für die Prüfungen bitte die jeweils für Ihren Studiengang gültigen Prüfungsregelungen beachten

Organisatorisches

- **Öffnungszeiten des Sekretariats**
  - Montag – Donnerstag von 11:30 Uhr bis 15:30 Uhr
  - Freitag von 11:30 Uhr bis 14:30 Uhr
- **Anmeldungen zu Praktika / Seminaren**
  - Per Web unter www.tm.kit.edu
  - … oder bei Fragen und Problemen
    - im Sekretariat von Prof. Zitterbart bei Frau Wagner oder
    - per E-Mail/Telefon an Frau Wagner

Seminare des Institutsteils Prof. Dr. Zitterbart

- Veranstaltungsort
  - Seminarraum 367 (SR 367), Informatikgebäude am Schloss (Geb. 20.20)
  - Genauere Hinweise jeweils im Web erhältlich sowie bei den Betreuern
- Seminare im Sommersemester
  - Future Internet
    - Neue Konzepte: inkrementelle Verbesserungen und ‚Clean Slate‘-Ansätze
    - Betreuer: S. Mies, O. Waldhorst
  - Sensornetze
    - Architekturen, Protokolle, Sicherheit
    - Betreuer: D. Dudek, Ch. Haas
  - Mitarbeiter- und Diplomandenseminar
    - Vorträge über Studien- und Diplomarbeiten sowie über aktuelle Arbeiten
    - Betreuer: T. Gamer
- Arbeitsgemeinschaften im Sommersemester
  - P2P / Overlay-Netze
  - Sensornetze
  - Service Composition
  - Sicherheit

Seminare des Institutsteils Prof. Dr. Zitterbart

- Veranstaltungsort
  - Seminarraum 367 (SR 367), Informatikgebäude am Schloss (Geb. 20.20)
  - Genauere Hinweise jeweils im Web erhältlich sowie bei den Betreuern
- Seminare im Wintersemester
  - Future Internet
    - Neue Konzepte: inkrementelle Verbesserungen und ‚Clean Slate'-Ansätze
    - Betreuer: S. Mies, R. Bless
  - Technologien des Internets (Proseminar)
    - Überblick über Schlüsseltechnologien des Internets sowie Grundlagen des wissenschaftlichen Schreibens und Vortragens
    - Betreuer: H. Wippel
  - Mitarbeiter- und Diplomandenseminar
    - Vorträge von Studien- und Diplomarbeiten sowie über aktuelle Arbeiten
    - Betreuer: T. Gamer
- Arbeitsgemeinschaften im Wintersemester
  - P2P / Overlay-Netze
  - Sensornetze
  - Service Composition
  - Sicherheit

Praktika des Institutsteils Prof. Dr. Zitterbart

- Projektpraktika im Bachelor
  - **Praxis der Softwareentwicklung 20**
    - Inhalte bisher:
      - WS 2009/2010: Visualisierung komplexer Kommunikationsvorgänge für Lehrveranstaltungen
    - Betreuer: D. Dudek, J. Furthmüller, Ch. Haas
  - **Praxis der Softwareentwicklung 21**
    - Inhalte bisher:
      - SS 2010: Weiterentwicklung des „Gluck" Online-Systems zur Getränke-Verwaltung und Abrechnung
    - Betreuer: H. Backhaus, H. Wippel
  - Jeweils im Wintersemester und Sommersemester
  - Aktuelle Themen unter http://www.tm.uka.de/

Praktika des Institutsteils Prof. Dr. Zitterbart

- Projektpraktika im Master (bzw. Hauptdiplom)
  - **Sensornetze** (im Sommersemester)
    - Aufgaben zu folgenden Themen
      - Das Praktikum befasst sich mit Problemen, welche bei der realen Umsetzung von Sensornetzen auftreten
      - Eigenständige Planung, Implementierung und Evaluierung einer Sensornetz-Anwendung
      - Untersuchung der Anwendung auf Energieeffizienz
    - Organisatorisches
      - Betreuer: Ch. Haas, A. Hergenröder, J. Horneber
  - **Technologien des Future Internets**
    - Aufgaben zu folgenden Themen
      - Das Praktikum orientiert sich an aktuellen Forschungsfragen in laufenden Projekten
      - Projekt SpoVNet
      - Projekt G-Lab
    - Organisatorisches
      - Betreuer: H. Backhaus, Ch. Hübsch, D. Martin, Ch. Mayer, S. Mies, M. Röhricht, Ch. Werle, H. Wippel

