**Fachbereich Informatik**

Fachhochschule Gelsenkirchen

# MODULHANDBUCH

Master-Studiengang

## Internet-Sicherheit

7. Juni 2010

# Inhaltsverzeichnis



# Hinweis zum Verständnis der Modulbeschreibungen

Im Anhang B0 des Modulhandbuchs wird eine allgemeine Erläuterung der Bedeutung der einzelnen Felder der Modulbeschreibungen und ihrer Zusammenhänge gegeben. Insbesondere ist dort jeweils auch die Bedeutung für den Eintrag „Standard" in einem Feld der Modulbeschreibung beschrieben.

# Studienplan

<table>
<tr><td>Semester</td><td colspan="30"></td></tr>
<tr><td>4</td><td colspan="28">Master-Arbeit</td><td colspan="2">Master-Kollo-quium</td></tr>
<tr><td>3</td><td colspan="6">Wissensch. Vertief.</td><td colspan="6">Internet-Sicherheit</td><td colspan="6">Master-Seminar Internet-Sicherheit</td><td colspan="6">Ausgewählte Themen aus dem Bereich Internet und Sicherheit</td><td colspan="6">Wahlpflicht-modul 2</td></tr>
<tr><td>2</td><td colspan="6">Master-Projekt Internet-Sicherheit</td><td colspan="6">Weiterführende Konzepte z. Betrieb komplexer verteilter Systeme</td><td colspan="6">Internet-Sicherheit B</td><td colspan="6">Wahlpflicht-modul 1</td></tr>
<tr><td>1</td><td colspan="6">Intelligente Systeme</td><td colspan="6">Programmier-methodik und Sicherheit</td><td colspan="6">Datenschutz und Ethik</td><td colspan="6">Internet-Sicherheit A</td><td colspan="6">Höhere Stochastik</td></tr>
<tr><td>ECTS</td><td>1</td><td>2</td><td>3</td><td>4</td><td>5</td><td>6</td><td>7</td><td>8</td><td>9</td><td>10</td><td>11</td><td>12</td><td>13</td><td>14</td><td>15</td><td>16</td><td>17</td><td>18</td><td>19</td><td>20</td><td>21</td><td>22</td><td>23</td><td>24</td><td>25</td><td>26</td><td>27</td><td>28</td><td>29</td><td>30</td></tr>
</table>

Abbildung 1: Verlaufsplan des Masterstudiengangs Internet-Sicherheit

| Kategorie | Vorgabe in ECTS laut ASIIN-FEH | IS |
|---|---|---|
| Informatik | 60-70 | 66 |
| Fachübergreifende Vertiefungen | 8-16 | 12 |
| Soft Skills (überfachliche Schlüsselkompetenzen) | 6-12 | 12 |
| Master-Arbeit inkl. Kolloquium | 30 | 30 |

# Ausgewählte Themen aus dem Bereich Internet und Sicherheit

| | |
|---|---|
| *Kürzel:* | ATIS |
| *Untertitel:* | Aktuelle Themen im Bereich Internet und Sicherheit |
| *Studiensemester:* | 3. (oder 2.) |
| *Modulverantwortliche(r):* | Studiengangsbeauftragte/r Internet-Sicherheit |
| *Dozent(in):* | Lehrbeauftragte/r |
| *Sprache:* | Deutsch |

*Zuordnung zum Curriculum:*

| I/PI | I/TI | I/ISE | MI | WI | IS |
|---|---|---|---|---|---|
| WP | WP | - | WP | WP | 3 |

| | |
|---|---|
| *Lehrform / SWS:* | 2 SWS Vorlesung, 1 SWS Übung, 1 SWS Praktikum |
| *Gruppengröße:* | Standard |
| *Arbeitsaufwand:* | Standard |
| *Leistungspunkte:* | 6 |
| *Turnus:* | Wintersemester, jährlich |
| *Teilnehmerzahl:* | Standard |
| *Anmeldungsmodalitäten:* | Siehe Aushang |
| *Voraussetzungen nach Prüfungsordnung:* | Keine besonderen |
| *Empfohlene Voraussetzungen:* | --- |
| *Angestrebte Lernergebnisse:* | ○ Gutes Verständnis von möglichen Angriffen und geeigneten Gegenmaßnahmen im Bereich der ausgewählten Themen<br>○ Erlangen der Kenntnisse über den Aufbau, die Prinzipien, die Architektur und die Funktionsweise der ausgewählten Themen im Bereich Internet und Sicherheit<br>○ Gewinnen von praktischen Erfahrungen über die Nutzung und die Wirkung der ausgewählten Themen |
| *Inhalt:* | Ausgewählte Themen aus dem Bereich Internet und Sicherheit (z.B. E-Commerce, Bezahlsysteme im Internet, Internet-Infrastruktur, …) |
| *Studien- / Prüfungsleistungen:* | Studienleistungen: Erfolgreich absolviertes Praktikum als Vorleistung und Voraussetzung zur Prüfungszulassung<br>Prüfungsleistungen: Klausur (90 Min.) |
| *Medienformen:* | Beamer |
| *Literatur:* | Nach Bekanntgabe in der Vorlesung<br>Ausgewählte Themen werden an Hand von aktueller Primärliteratur behandelt. |

| | |
|---|---|
| *Bemerkungen:* | --- |

# Datenschutz und Ethik

| | |
|---|---|
| *Kürzel:* | DSE |
| *Untertitel:* | --- |
| *Studiensemester:* | 1. |
| *Modulverantwortliche(r):* | Studiengangsbeauftragte/r Internet-Sicherheit |
| *Dozent(in):* | NN (Lehrbeauftagte/r) |
| *Sprache:* | Deutsch |

| *Zuordnung zum Curriculum:* | I/PI | I/TI | I/ISE | MI | WI | IS |
|---|---|---|---|---|---|---|
| | - | - | - | - | - | 1 |

| | |
|---|---|
| *Lehrform / SWS:* | 2 SWS Seminar |
| *Gruppengröße:* | Standard |
| *Arbeitsaufwand:* | Standard |
| *Leistungspunkte:* | 6 |
| *Turnus:* | Wintersemester, regelmäßig |
| *Teilnehmerzahl:* | Standard |
| *Anmeldungsmodalitäten:* | Siehe Aushang |
| *Voraussetzungen nach Prüfungsordnung:* | Keine besonderen |
| *Empfohlene Voraussetzungen:* | --- |

