Hochschule
Albstadt-Sigmaringen
Albstadt-Sigmaringen University

Wahlpflichtmodul-Katalog

Fakultät Informatik
Studiengang
Advanced IT Security M.Sc.

StuPO 21.2
ab Wintersemester 2021/22
Ersteller: Prof. Dr. German Nemirovski, Studiendekan
Verantwortlich: Prof. Dr. German Nemirovski, Studiendekan

Inhaltsverzeichnis

1 Qualifikationsziel-Modul-Matrix

			Unterstützung der Qualifikationsziele in den Modulen (0=keine Unterstützung, 1=indirekte Unterstützung, 2=direkte Unterstützung)					
Modul-Nr.	**Modulbezeichnung**	**Summe der Unterstützungs-punkte**	Sicherheitskompetenz	Methodenkompetenz	Ethische und Rechtliche Kompetenz	Konzeptionelle Fähigkeit	Vernetztes Denken	Forschungskompetenz
52600	Advanced Network and Internet Security	9	2	2	1	1	2	1
51100	Business Intelligence	6		2		2	1	1
52300	Distributed Enterprise Applications	7	1	2	0	2	1	1
xxxxx	Einführung in die Cyberpsychologie	9	1	2	1	2	2	1
xxxxx	Einführung in die Grundlagen der Quantuminformatik	6		1		2	1	2
xxxxx	Entscheidungen, Performance und Kognition im Cyberspace II	10	1	2	1	2	2	2
xxxxx	File System Forensics	10	2	2	2	2	1	1
52400	Financial Risk & Financial Management	10	1	2	2	1	2	2
xxxxx	Fortgeschrittene Zahlentheoretische Algorithmen	8	2	2		2	1	1
xxxxx	Highly Optimized Hardware Cryptography	8	1	2		2	1	2
51700	Incident Response and Malware Defence	8	2	1	1	1	1	2
52500	Innovation and Transfer Competence	7		1		2	2	2
xxxxx	Post-Quantum Cryptography and Quantum Key Exchange	8	2	2		2	1	1
51400	Semantic Web	5		1		2		2
xxxxx	Tutorials	5		2		2		1

2 Studiengangs-Kompetenzmatrix

	Kompetenzen	**Fachkompetenz**					**Personale Kompetenz**					
		Wissen		**Fertigkeiten**			**Sozial-kompetenz**			**Selbständig-keit**		
Modul-Nr.	**Ausprägung** **Modulbezeichnung**	Tiefe	Breite	Instrumentelle Fertigkeiten	systemische Fertigkeiten	Beurteilungs-fähigkeit	Team-/Führungs-fähigkeit	Mitgestaltung	Kommunikation	Eigenständigkeit/ Verantwortung	Reflexivität	Lernkompetenz
52600	Advanced Network and Internet Security	7		7		7			7	7		
51100	Business Intelligence	7	7	7				7			7	
52300	Distributed Enterprise Applications	7		7		7			7	7		
xxxxx	Einführung in die Cyberpsychologie II	7	7			7	7		7			7
xxxx	Einführung in die Grundlagen der Quantuminformatik	7		7								7
xxxxx	Entscheidungen, Performance u. Kognition im Cyberspace II	7		7		7			7			7
xxxxx	File System Forensics	7		7		7			7	7		
52400	Financial Risk & Financial Management	7		7		7			7	7		
xxxxx	Fortgeschrittene Zahlentheoretische Algorithmen	7		7					7	7		
xxxxx	Highly Optimized Hardware Cryptography	7		7		7	7			7		
51700	Incident Response and Malware Defence	7	7	7	7				7	7	7	
52500	Innovation and Transfer Competence		7	7	7		7			7		7
xxxxx	Post-Quantum Cryptography and Quantum Key Exchange	7		7	7	7			7	7		
51400	Semantic Web	7		6	7				7	7		
xxxxx	Tutorials	7			7				7			7