Praktika des Institutsteils Prof. Dr. Zitterbart

- Praktika im Master (bzw. Hauptdiplom)
  - **Mobilkommunikation** (im Wintersemester)
    - Aufgaben zu folgenden Themen
      - Themen: WLAN, Bluetooth, Mobile-IP, Ad-Hoc-Netze
      - Die entsprechenden Themenfelder der Vorlesung Mobilkommunikation werden vertieft.
      - Programmiersprachen: C und C++
    - Organisatorisches
      - Betreuer: I. Baumgart, B. Heep, A. Kuntz

Organisatorisches zur Netzsicherheit

- Vorlesung Netzsicherheit ist in folgenden Modulen prüfbar:
  - Bachelor Informatik: Netzsicherheit: Architekturen und Protokolle [IN3INNAP]
  - Bachelor Informationswirtschaft: Telematics II [IW3INTM2]
  - Master Informatik/Informationswirtschaft:
    - Networking [IN4INNW]
    - Wireless Networking [IN4INWN]
    - Networking Labs [IN4INNL]
    - Netzsicherheit - Theorie und Praxis [IN4INNTP]
  - Bachelor Informationswirtschaft (SPO 2005): Infrastruktur [IW3INNET0]
  - Master Informationswirtschaft (SPO 2006): Advanced Infrastructures [IW4INNET]
- Es gelten die Regelungen des jeweils aktuellen Modulhandbuchs

Weiteres

- Internet-Standards
  - Die Standard-Dokumente zu den Internet-Protokollen sind online frei zugänglich (http://www.ietf.org).
    - RFC-Suche (http://rfc-editor.org/rfcsearch.html)
- Allgemeines zum Internet
  - Informationen über das Internet finden Sie auch unter der folgenden Web-Adresse: http://info.isoc.org/internet/
- Artikel in Fachzeitschriften über
  - IEEE Bib (http://ieeexplore.ieee.org)
  - ACM BIB (http://portal.acm.org)
  - Frei zugänglich aus dem Universitätsnetz

Forschungsgruppe Prof. Dr. Zitterbart

Mitarbeiter

5 Technik, Sekretariat

~20 Doktoranden

3 Post-Doktoranden

Ca. 75% Drittmittel

Studierende

Über 140 mündliche Prüfungen in Telematik im letzten Jahr

Selber aktiv werden?

- Falls Sie über die Lehrveranstaltungen hinaus Interesse haben, sich mit dem Fachgebiet vertraut zu machen, wie wäre es denn als
  - Hiwi
  - Bachelor-/Studienarbeiter
  - Master-/Diplomarbeiter
  - ... oder als aktiver Teilnehmer an einer/mehreren der Arbeitsgemeinschaften?

- Sowohl die Mitarbeiter als auch ich selbst stehen Ihnen hierzu gerne als Ansprechpartner zur Verfügung.
- Schauen Sie doch einfach mal am Institut vorbei!
  - Informatikgebäude am Schloss (Geb. 20.20), 3. Stock

Relevante Fachgruppen

- Gesellschaft für Informatik
  - www.gi-ev.de
  - Relevante Fachgruppe: KuVS (Kommunikation und Verteilte Systeme): www.kuvs.de
- IEEE (Institute of Electrical and Electronics Engineers)
  - www.ieee.org
  - Relevante Society: Communications Society (www.comsoc.org)
    - Spezielle Studentenpreise
- ACM (Association for Computing Machinery)
  - www.acm.org
  - Relevante Fachgruppe („Special Interest Group“, SIG): SIGCOMM