*Angestrebte Lernergebnisse:*

- Die Studierenden besitzen grundlegende Kenntnisse über Datenschutz und Ethik.
- Sie haben ein gutes Verständnis über die fundamentalen Gesetzte, Verordnungen und Strategien im Datenschutz.
- Sie erlernen den Sinn und Zweck einer Ethik in der vernetzten Informations- und Wissensgesellschaft.

*Inhalt:*

- Einführung in Datenschutz und Ethik.
- Begriffsbestimmungen: personenbezogene Daten, Datenregister, …
- Informationelle Selbstbestimmung, Bundesdatenschutzgesetz, Teledienstedatenschutz, Telekommunikationsgesetz, …
- Rechte der Betroffenen.
- Organisatorische und technische Maßnahmen zum Schutz personenbezogene Daten .
- Ethik in der vernetzten Informations- und Wissensgesellschaft.

| | |
|---|---|
| *Studien- / Prüfungsleistungen:* | Prüfungsleistungen: Klausur (90 Min.) |
| *Medienformen:* | Beamer |

| | |
|---|---|
| *Literatur:* | Nach Bekanntgabe in der Vorlesung<br>Themen werden an Hand von aktueller Primärliteratur behandelt. |
| *Bemerkungen:* | --- |

# Höhere Stochastik

| | |
|---|---|
| *Kürzel:* | HST |
| *Untertitel:* | --- |
| *Studiensemester:* | 1. |
| *Modulverantwortliche(r):* | Prof. Dr. Wolfgang Engels |
| *Dozent(in):* | Prof. Dr. Wolfgang Engels |
| *Sprache:* | Deutsch |

*Zuordnung zum Curriculum:*

| I/PI | I/TI | I/ISE | MI | WI | IS |
|---|---|---|---|---|---|
| WP | WP | - | WP | 1 | 1 |

| | |
|---|---|
| *Lehrform / SWS:* | 3 SWS Vorlesung, 1 SWS Übung |
| *Gruppengröße:* | Standard |
| *Arbeitsaufwand:* | Standard |
| *Leistungspunkte:* | 6 |
| *Turnus:* | Wintersemester, jährlich |
| *Teilnehmerzahl:* | Standard |
| *Anmeldungsmodalitäten:* | Keine |
| *Voraussetzungen nach Prüfungsordnung:* | Keine besonderen |
| *Empfohlene Voraussetzungen:* | --- |
| *Angestrebte Lernergebnisse:* | Fundiertes Erarbeiten der wahrscheinlichkeitstheoretischen Basis und der entsprechenden stochastischen Grundbegriffe, sowie Einordnung, Anwendung und Umgang mit den wesentlichen stochastischen Parametern und den Hauptergebnissen der Stochastik.<br>Sicheres Argumentieren mit den Fragestellungen der Gesetze der großen Zahlen und der einschlägigen Grenzwertresultate. |
| *Inhalt:* | • Wahrscheinlichkeitsräume, Axiomatik, σ-Algebren, Maßtheorie, Lebesgue'sches Maß, Zufallsgrößen, Lebesgue-Integral, Eigenschaften der L-Integration, Konvergenzsätze<br>• Bedingte Wahrscheinlichkeiten, Stochastische Unabhängigkeit<br>• Diskrete und reelle Wahrscheinlichkeitsmaße<br>• Zufallsvariable, messbare Abbildungen, Parameter der Wahrscheinlichkeit<br>• Wahrscheinlichkeitstheoretische Grundlagen der Informationstheorie<br>• Dichte- und Verteilungsfunktion<br>• Charakteristische Funktionen<br>• Konvergenzbegriffe in der Stochastik |

| | |
|---|---|
| | • Gesetze der großen Zahlen, Kolmogoroff und Cantelli Theorem<br>• Zentraler Grenzwertsatz, allgemeine Grenzwertsätze der Stochastik<br>• Gesetz von iterierten Logarithmus, unbeschränkt teilbare Verteilungen |
| *Studien- / Prüfungsleistungen:* | Prüfungsleistungen: Mündliche Prüfung (45 Min.) |
| *Medienformen:* | Overhead |
| *Literatur:* | Bauer, Heinz: Wahrscheinlichkeitstheorie, de Gruyter, 2001<br>Bauer, Heinz: Maß- und Integrationstheorie, de Gruyter, 1990<br>Feller, W: An introduction to Probability Theory and its Applications, Wiley, 1966<br>Krengel, Ulrich: Einführung in die Wahrscheinlichkeitstheorie und Statistik, Vieweg, 2002<br>Irle, Albrecht: Wahrscheinlichkeitsrechnung und Statistik, Teubner, 2001<br>Hesse, Albrecht: Angewandte Wahrscheinlichkeitstheorie, Vieweg, 2003<br>Gnedenko, B.W.: Einführung in die Wahrscheinlichkeitstheorie, Akademie Verlag, 1991 |
| *Bemerkungen:* | --- |

# Intelligente Systeme

| | |
|---|---|
| *Kürzel:* | INT |
| *Untertitel:* | --- |
| *Studiensemester:* | 1. |
| *Modulverantwortliche(r):* | Prof. Dr. Wolfram Conen |
| *Dozent(in):* | Prof. Dr. Wolfram Conen |
| *Sprache:* | Deutsch |