3 Modulbeschreibungen

3.1 Wintersemester

3.1.1 51100 – Business Intelligence

Studiengang: INF
StuPO-Version: 21.2

Semester: WS 2021/22
Letzte Bearbeitung: 15.09.21

<table>
<tr><td colspan="8">Modul: Business Intelligence</td></tr>
<tr><td colspan="2">Kennnummer
51100</td><td>Workload
180 h</td><td>Modulart
WPM</td><td colspan="2">Studiensemester
1</td><td>Dauer
1 Semester</td><td>Häufigkeit
WS</td></tr>
<tr><td>1</td><td colspan="2">Lehrveranstaltung(en)
Vorlesung Business Intelligence
Project Business Intelligence</td><td colspan="2">Sprache
Deutsch oder Englisch, wenn von den Modulteil-nehmern gewünscht (deutsches und englisches Literatur-studium erforderlich)</td><td>Kontakt-zeit
4 SWS / 60 h</td><td>Selbst-studium
120 h</td><td>Credits (ECTS)
6</td></tr>
<tr><td>2</td><td colspan="7">Lehrform(en) / SWS:
Vorlesung: 2 SWS
Projekt: 2 SWS</td></tr>
<tr><td>3</td><td colspan="7">Lernergebnisse (learning outcomes), Kompetenzen:

Kompetenz Wissen
Die Studierenden kennen den elementaren Aufbau von Data Warehouse Systemen und sind mit den zentralen Konzepten der Informationsvisualisierung vertraut [Wissen, 7]</td></tr>
<tr><td></td><td colspan="7">Kompetenz Fertigkeiten
Die Studierenden sind in der Lage, die Konzepte des Data Warehousing in realen Anwendungsszenarien konzeptionell und operativ umzusetzen. Sie können Kennzahlen mittels geeigneter Methoden visualisieren. [Instrumentelle Fertigkeiten, 7]</td></tr>
<tr><td></td><td colspan="7">Sozialkompetenz
Die Studierenden erarbeiten gemeinsam Lösungsansätze zu vorgegebenen Fragestellungen [Mitgestaltung, 7]</td></tr>
<tr><td></td><td colspan="7">Selbstständigkeit
Konzeption und Aufbau von Szenarien zur Erfassung, Aufbereitung und Analyse von Kennzahlen wird in Bezug auf die jeweiligen Anforderungen kritisch diskutiert. [Reflexivität, 7]</td></tr>
</table>

4	**Inhalte*:*** Abgrenzung dispositive vs. operative Datenbestände (OLTP / OLAP) Data Warehouse Architekturen ETL-Prozesse (Datenqualität, Datenbereinigung, Transformation, etc. Logische und semantische Datenmodelle für Data Warehouses (Star-/Snowflake-Schema,…) Implementierung von Data Warehouses (MOLAP, ROLAP,..) spezielle Aspekte im Zusammenhang mit Data Warehouses (slowly changing dimensions,…) Date Warehouse Projekte (agiles Vorgehen) Aufbau eines Data Warehousing Prozesses mittels SAP BW on HANA Visualisierung von Kennzahlen Konzeption und Aufbau von Dashoards Visual Analytics (Reduktion von Darstellungsdimensionen, Visualisierung von Objekten auf Grundlage von Unähnlichkeitsmaßen…)
	Empfohlene Literaturangaben: Bauer, A, Günzel, H (Hrsg): Data Warehouse Systeme – Architekur, Entwickung, Anwendung, dpunkt verlag, 2013 Müller, R.M., Lenz, H.-J.: Business Intelligence, Springer Vieweg, 2013 Kemper, H. G., Mehanna, W., & Unger, C. : Business Intelligence– Grundlagen und praktische Anwendungen, Vieweg, Wiesbaden, 2004, ISBN:3834807192 Klein, A., Gräf, J.: Reporting und Business Intelligence, Haufe-Lexware, 2014, ISBN: 364804771X Sharda, T. Aronson, King, A.:Business Intelligence: A Managerial Approach, Pearson Verlag, 2008, ISBN: 013610066X Kohlhammer, J., Proff, D.U., Wiener, A.: Visual Business Analytics: Effektiver Zugang zu Daten und Informationen. dpunkt.verlag GmbH, 2014, ISBN: 3864900441
5	**Teilnahmevoraussetzungen:** Empfohlen: Datenbank-Grundlagen
6	**Prüfungsformen***:* Klausur 90 min., benotet Praktische Arbeit, unbenotet
7	***Voraussetzungen für die Vergabe von Kreditpunkten:*** Bestandene schriftliche Modulprüfung; erfolgreiche Bearbeitung der Aufgaben im Praktikum
8	***Verwendbarkeit des Moduls:*** Business and Security Analytics, M.Sc., Advanced IT Security M.Sc., Systems Engineering M.Eng. (Für SE-Studierende ergibt sich durch das Belegen des Moduls ggf. ein höherer Workload als in StuPO vorgesehen)
9	***Modulverantwortliche(r):*** Prof. Dr. Bernd Stauß Dozenten: Prof. Dr. Bernd Stauß, N.N.
10	***Optionale Informationen:*** Studiengangsspezifische, zusätzliche Informationen zum Modul

3.1.2 XXXXX – Einführung in die Cyberpsychologie II

Studiengang: INF
StuPO-Version: 21.2

Semester: WS 2021/22
Letzte Bearbeitung: 15.09.21

Modul: Einführung in die Cyberpsychologie II						
Kennnummer XXXX	**Workload** 90 h	**Modulart** WPM	**Studiensemester** 1	**Dauer** 1	**Häufigkeit** WS und SS	
1	**Lehrveranstaltung(en)** Einführung in die Cyberpsychologie II	**Sprache** Deutsch und Englisch	**Kontakt-zeit** 2 SWS / 30	**Selbst-studium** 60 h	**Credits (ECTS)** 3	
2	**Lehrform(en) / SWS:** Vorlesung mit Übungen / 2 SWS					
3	**Lernergebnisse (learning outcomes), Kompetenzen:** *Kompetenz Wissen* Die Studierenden kennen eine breite Auswahl Grundkonzepte im Bereich der Informatik. *[Wissen, 7]* Weiter haben die Studierenden Detailwissen über gängige Forschungsmethoden und -ergebnisse im Bereich der Cyberpsychologie. *[Wissen, 7]* *Kompetenz Fertigkeiten* Kompetenz zur Identifikation forschungsrelevanter Fragestellung, deren methodischer Umsetzung und zur kritischen Beurteilung publizierter internationaler Forschung. *[Instrumentelle Fertigkeiten, 7]* *Sozialkompetenz* Sicherheit und Routine im forschungsbezogenen Dialog mit fremdsprachigen Experten. Sicherheit und Routine in der gemeinsamen Erörterung spezifischer Fragestellungen mit internen und externen Partnern. *[Kommunikation, 7]* *Selbstständigkeit* Studierende verstehen das Lernen als einen zuweilen herausfordernden Prozess, der individuelle sowie auch soziale Komponenten umfasst; Sie verfügen über überdurchschnittliche Motivation und Ausdauer um komplexe und insbesondere interdisziplinäre Inhalte zu erlernen und verwenden dabei etablierte Prozesse und Kriterien wissenschaftlichen Forschens. *[Lernkompetenz, 7]*					
4	Inhalte: - Gaming und Gamification - Cyberkognition - Human Factor in Cybersecurity und Social Engineering - Cyberkriminalität und Netzwerkverteidigung - e-Health					

	- Forschungsmethoden Cyberpsychologie - Neuro- and biopsychologische Aspekte der human-computer-interaction und Usability - Avatare, virtuelle Agenten, human-robot-interaction -
	Empfohlene Literaturangaben: Attrill-Smith, A., Fullwood, C., Keep, M., & Kuss, D. J. (Eds.). (2019). The Oxford Handbook of Cyberpsychology. Oxford University Press. Edgar, T.W., & Manz, D.O. (2017). Research Methods for Cybersecurity. Elsevier: Cambridge.
5	**Teilnahmevoraussetzungen:** Keine über die Studien- und Prüfungsordnung hinausgehenden Voraussetzungen.
6	**Prüfungsformen***:* Schriftliche Prüfung (K60)
7	***Voraussetzungen für die Vergabe von Kreditpunkten:*** Bestandene Prüfung
8	***Verwendbarkeit des Moduls:*** Advanced IT Security M.Sc., Business and Security Analytics M.Sc., Systems Engineering M.Eng. (Für SE-Studierende ergibt sich durch das Belegen des Moduls ggf. ein höherer Workload als in StuPO vorgesehen)
9	***Modulverantwortliche(r):*** Prof. Dr. Stefan Sütterlin Dozent: Prof. Dr. Stefan Sütterlin
10	***Optionale Informationen:*** Studiengangsspezifische, zusätzliche Informationen zum Modul