*Zuordnung zum Curriculum:*

| I/PI | I/TI | I/ISE | MI | WI | IS |
|---|---|---|---|---|---|
| 1 | 1 | 1 | 1 | WP | 1 |

| | |
|---|---|
| *Lehrform / SWS:* | 2 SWS Vorlesung, 1 SWS Übung, 1 SWS Praktikum |
| *Gruppengröße:* | Standard |
| *Arbeitsaufwand:* | Standard |
| *Leistungspunkte:* | 6 |
| *Turnus:* | Wintersemester, jährlich |
| *Teilnehmerzahl:* | Standard |
| *Anmeldungsmodalitäten:* | Siehe Aushang |
| *Voraussetzungen nach Prüfungsordnung:* | Keine besonderen |
| *Empfohlene Voraussetzungen:* | Kenntnisse in Algorithmen und Datenstrukturen, Objektorientierter und Prozeduraler Programmierung, Softwaretechnik sowie Grundlagen der künstlichen Intelligenz auf Bachelor-Niveau |
| *Angestrebte Lernergebnisse:* | Die Studierenden kennen grundlegende Methoden und Strukturen aus ausgewählten Kapiteln der künstlichen Intelligenz und können sie zur Konstruktion von intelligenten Systemen anwenden.<br>Sie sind insbesondere in der Lage, durch Abstraktion und Modellbildung Problemstellungen zu analysieren, Zusammenhänge zu vorhandenem Wissen zu erkennen und entsprechende Lösungsansätze zu identifizieren und umzusetzen.. |
| *Inhalt:* | • Einführendes: Geschichte der KI, Ausgewählte implementierte intelligente Systeme (10 %)<br>• Rückblick: Problemlösung mit exakter Suche, mit Logik (15%)<br>• Suche weiterführend: Heuristiken für A*, Constraints, Suche in Spielen (MinMax, Alpha-Beta, Gleichgewichte), heuristische Suchen, naturanaloge Suchverfahren (25%)<br>• Strukturfindung, Mustererkennung, Lernen und intelligente Informationsanalyse: klassische Verfahren (Kategorisierung, Clustering: Naive Bayes, Decision Trees, EM), stochastische Ver- |

| | |
|---|---|
| | fahren (Hidden Markov, POMDP), naturanaloge Verfahren (NN) (30%)<br>• Planen, Entscheiden, Unsicherheit: Logik und Suche in der Planung; Modellierung von Entscheidungsproblemen, Bayes'sche Netze, Entscheidungstheorie (20%) |
| *Studien- / Prüfungsleistungen:* | Studienleistungen: Ggfs. Zwischenprüfung (45 Min.), erfolgreiche Teilnahme an Übungen und Praktikum.<br>Prüfungsleistungen: Abschlussklausur (75 Min.), |
| *Medienformen:* | Beamer |
| *Literatur:* | Russell, Norvic: Artificial Intelligence, a Modern Approach, Prentice Hall, aktuelle Auflage<br>Ergänzend: aktuelle und historische Papiere der KI-Forschung, je nach Praktikumsprojekt (P) und Vortragsthemen (Ü). |
| *Bemerkungen:* | --- |

# Internet-Sicherheit A

| | |
|---|---|
| *Kürzel:* | ISA |
| *Untertitel:* | --- |
| *Studiensemester:* | 1. |
| *Modulverantwortliche(r):* | Prof. Dr. Norbert Pohlmann |
| *Dozent(in):* | Prof. Dr. Norbert Pohlmann |
| *Sprache:* | Deutsch |

*Zuordnung zum Curriculum:*

| I/PI | I/TI | I/ISE | MI | WI | IS |
|---|---|---|---|---|---|
| WP | WP | - | WP | 1 | 1 |

| | |
|---|---|
| *Lehrform / SWS:* | 3 SWS Vorlesung, 1 SWS Praktikum |
| *Gruppengröße:* | Standard |
| *Arbeitsaufwand:* | Standard |
| *Leistungspunkte:* | 6 |
| *Turnus:* | Wintersemester, jährlich |
| *Teilnehmerzahl:* | Standard |
| *Anmeldungsmodalitäten:* | Keine |
| *Voraussetzungen nach Prüfungsordnung:* | Keine besonderen |
| *Empfohlene Voraussetzungen:* | --- |

*Angestrebte Lernergebnisse:*

- Gutes Verständnis von möglichen Angriffen und geeigneten Gegenmaßnahmen im Bereich der Endgeräte und Anwendungen
- Erlangen der Kenntnisse über den Aufbau, die Prinzipien, die Architektur und die Funktionsweise von Sicherheitskomponenten und –systemen im Bereich Trusted Computing und PKI-orientierten Sicherheitssystemen
- Sammeln von Erfahrungen bei der Ausarbeitung und Präsentation von neuen Themen aus dem Bereich Internet-Sicherheit
- Gewinnen von praktischen Erfahrungen über die Nutzung und die Wirkung von Sicherheitssystemen im Bereich Trusted Computing und PKI-orientierten Sicherheitssystemen
- Erleben der Notwendigkeit und Wichtigkeit der Internet-Sicherheit