3.1.3 XXXXX – Einführung in die Grundlagen der Quantuminformatik

Studiengang: INF
StuPO-Version: 21.2

Semester: WS 2021/22
Letzte Bearbeitung: 15.09.21

<table>
<tr><td colspan="8">Modul: Einführung in die Grundlagen der Quantuminformatik</td></tr>
<tr><td colspan="2">Kennnummer
XXXX</td><td>Workload
180 h</td><td>Modulart
WPM</td><td colspan="2">Studiensemester
1</td><td>Dauer
1</td><td>Häufigkeit
WS</td></tr>
<tr><td>1</td><td colspan="3">Lehrveranstaltung(en)
a. XXX Vorlesung Grundlagen der Quantuminformatik
b. XXX Übung Grundlagen der Quantuminformatik</td><td>Sprache
a.,b., deutsch oder englisch</td><td>Kontakt-zeit
4 SWS /
a. 30 h
b. 30 h</td><td>Selbst-studium
120 h</td><td>Credits (ECTS)
6</td></tr>
<tr><td>2</td><td colspan="7">Lehrform(en) / SWS:
a. Vorlesung, b. Übung (4 SWS)</td></tr>
<tr><td>3</td><td colspan="7">Lernergebnisse (learning outcomes), Kompetenzen:

Kompetenz Wissen
Die Studierenden beherrschen die Grundlagen der Quanteninformatik: Grundlagen der Quantenmachnik und Ihrer potenziellen Anwendung in der Datenverarbeitung. [Wissen, 7]

Kompetenz Fertigkeiten
Die Studierenden entwickeln die Fähigkeit, die Weiterentwicklung der Quanteninformatik zu verfolgen um die Auswirkungen auf die IT-Industrie abschätzen zu können. [Instrumentelle Fertigkeiten, 7]

Sozialkompetenz
Nicht relevant

Selbstständigkeit
Die Studierenden sind in der Lage, komplexe Fragestellungen selbständig zu Bearbeiten und den eigenen Fortschritt adäquat zu bemessen [Lernkompetenz, 7]</td></tr>
<tr><td>4</td><td colspan="7">Inhalte:
Grundlagen der Quantentheorie: Postulate der Theorie, Prozess der Messung in Quantenmechanik. Verschränkung. Entropie. Quantum Gates und Schaltungen. Anwendungsbeispiele: Transportation, Cloning, Cryptographie. Typen der Quantumalgorithmen und Beispiele.</td></tr>
<tr><td></td><td colspan="7">Empfohlene Literaturangaben:
Michael Nielsen, Issak Chuang, Quantum Computation and Quantum Information, Cambridge University Press.
Benjamin Schumacher and Mike Westmoreland, Quantum Processes Systems, and Information, Cambridge University Press.</td></tr>
</table>

	Mark M. Wilde, Quantum Information Theory, Cambridge University Press. Thomas Cover, Elements of Information Theory, Wiley.
5	**Teilnahmevoraussetzungen:** Gute Mathematikkenntnisse auf dem Niveau der Mathematik für Informatik (Bachelor). Solide Grundkenntnisse der komplexen Arithmetik und der linearen Algebra sind wichtig. Der Begriff des Tensorproduktes und die Eigenvektoren werden in der Vorlesung wiederholt. Es werden keine Vorkenntnisse der Quantenmechanik vorausgesetzt.
6	**Prüfungsformen***:* Mündliche Prüfung 45 min. (Modulprüfung)
7	***Voraussetzungen für die Vergabe von Kreditpunkten:*** Bestandene mündliche Prüfung
8	***Verwendbarkeit des Moduls:*** Advanced IT Security M.Sc., Business and Security Analytics M.Sc., Systems Engineering M.Eng. (Für SE-Studieremde ergibt sich durch das Belegen des Moduls ggf. ein höherer Workload als in StuPO vorgesehen)
9	***Modulverantwortliche(r):*** Prof. Dr. German Nemirovski Dozent: Dr. Andreas Teshler
10	***Optionale Informationen:*** Studiengangsspezifische, zusätzliche Informationen zum Modul

3.1.4 XXXXX – Entscheidungen, Performance und Kognition im Cyberspace II

Studiengang: INF
StuPO-Version: 21.2

Semester: WS 2021/22
Letzte Bearbeitung: 15.09.21

Modul: Entscheidungen, Performance und Kognition im Cyberspace II					
Kennnummer XXXX	**Workload** 90 h	**Modulart** WPM	**Studiensemester** 1	**Dauer** 1	**Häufigkeit** WS