*Inhalt:*

- Trusted Computing
  - TPM (Aufbau und Funktionen)
  - TC Funktionen (Trusted Boot, Binding, Sealing, and (Remote) Attestation),
  - Trusted Computing Base
  - Sicherheitsplattform (Idee, Ziele, Methoden, …)
  - Anwendungsbeispiele

| | |
|---|---|
| | • Trusted Network Connect (TNC)<br>- grundsätzliche Idee<br>- TNC Architektur<br>- T-NAC (Idee, Ziele, Methoden, …)<br>• Public-Key-Infrastruktur (PKI): Aufgaben, Komponenten, gesetzlicher Hintergrund, Modelle, Umsetzungskonzepte und praktische Beispiele<br>• Digitale Signatur: Gesetzliche Grundlagen, Mechanismen und Prinzipien, Anwendungsbeispiele<br>• E-Mail-Security: Elemente, Konzepte und praktischer Einsatz<br>• Anti-Spam-System: Schäden, Quellen; Anti-Spam-Technologien, Kopfzeilenanalyse, Textanalyse, Blacklist, Distributed Checksum Clearinghouse (DCC), Distributed IP Reputation System, usw. |
| *Studien- / Prüfungsleistungen:* | Studienleistungen: Erfolgreich absolviertes Praktikum als Vorleistung für die Prüfungszulassung<br>Prüfungsleistungen: Klausur (90 Min.) |
| *Medienformen:* | Beamer |
| *Literatur:* | Pohlmann, N.: Firewall-Systeme - Sicherheit für Internet und Intranet, E-Mail-Security, Virtual Private Network, Intrution Detection-System, Personal Firewalls. 5. aktualisierte und erweiterte Auflage; ISBN 3-8266-0988-3; MITP-Verlag, Bonn 2003<br>A Campo, M.; Pohlmann, N.: Virtual Private Network (VPN). 2. aktualisierte und erweiterte Auflage, ISBN 3-8266-0882-8; MITP-Verlag, Bonn 2003<br>Pohlmann, N.; Reimer, H.: "Trusted Computing - Ein Weg zu neuen IT-Sicherheitsarchitekturen", ISBN 978-3-8348-0309-2, Vieweg-Verlag, Wiesbaden 2008 |
| *Bemerkungen:* | --- |

# Internet-Sicherheit B

| | |
|---|---|
| *Kürzel:* | ISB |
| *Untertitel:* | --- |
| *Studiensemester:* | 2. (oder 1.) |
| *Modulverantwortliche(r):* | Prof. Dr. Norbert Pohlmann |
| *Dozent(in):* | Prof. Dr. Norbert Pohlmann |
| *Sprache:* | Deutsch |

*Zuordnung zum Curriculum:*

| I/PI | I/TI | I/ISE | MI | WI | IS |
|---|---|---|---|---|---|
| - | - | - | - | WP | 2 |

| | |
|---|---|
| *Lehrform / SWS:* | 2 SWS Vorlesung, 1 SWS Übung, 1 SWS Praktikum |
| *Gruppengröße:* | Standard |
| *Arbeitsaufwand:* | Standard |
| *Leistungspunkte:* | 6 |
| *Turnus:* | Sommersemester, jährlich |
| *Teilnehmerzahl:* | Standard |
| *Anmeldungsmodalitäten:* | Keine |
| *Voraussetzungen nach Prüfungsordnung:* | Keine besonderen |
| *Empfohlene Voraussetzungen:* | --- |

*Angestrebte Lernergebnisse:*

- Gutes Verständnis von möglichen Angriffen und geeigneten Gegenmaßnahmen im Bereich der Internet-Infrastruktur
- Erlangen der Kenntnisse über den Aufbau, die Prinzipien, die Architektur und die Funktionsweise von Sicherheitskomponenten und –systemen im Bereich von Frühwarn- und Infrastruktur Sicherheitssystemen
- Sammeln von Erfahrungen bei der Ausarbeitung und Präsentation von neuen Themen aus dem Bereich Internet-Sicherheit
- Gewinnen von praktischen Erfahrungen über die Nutzung und die Wirkung von Sicherheitssystemen im Bereich der Internet-Infrastruktur
- Erleben der Notwendigkeit und Wichtigkeit der Internet-Sicherheit

*Inhalt:*

- IT und Internet Frühwarnsysteme
  - Grundlagen
  - Internet Analyse System (Idee, Ziele, Methoden, …)
  - Internet Verfügbarkeitssystem (Idee, Ziele, Methoden, …)
  - Log-Daten Analyse System (Idee, Ziele, Methoden, …)

| | |
|---|---|
| | • Firewall-Systeme: Definition, Elemente, Konzepte, praktischer Einsatz, die Wirkung und die Mög-lichkeiten und Grenzen von Firewall-Systemen<br>• Personal Firewall: Ziel, Sicherheitskomponenten, Architektur und die Funktionsweise<br>• VPN-Systeme: Ziele, Anwendungsformen, Konzepte, Mechanismen und Protokolle von VPNs und Anwendungsbeispiele<br>• Secure Socket Layer (SSL), Transport Layer Security (TLS): Idee, Mechanismen, Protokolle und Umsetzungskonzepte<br>• Intrusion Detection System: Aufbau, Funktionsweise, Komponenten und Auswertungskonzepte<br>• Security Gateway Konzepte: Authentication, E-Mail, Signatur<br>• Zusammenwirkung der unterschiedlichen Sicherheitssysteme |
| *Studien- / Prüfungsleistungen:* | Studienleistungen: Erfolgreich absolviertes Praktikum als Vorleistung für die Prüfungszulassung<br>Prüfungsleistungen: Klausur (90 Min.) |
| *Medienformen:* | Beamer |
| *Literatur:* | Pohlmann, N.: Firewall-Systeme - Sicherheit für Internet und Intranet, E-Mail-Security, Virtual Private Network, Intrution Detection-System, Personal Firewalls. 5. aktualisierte und erweiterte Auflage; ISBN 3-8266-0988-3; MITP-Verlag, Bonn 2003<br>A Campo, M.; Pohlmann, N.: Virtual Private Network (VPN). 2. aktualisierte und erweiterte Auflage, ISBN 3-8266-0882-8; MITP-Verlag, Bonn 2003<br>Pohlmann, N.; Reimer, H.: "Trusted Computing - Ein Weg zu neuen IT-Sicherheitsarchitekturen", ISBN 978-3-8348-0309-2, Vieweg-Verlag, Wiesbaden 2008 |
| *Bemerkungen:* | --- |