1	**Lehrveranstaltung(en)** Entscheidungen, Performance und Kognition im Cyberspace	**Sprache** Deutsch und Englisch	**Kontakt-zeit** 2 SWS / 30 h	**Selbst-studium** 60 h / 2 SWS	**Credits (ECTS)** 3
2	**Lehrform(en) / SWS:** Vorlesung mit Übungen (2 SWS)				
3	**Lernergebnisse (learning outcomes), Kompetenzen:** *Kompetenz Wissen* Die Studierenden sind mit dem neuesten interdisziplinären Forschungsstand in den Bereichen der Kognitiven Psychologie, Leistungs- und Entscheidungspsychologie mit jeweiliger Relevanz für die Cyberpsychologie vertraut *[Wissen, 7]* *Kompetenz Fertigkeiten* Selbständiges Reflektieren eigener und kritisches Beurteilen anderer international publizierter Forschungsansätze. Fähigkeit, fachfremde Forschungspublikationen methodisch und inhaltlich zu erfassen und selbständig zu erarbeiten. *[Instrumentelle Fertigkeiten, 7]* *Sozialkompetenz* Fortgeschrittene Kompetenzen in der Konsultation und fachlichen Kommunikation mit internationalen fremdsprachigen Experten. *[Kommunikation, 7]* *Selbstständigkeit* Die Studiereden verstehen das Lernen als einen anspruchsvollen und komplexen Prozess, der indivuduelle sowie auch soziale Komponenten umfasst; Sie verfügen über überdurchschnittliche Motivation, Ausdauer und Selbstvertrauen um komplexe Inhalte internationaler englischsprachiger Forschungspublikationen inhaltlich zu erlernen und methodisch zu bewerten und verwenden dabei die Prinzipien guter wissenschaftlicher Praxis. *[Lernkompetenz, 7]*				
4	Inhalte: Angewandte Kognitionspsychologie: - Cyberkognition: Effekte von Online-Welten und digitaler Interaktion auf Denken u. Entscheiden - Mechanismen menschlicher Entscheidungsfindungen - Gaming, Gamers, Gamification – Implikationen für Performance im IT-Bereich - Einflüsse von Gaming auf kognitive Leistungsfähigkeit, Brain Training - Human-robot-interaction, Avatare und intelligente Agenten Angewandte Beispiele der Personal- und Organisationspsychologie, Werbepsychologie				

	und Wirtschaftsinformatik: - Virtuelle Gruppen- und Teamkommunikation - Beeinflussung von Online-Kaufentscheidungen Cyberkriminalität und IT-Sicherheit: - Psychologische Aspekte in forensischen Ermittlungen - Die Rolle menschlichen Verhaltens in sicherheitssensitiven Bereichen - Social Engineering – Grundlagen sozialer Manipulationstechniken und IT-Sicherheit - Human Factor in Cybersecurity Methodik: Neuro- und biopsychologische Grundlagen menschl. Verhaltens im Cyberspace Forschungsmethoden Cyberpsychologie (Forschungsdesigns, Experimente) - Avatare, virtuelle Agenten, human-robot-interaction
	Empfohlene Literaturangaben: Attrill-Smith, A., Fullwood, C., Keep, M., & Kuss, D. J. (Eds.). (2019). The Oxford Handbook of Cyberpsychology. Oxford University Press. Edgar, T.W., & Manz, D.O. (2017). Research Methods for Cybersecurity. Elsevier: Cambridge.
5	**Teilnahmevoraussetzungen:** Keine über die Studien- und Prüfungsordnung hinausgehenden Voraussetzungen.
6	**Prüfungsformen***:* Schriftliche Prüfung (K60)
7	***Voraussetzungen für die Vergabe von Kreditpunkten:*** Bestandene Prüfung
8	***Verwendbarkeit des Moduls:*** Advanced IT Security M.Sc., Business and Security Analytics M.Sc., Systems Engineering M.Eng. (Für SE-Studieremde ergibt sich durch das Belegen des Moduls ggf. ein höherer Workload als in StuPO vorgesehen)
9	***Modulverantwortliche(r):*** Prof. Dr. Stefan Sütterlin Dozent: Prof. Dr. Stefan Sütterlin
10	***Optionale Informationen:*** Studiengangsspezifische, zusätzliche Informationen zum Modul