# Master-Arbeit Internet-Sicherheit

| | |
|---|---|
| *Kürzel:* | MIS |
| *Untertitel:* | Abschlussarbeit des Master-Studiums der Internet-Sicherheit |
| *Studiensemester:* | 4. (oder 3.) |
| *Modulverantwortliche(r):* | Studiengangsbeauftragte/r Internet-Sicherheit |
| *Dozent(in):* | Alle Professoren des Master-Studiengangs Internet-Sicherheit |
| *Sprache:* | Deutsch oder Englisch |

*Zuordnung zum Curriculum:*

| I/PI | I/TI | I/ISE | MI | WI | IS |
|---|---|---|---|---|---|
| - | - | - | - | - | 4 |

| | |
|---|---|
| *Lehrform / SWS:* | Master-Arbeit |
| *Gruppengröße:* | Im Regelfall Gruppengröße 1, größere Gruppen möglich (Details zu Gruppenarbeiten siehe Prüfungsordnung) |
| *Arbeitsaufwand:* | 810 Stunden |
| *Leistungspunkte:* | 27 |
| *Turnus:* | Die Vergabe einer Master-Arbeit ist jederzeit möglich. |
| *Teilnehmerzahl:* | Wie Gruppengröße |
| *Anmeldungsmodalitäten:* | In der Prüfungsordnung geregelt |
| *Voraussetzungen nach Prüfungsordnung:* | Zur Master-Arbeit kann zugelassen werden, wer in diesem Studiengang mindestens 48 Leistungspunkte erworben hat. Die fehlenden Prüfungen sollten das Thema der Masterarbeit nicht wesentlich berühren. |
| *Empfohlene Voraussetzungen:* | --- |
| *Angestrebte Lernergebnisse:* | Die/der Studierende ist in der Lage, innerhalb einer vorgegebenen Frist entweder<br>• eine schwierige und komplexe praxisorientierte Problemstellung aus der Internet-Sicherheit sowohl in ihren fachlichen Einzelheiten als auch in den themen- und fachübergreifenden Zusammenhängen nach wissenschaftlichen Methoden selbständig zu bearbeiten und zu lösen oder<br>• eine anspruchsvolle Fragestellung aus der aktuellen Forschung auf dem Gebiet der Internet-Sicherheit unter Anleitung eigenständig zu bearbeiten und selbstständig ein neues wissenschaftliches Ergebnis zu entwickeln. |
| *Inhalt:* | Es soll eine praxisorientierte Problemstellung oder eine Fragestellung aus der Forschung auf dem Gebiet der Internet-Sicherheit mit den im Studium erworbenen oder während der Master-Arbeit neu erlernten wissenschaftlichen Methoden in begrenzter Zeit mit Unterstützung eines erfahrenen Betreuers gelöst |

| | |
|---|---|
| | werden. |
| *Studien- / Prüfungsleistungen:* | In der Prüfungsordnung geregelt |
| *Medienformen:* | Themenspezifisch |
| *Literatur:* | Franck, N.; Stary, J.: Die Technik wissenschaftlichen Arbeitens. UTB-Verlag Stuttgart 2009 (15. Auflage). ISBN-10: 3825207242<br><br>Ebel, H.; Bliefert, C.: Bachelor-. Master- und Doktorarbeit – Anleitungen für den naturwissenschaftlich-technischen Nachwuchs. Verlag Wiley 2009 (4. Auflage). ISBN-10: 3527324771<br><br>Gockel, T.: Form der wissenschaftlichen Ausarbeitung. Springer-Verlag Berlin 2008. ISBN-10: 3540786139<br><br>Themenspezifische Literatur |
| *Bemerkungen:* | --- |

# Kolloquium zur Master-Arbeit Internet-Sicherheit

| | |
|---|---|
| *Kürzel:* | KMIS |
| *Untertitel:* | Abschlussprüfung im Master-Studium der Internet-Sicherheit |
| *Studiensemester:* | 4. |
| *Modulverantwortliche(r):* | Studiengangsbeauftragte/r Internet-Sicherheit |
| *Dozent(in):* | Alle Professoren des Master-Studiengangs Internet-Sicherheit |
| *Sprache:* | Deutsch und Englisch |

*Zuordnung zum Curriculum:*

| I/PI | I/TI | I/ISE | MI | WI | IS |
|---|---|---|---|---|---|
| - | - | - | - | - | 4 |

| | |
|---|---|
| *Lehrform / SWS:* | Kolloquium zur Master-Arbeit |
| *Gruppengröße:* | Im Regelfall Gruppengröße 1, größere Gruppen bei Master-Gruppenarbeiten möglich (Details zu Master-Gruppenarbeiten siehe Prüfungsordnung) |
| *Arbeitsaufwand:* | 90 Stunden |
| *Leistungspunkte:* | 3 |
| *Turnus:* | Das Kolloquium zur Master-Arbeit ist jederzeit möglich. |
| *Teilnehmerzahl:* | Wie Gruppengröße |
| *Anmeldungsmodalitäten:* | In der Prüfungsordnung geregelt |
| *Voraussetzungen nach Prüfungsordnung:* | Das Kolloquium zur Masterarbeit kann nur erfolgen, wenn die/der Studierende alle für die Ableistung des Studienganges geforderten Prüfungen bestanden hat und somit mindestens 90 Leistungspunkte erworben hat und die Masterarbeit mindestens als „ausreichend" bewertet worden ist. |
| *Empfohlene Voraussetzungen:* | --- |
| *Angestrebte Lernergebnisse:* | Die/der Studierende ist in der Lage, die Ergebnisse ihrer/seiner Master-Arbeit aus der Internet-Sicherheit, ihre fachlichen Grundlagen, ihre Einordnung in den aktuellen Stand der Technik, bzw. der Forschung, ihre fächerübergreifenden Zusammenhänge und ihre außerfachliche Bezüge in begrenzter Zeit in einem Vortrag zu präsentieren.<br><br>Darüber hinaus kann sie/er Fragen zu inhaltlichen Details, zu fachlichen Begründungen und Methoden sowie zu inhaltlichen Zusammenhängen zwischen Teilbereichen ihrer/seiner Arbeit beantworten.<br>Die/der Studierende kann ihre/seine Master-Arbeit auch im Kontext beurteilen und ihre Bedeutung für die Praxis und die Forschung einschätzen und ist in der Lage, auch entsprechende Fragen nach themen- und fachübergreifenden Zusammenhängen zu beantworten. |

| | |
|---|---|
| *Inhalt:* | Zunächst wird der Inhalt der Master-Arbeit aus der Internet-Sicherheit im Rahmen eines Vortrages präsentiert. Anschließend sollen in einer Diskussion Fragen zum Vortrag und zur Master-Arbeit beantwortet werden.<br><br>Die Prüfer können weitere Zuhörer zulassen. Diese Zulassung kann sich nur auf den Vortrag, auf den Vortrag und einen Teil der Diskussion oder auf das gesamte Kolloquium zur Master-Arbeit erstrecken.<br><br>Der Vortrag soll die Problemstellung der Master-Arbeit, die vergleichende Darstellung alternativer oder konkurrierender Lösungsansätze mit Bezug zum aktuellen Stand der Technik, bzw. Forschung, den gewählten Lösungsansatz, die erzielten Ergebnisse zusammen mit einer abschließenden Bewertung der Arbeit sowie einen Ausblick beinhalten. Je nach Thema können weitere Anforderungen hinzukommen. Die Dauer des Vortrages wird vom Erstprüfer festgelegt und kann zwischen 30 und 40 Minuten betragen.<br><br>In der anschließenden Diskussion werden Fragen von den Prüfern gestellt. Fragen der übrigen Zuhörer des Kolloquiums können durch die Prüfer ebenfalls zugelassen werden. Die Dauer der Diskussion wird durch die Prüfer bestimmt und beträgt ca. 30-45 Minuten. |
| *Studien- / Prüfungsleistungen:* | Benotung des Vortrages und der anschließenden Diskussion durch die Prüfer laut Prüfungsordnung |
| *Medienformen:* | Themenspezifisch |
| *Literatur:* | Kuzbari, R.; Ammer, R.: Der wissenschaftliche Vortrag. Springer-Verlag Wien New York, 2006. ISBN-10 3-211-23525-6<br><br>Leopold-Wildburger, U.; Schütze, J.: Verfassen und Vortragen - Wissenschaftliche Arbeiten und Vorträge leicht gemacht. Springer-Verlag Berlin Heidelberg New York, 2002. ISBN 3-540-43027-X |
| *Bemerkungen:* | --- |

# Master-Projekt Internet-Sicherheit

| | |
|---|---|
| *Kürzel:* | MPIS |
| *Untertitel:* | --- |
| *Studiensemester:* | 2. (oder 1.) |
| *Modulverantwortliche(r):* | Studiengangsbeauftragte/r Internet-Sicherheit |
| *Dozent(in):* | Alle am Master-Studiengang Internet-Sicherheit beteiligten Professoren |
| *Sprache:* | Deutsch oder Englisch |

| *Zuordnung zum Curriculum:* | I/PI | I/TI | I/ISE | MI | WI | IS |
|---|---|---|---|---|---|---|
| | - | - | - | - | - | 2 |

| | |
|---|---|
| *Lehrform / SWS:* | 4 SWS Projekt |
| *Gruppengröße:* | Standard, Projektteams von 6 bis 8 Studierenden |
| *Arbeitsaufwand:* | Standard |
| *Leistungspunkte:* | 12 |
| *Turnus:* | Sommersemester, jährlich |
| *Teilnehmerzahl:* | Standard |
| *Anmeldungsmodalitäten:* | Siehe Aushang |
| *Voraussetzungen nach Prüfungsordnung:* | Keine besonderen |
| *Empfohlene Voraussetzungen:* | --- |
| *Angestrebte Lernergebnisse:* | Die Studierenden sind in der Lage, ihre bisher erworbenen speziellen Kenntnisse, Fertigkeiten und Lösungsstrategien aus der Informatik auf interdisziplinäre Problemstellungen anwenden. |
| *Inhalt:* | Im Master-Projekt Internet-Sicherheit wird besonders die interdisziplinäre Komponente des Masterstudiengangs Internet-Sicherheit in den Mittelpunkt gerückt. Während der Projektarbeit sollen die Studenten vor allem ihre speziellen Kenntnisse, Fertigkeiten und Lösungsstrategien aus der Informatik auf interdisziplinäre Problemstellungen anwenden.<br><br>Interdisziplinäre Projekte können mit den anderen Master-Studiengänge koordiniert werden: Beispiele sind: Wirtschaftsinformatik (Return of Security Investment (RoSI), Mehrwerte von Internet-Sicherheit, …) oder Technische Informatik (Sicherheit bei „Internet der Dinge", …) oder Medieninformatik (Vertrauenswürdige Gestaltung von Oberflächen, Darstellung von sicherheitsrelevanten Ereignissen auf einer intuitiven Weise, …) oder Praktische Informatik (Integration von IT-Sicherheit in Anwendungen, …).<br><br>Die Projektteams haben dabei die Verantwortung für die genaue Ausgestaltung und das Zeitmanagement. |
| *Studien- / Prüfungsleistungen:* | Prüfungsleistungen: Ausarbeitung |

| | |
|---|---|
| *Medienformen:* | Themenabhängig |
| *Literatur:* | Themenabhängig, wird zu Veranstaltungsbeginn bekannt gegeben |
| *Bemerkungen:* | --- |