3.1.5 XXXXX – Fortgeschrittene Zahlentheoretische Algorithmen

Studiengang: INF
StuPO-Version: 21.2

Semester: WS 21/22
Letzte Bearbeitung: 15.09.21

<table>
<tr><td colspan="7">Modul: Fortgeschrittene Zahlentheoretische Algorithmen / Advanced Number Theoretic Algorithms</td></tr>
<tr><td colspan="2">Kennnummer
z.B. 15100</td><td>Work-load
180 h</td><td>Modulart
WPM</td><td>Studiensemester
1. + 2. Semester</td><td>Dauer
1 Semester</td><td>Häufigkeit
WS</td></tr>
<tr><td>1</td><td colspan="2">Lehrveranstaltung(en)
Vorlesung Fortgeschrittene Zahlentheoretische Algorithmen
Projekt Fortgeschrittene Zahlentheoretische Algorithmen</td><td>Sprache
Deutsch oder Englisch</td><td>Kontakt-zeit
Vorlesung 2 SWS / 30h
Projekt 2 SWS / 30h</td><td>Selbst-studium
120 h</td><td>Credits (ECTS)
6</td></tr>
<tr><td>2</td><td colspan="6">Lehrform(en) / SWS:
Vorlesung Fortgeschrittene Zahlentheoretische Algorithmen (2 SWS)
Projektarbeit Fortgeschrittene Zahlentheoretische Algorithmen (2 SWS)</td></tr>
<tr><td>3</td><td colspan="6">Lernergebnisse (learning outcomes), Kompetenzen:

Kompetenz Wissen
Die Studierenden verstehen die theoretischen Grundlagen zur Implementierung von Algorithmen zur Faktorisierung, zum Primzahltest, zur Berechnung von diskreten Logarithmen und weiterer relevanter zahlentheoretischer Algorithmen nach dem Stand der Technik. Die Studierenden können auch auf Basis der theoretischen Grundlagen aktuelle Optimierungen für entsprechende Algorithmen verstehen und implementieren. [Wissen, 7]
Kompetenz Fertigkeiten
Die Studierenden können die theoretischen Sicherheitsabschätzungen für die Wahl der Schlüssellängen bei asymmetrischen Algorithmen verstehen und beurteilen. [Instrumentelle Fertigkeiten, 7]
Sozialkompetenz
Die Studierenden können die Wahl von Schlüssellängen für asymmetrische Algorithmen kompetent diskutieren, sowie sich mit Experten darüber austauschen. [Kommunikation, 7]
Selbstständigkeit
Die Studierenden können selbstständig beurteilen, ob Neuerungen in der Kryptoanalyse signifikante Durchbrüche sind, oder nur Detailoptimierungen. [Eigenständigkeit/Verantwortung, 7]</td></tr>
</table>

4	**Inhalte*:*** Vorlesung - Wiederholung der Grundlagen von RSA und ECC - Einführung der zahlentheoretischen Grundlagen: Satz von Euklid, Primzahlsatz, Fundamentalsatz der Zahlentheorie, Kettenbrüche, Integritätsbereiche, Restklassenringe, - Faktorisierungsalgorithmen in Exponentialzeit und Sub-Exponentialzeit - Baby-Step Giant-Step Algorithmus zum Berechnen eines diskreten Logarithmus - Randomisierte Primzahltests - Polynomialzeit-Primzahltest (AKS Algorithmus) - Grundlagen des Zahlenkörpersiebs - Einführung zur Riemannsche Zeta-Funktion, die Riemannsche Vermutung und praktische Auswirkungen Praktikum - Implementierung von mehreren Exponentialzeit-Faktorisierungsalgorithmen - Alternativ Implementierung und Optimierung eines Sub-Exponentialzeitalgorithmus zur Faktorisierung - Alternativ: Implementierung und Optimierung des Baby-Step Giant-Step Algorithmus
	Empfohlene Literaturangaben: Pomerance C., Crandall, R. - Prime Numbers: A Computational Perspective, Springer-Verlag, 2006 Bundschuh, P. - Einführung in die Zahlentheorie, 6. Auflage, Springer-Verlag, 2008
5	**Teilnahmevoraussetzungen:** Grundlagen der Kryptologie, Programmierkenntnisse in Python, C, C++, Java oder einer anderen Hochsprache
6	**Prüfungsformen***:* Wissenschaftliche Ausarbeitung (Hausarbeit) zum Projekt, benotet Referet 20 min., Diskussion, benotet
7	***Voraussetzungen für die Vergabe von Kreditpunkten:*** Ausreichend bewertete Hausarbeit Ausreichend bewertetes Referat
8	***Verwendbarkeit des Moduls:*** Business and Securoity Analytics MSc. Advanced IT Security M.Sc., Systems Engineering M.Eng. (Für SE-Studierende ergibt sich durch das Belegen des Moduls ggf. ein höherer Workload als in StuPO vorgesehen)
9	***Modulverantwortliche(r):*** Prof. Dr. Bernhard Jungk
10	***Optionale Informationen:*** Studiengangsspezifische, zusätzliche Informationen zum Modul