# Master-Seminar Internet-Sicherheit

| | |
|---|---|
| *Kürzel:* | MSIS |
| *Untertitel:* | Fachseminar zu aktuellen Themen der Internet-Sicherheit |
| *Studiensemester:* | 3. |
| *Modulverantwortliche(r):* | Studiengangsbeauftragte/r Internet-Sicherheit |
| *Dozent(in):* | Alle Professoren des Master-Studiengangs Internet-Sicherheit |
| *Sprache:* | Deutsch |

*Zuordnung zum Curriculum:*

| I/PI | I/TI | I/ISE | MI | WI | IS |
|---|---|---|---|---|---|
| - | - | - | - | - | 3 |

| | |
|---|---|
| *Lehrform / SWS:* | 2 SWS Seminar |
| *Gruppengröße:* | Standard |
| *Arbeitsaufwand:* | Standard<br>Präsenz: Seminar und individuelle Vorbesprechungen mit dem Dozenten<br>Eigenstudium: Aufarbeitung des Themas, Erarbeitung der Seminarausarbeitung und des Seminarvortrags |
| *Leistungspunkte:* | 6 |
| *Turnus:* | Zu jedem Semester |
| *Teilnehmerzahl:* | Wie Gruppengröße |
| *Anmeldungsmodalitäten:* | Elektronische Anmeldung erbeten |
| *Voraussetzungen nach Prüfungsordnung:* | Keine besonderen |
| *Empfohlene Voraussetzungen:* | --- |
| *Angestrebte Lernergebnisse:* | Die Studierenden besitzen die folgenden Fähigkeiten:<br>• Sie sind in der Lage zur selbstständigen Einarbeitung in aktuelle Forschungsfragen zur Internet-Sicherheit auf der Basis von Primärliteratur (Publikationen in Fachzeitschriften sowie Tagungsbeiträge);<br>• Sie können Informationsrecherchen zu forschungsorientierten Fragestellungen durchführen und sind in der Lage dazu eine strukturierte schriftliche Aufbereitung des aktuellen Stands der Forschung zu erarbeiten;<br>• Sie können eine zusammengefasste Darstellung der Ergebnisse zu einer Fragestellung präsentieren sowie in der Diskussion mit allen Seminarteilnehmern sich ergebende Fragen beantworten und aufgestellte Thesen verteidigen. |
| *Inhalt:* | Im Rahmen dieses Seminars bearbeiten die Studenten ausgewählte Themen aus dem Bereich Internet- |

| | |
|---|---|
| | Sicherheit. Die Studenten bearbeiten die Themen und den Ablauf eigenständig. Der Dozent und die anderen teilnehmenden Studenten sind unterstützend tätig und der Dozent vermittelt bei Bedarf die Inhalte.<br><br>Jeweils ein Student moderiert die Seminarstunde. Ein anderer Student schreibt das Protokoll für die Seminarstunde. Die Aufgaben wechseln jedes Mal. Die Studenten erarbeiten Zwischenpräsentationen und eine Abschlusspräsentation und tragen diese jeweils mit anschließender Diskussion vor. |
| *Studien- / Prüfungsleistungen:* | Prüfungsleistungen: Ausarbeitung und Vortrag |
| *Medienformen:* | Themenspezifisch |
| *Literatur:* | In der Regel Primärliteratur aus der aktuellen Forschung, themenspezifisch |
| *Bemerkungen:* | --- |

# Programmiermethodik und Sicherheit

| | | | | | | |
|---|---|---|---|---|---|---|
| *Kürzel:* | PRMS | | | | | |
| *Untertitel:* | --- | | | | | |
| *Studiensemester:* | 1. (oder 2.) | | | | | |
| *Modulverantwortliche(r):* | Prof. Dr. Marcel Luis | | | | | |
| *Dozent(in):* | Prof. Dr. Marcel Luis oder Lehrbeauftragte/r | | | | | |
| *Sprache:* | Deutsch | | | | | |
| *Zuordnung zum Curriculum:* | I/PI | I/TI | I/ISE | MI | WI | IS |
| | WP | WP | - | WP | WP | 1 |
| *Lehrform / SWS:* | 2 SWS Vorlesung, 2 SWS Praktikum | | | | | |
| *Gruppengröße:* | Standard | | | | | |
| *Arbeitsaufwand:* | Standard | | | | | |
| *Leistungspunkte:* | 6 | | | | | |
| *Turnus:* | Wintersemester, jährlich | | | | | |
| *Teilnehmerzahl:* | Standard | | | | | |
| *Anmeldungsmodalitäten:* | --- | | | | | |
| *Voraussetzungen nach Prüfungsordnung:* | Keine besonderen | | | | | |
| *Empfohlene Voraussetzungen:* | Kenntnisse in objektorientierter Software-Entwicklung auf Bachelor-Niveau | | | | | |
| *Angestrebte Lernergebnisse:* | Die Studierenden kennen Methoden und Techniken, um effizient zuverlässige Software hoher Qualität für sich schnell ändernde und wachsende Anforderungen zu erstellen - insbesondere für Anwendungen mit hohen Anforderungen an Sicherheit. | | | | | |
| *Inhalt:* | • Test-Driven Design<br>• Testautomatisierung mit Mock-Objekten<br>• Refaktorisierung<br>• Generische und Meta-Programmierung<br>• Inversion of Control<br>• Convention over Configuration<br>• Programming by Contract<br>• Nebenläufige Programmierung | | | | | |
| *Studien- / Prüfungsleistungen:* | Prüfungsleistungen: Klausur (90 Min.) oder mündliche Prüfung | | | | | |
| *Medienformen:* | Beamer-Präsentation | | | | | |
| *Literatur:* | Steve Freeman, Nat Pryce; Growing Object-Oriented Software, Guided by Tests; Addison-Wesley Longman, 2009<br>Martin Fowler; Refactoring; Addison-Wesley; 2005 | | | | | |

| | |
|---|---|
| | Bertrand Meyer; Object-Oriented Software Construction; Prentice Hall; 2000<br>Martin Fowler; Using Metadata; IEEE Software 19(6), S. 13-17; 2002<br>Martin Fowler; To Be Explicit; IEEE Software 18(6), S. 10-15; 2001 |
| *Bemerkungen:* | --- |