3.1.6 51700 - Incident Response and Malware Defence

Studiengang: INF
StuPO-Version: 21.2

Semester: WS 2021/22
Letzte Bearbeitung: 15.09.21

<table>
<tr><td colspan="7">Modul: Incident Response und Malware Defense</td></tr>
<tr><td colspan="2">Kennnummer
52700</td><td>Workload
180 h</td><td>Modulart
WPM</td><td colspan="2">Studiensemester
1</td><td>Dauer
1 Semester</td><td>Häufigkeit
WS</td></tr>
<tr><td>1</td><td colspan="3">Lehrveranstaltung(en)
Vorlesung Incident Response und Malware Defense
Praktikum Incident Response und Malware Defense</td><td>Sprache
Deutsch</td><td>Kontakt-zeit
60 SWS / 4 h</td><td>Selbst-studium
120 h</td><td>Credits (ECTS)
6</td></tr>
<tr><td>2</td><td colspan="7">Lehrform(en) / SWS:
Vorlesung: 2 SWS
Praktikum: 2 SWS</td></tr>
<tr><td>3</td><td colspan="7">Lernergebnisse (learning outcomes), Kompetenzen:

Kompetenz Wissen
Die Studierenden Kennen die Kategorien der Schadsoftware und deren Auswirkung. [Wissen, 7]

Kompetenz Fertigkeiten
Die Studierenden können Methoden entwickeln und anwenden um IT-Angriffe zu erkennen, zu analysieren, einzudämmen und zu beseitigen [Systemische Fertigkeiten, 7]

Sozialkompetenz
Die Studierenden sind in der Lage, sich mittels dem spezifischen Vokabular auszudrücken, sich verständlich zu machen und andere zu verstehen [Kommunikation, 7]

Selbstständigkeit
Die Studierenden sind in der Lage größere Aufgaben, deren Bearbeitung auch mehrere Tage in Anspruch nimmt, verantwortungsvoll zu erfüllen, realistische Ziele zu definieren und diese konsequent zu verfolgen [Eigenständigkeit/Verantwortung, 7]</td></tr>
<tr><td>4</td><td colspan="7">Inhalte:

1. Der Incident Response Prozess: Preparation, Detection, Analysis, Containment, Recovery, Post Incident Activity
Veranschaulichung und Vertiefung der Phasen an Beispielen
2. Klassifikation und Taxonomie von Incidents
3. Systemsicherung: Sicherung systemwichtiger Daten
4. Spurensicherung: Netzbasierte Spuren (Netzwerkmitschnitte und Netzwerk-Komponenten), Host-basierte Spuren (persistente und nicht persistente Spuren, Arbeitsspeicher)</td></tr>
</table>