# Weiterführende Konzepte zum Betrieb komplexer verteilter Systeme

| | |
|---|---|
| *Kürzel:* | WKV |
| *Untertitel:* | --- |
| *Studiensemester:* | 2. (oder 1.) |
| *Modulverantwortliche(r):* | Prof. Dr. Andreas Cramer |
| *Dozent(in):* | Prof. Dr. Andreas Cramer |
| *Sprache:* | Deutsch |

*Zuordnung zum Curriculum:*

| I/PI | I/TI | I/ISE | MI | WI | IS |
|---|---|---|---|---|---|
| WP | - | - | - | WP | 2 |

| | |
|---|---|
| *Lehrform / SWS:* | 2 SWS Vorlesung, 1 SWS Übung, 1 SWS Praktikum |
| *Gruppengröße:* | Standard |
| *Arbeitsaufwand:* | Standard |
| *Leistungspunkte:* | 6 |
| *Turnus:* | Sommersemester, jährlich |
| *Teilnehmerzahl:* | Standard |
| *Anmeldungsmodalitäten:* | Siehe Aushang |
| *Voraussetzungen nach Prüfungsordnung:* | Keine besonderen |
| *Empfohlene Voraussetzungen:* | Kenntnisse zum Betrieb komplexer verteilter Systeme auf Bachelor-Niveau |
| *Angestrebte Lernergebnisse:* | Die Studierenden lernen unterschiedliche Technologien, Konzepte und Verfahren kennen, die für den Betrieb großer IT-Infrastrukturen wichtig sind.<br>Sie erlernen erste Erfahrungen im Umgang mit diesen Technologien und Verfahren.<br>Sie erlangen die Fähigkeit, neue Technologien in diesem Umfeld schnell begreifen, einordnen und bewerten zu können. |
| *Inhalt:* | • ITIL<br>• IT-Controlling<br>• Fehlertoleranz<br>• Leistungsbewertung<br>• Modellierung, Warteschlangen, zeitbehaftete Petri-Netze<br>• Messungen, Software, HW, hybrid<br>• Zusammenhang zwischen Messung und Modellierung<br>• Rechner-Cluster<br>• Hochverfügbarkeit |

| | |
|---|---|
| | • Grids |
| *Studien- / Prüfungsleistungen:* | Prüfungsleistungen: Klausur oder mündliche Prüfung |
| *Medienformen:* | Präsentationsfolien mit Beamer |
| *Literatur:* | Nach Bekanntgabe in der Vorlesung |
| *Bemerkungen:* | --- |

# Wissenschaftliche Vertiefung Internet-Sicherheit

| | |
|---|---|
| *Kürzel:* | WVIS |
| *Untertitel:* | --- |
| *Studiensemester:* | 3. |
| *Modulverantwortliche(r):* | Studiengangsbeauftragte/r Internet-Sicherheit |
| *Dozent(in):* | Alle am Master-Studiengang Internet-Sicherheit beteiligten Professoren |
| *Sprache:* | Deutsch oder Englisch |

| *Zuordnung zum Curriculum:* | I/PI | I/TI | I/ISE | MI | WI | IS |
|---|---|---|---|---|---|---|
| | - | - | - | - | - | 3 |

| | |
|---|---|
| *Lehrform / SWS:* | 2 SWS Projekt |
| *Gruppengröße:* | Standard, Projektteams von 3 bis 5 Studierenden |
| *Arbeitsaufwand:* | Standard |
| *Leistungspunkte:* | 12 |
| *Turnus:* | Zu jedem Semester |
| *Teilnehmerzahl:* | Standard |
| *Anmeldungsmodalitäten:* | Siehe Aushang |
| *Voraussetzungen nach Prüfungsordnung:* | Keine besonderen |
| *Empfohlene Voraussetzungen:* | --- |
| *Angestrebte Lernergebnisse:* | Die Studierenden sind in der Lage, wissenschaftlich anspruchsvolle Problemstellungen selbstständig und zielorientiert zu bearbeiten. |
| *Inhalt:* | Im Rahmen dieses Projekts bearbeiten die Studierenden aktuelle Themen aus dem Bereich der Internet-Sicherheit. Die Themen orientieren sich an den Forschungsthemen des Instituts für Internet-Sicherheit - if(is). Die Rahmenbedingungen für das Projekt werden von den Lehrenden vorgegeben, die Ausgestaltung und die Verantwortung liegen aber bei den einzelnen Projektteams des Institutes. Dadurch sollen die Studierenden das selbstständige und zielorientierte Bearbeiten von wissenschaftlichen Problemstellungen über einen längeren Zeitraum erlernen. Ein Schwerpunkt dieses Seminars bildet die eigenständige Bearbeitung wissenschaftlicher Fragestellungen. |
| *Studien- / Prüfungsleistungen:* | Prüfungsleistungen: Ausarbeitung |
| *Medienformen:* | Themenabhängig |
| *Literatur:* | Themenabhängig, wird zu Veranstaltungsbeginn bekannt gegeben |
| *Bemerkungen:* | --- |