	5. Spurenanalyse: Netzbasierte Spuren (Netzwerkmitschnitte, Log-Dateien), Host-basierte Spuren (Arbeitsspeicher, Log-Dateien, Dateisysteme) 6. Detektion: Signatur-basierte und Regel-basierte Methoden 7. Methoden zur Einschränkung der Schadwirkung: Sandbox, Zugriffsschutz, Rechteüberwachung, Firewall, Proxy, Netzwerksegmentierung 8. Wiederherstellung: Backup und Systemsicherung anwenden 9. Statische Malware-Analyse: Aufbau der Malware, verwendete Bibliotheken, maliziöse Funktionen und Strukturen 10. Dynamische Malware-Analyse: Wirkungsweise der Malware, Schadwirkung lokalisieren 11. Reporting zur Malware-Analyse: Wirkungsweise, Schadenspotential, potentielle Quellen 12. Reporting zum Incident Response-Prozess 13. Post Incident Aktivitäten: Maßnahmen zur Verbesserung der Sicherheit treffen; Training von Incidents Beispiele für Projekte • Aufsetzen einer Signaturbasierten Detektion in einem System. Angriff auf das System. Incident behandeln • Aufsetzen eines Systems mit Schwachstellen (z. B. offene USB-Anschlüsse oder Mail-Clients ohne Makrovirenschutz); Eintragen einer Malware; Incident Response Prozess ausführen • Entwicklung einer Malware, die vermutete Systemschwächen ausnutzt (z. B. Keylogger, DLL-Injektor); Erproben der Malware an einem System mit Malware-Schutz; Incident Respons anwenden
	Empfohlene Literaturangaben: Alan J White (Autor), Ben Clark: Blue Team Field Manual. Create Space Independent Publishing Platform (2017) Gerard Johansen: Digital Forensics and Incident Response.Packt (2012 Johansen, Gerard. Digital Forensics and Incident Response: A practical guide to deploying digital forensic techniques in response to cyber security incidents (Kindle-Positionen14-15). Packt Publishing. Kindle-Version. Cameron H. Malin, Eoghan Casey, James M. Aquilina: Malware Forensics Guide for Windows Systems, Digital Forensics Field Guides. Elsevier (2012) Weitere Literatur, insbesondere aktuelle wissenschaftliche Artikel, werden in der Vorlesung bekannt gegeben.
5	**Teilnahmevoraussetzungen:** Die Studierenden besitzen Kenntnisse, Fertigkeiten und Erfahrungen in • Betriebssysteme • Netzwerke • Netzwerksicherheit • Programmierung in einer Hochsprache und einer Skriptsprache
6	**Prüfungsformen***:* Referat 20 min. mit Ausarbeitung, benotet Praktische Arbeit mit Präsentation 20 min. und Handout, benotet
7	***Voraussetzungen für die Vergabe von Kreditpunkten:*** Bestandenes Referat und bestandene Praktische Arbeit
8	***Verwendbarkeit des Moduls:*** Business and Security Analytics, Advanced ITS

9	***Modulverantwortliche(r):*** Prof. Dr. Rieger Dozenten: Prof. Dr. Rieger
10	***Optionale Informationen:*** Studiengangsspezifische, zusätzliche Informationen zum Modul

3.1.7 XXXXX - Post-Quantum Cryptography and Quantum Key Distribution

Studiengang: INF
StuPO-Version:.21.2

Semester: WS 2021/22
Letzte Bearbeitung: 18.03.21

<table>
<tr><td colspan="8">Modul: Post-Quantum Cryptography and Quantum Key Distribution</td></tr>
<tr><td colspan="2">Kennnummer
XXXX</td><td>Work-load
180 h</td><td>Modulart
WPM</td><td colspan="2">Studiensemester
1. Semester</td><td>Dauer
1 Semester</td><td>Häufigkeit
WS</td></tr>
<tr><td>1</td><td colspan="3">Lehrveranstaltung(en)
a. Vorlesung, Praktikum Post-Quantum Cryptography
b. Vorlesung Quantum Key Distribution</td><td>Sprache
Englisch (Literatur-studium in Deutsch und Englisch erforderlich)</td><td>Kontakt-zeit
4 SWS / 60 h</td><td>Selbst-studium
120 h</td><td>Credits (ECTS)
6</td></tr>
<tr><td>2</td><td colspan="7">Lehrform(en) / SWS:
Vorlesung, Praktikum Post-Quantum Cryptography: 3 SWS
Vorlesung Quantum Key Distribution: 1 SWS</td></tr>
<tr><td>3</td><td colspan="7">Lernergebnisse (learning outcomes), Kompetenzen:

Kompetenz Wissen
Die Studierenden können die Gefahren von Quantencomputern für etablierte kryptographische Verfahren erklären und quantensichere Verfahren aufzählen, die nicht betroffen sind. [Wissen, 7]

Die Studierenden können Funktionsweise, Voraussetzungen und Vor- und Nachteile von Quantum Key Distribution aufzählen. [Wissen, 7]

Kompetenz Fertigkeiten
Die Studierenden können quantensichere kryptographische Verfahren für eine Anwendung auswählen und implementieren. [Instrumentelle Fertigkeiten, 7]

Die Studierenden können die Eignung von Quantum Key Distribution für eine Anwendung bewerten. [Beurteilungsfähigkeit, 7]

Sozialkompetenz
Die Studierenden können sich auf Expertenebene mit der Fachcommunity über Post-Quatum Cryptography und Quantum Key Distribution unterhalten, Erkenntnisse und Methoden diskutieren und ihr Expertenwissen auch Fachabteilungen vermitteln [Kommunikation, 7]

Die Studierenden können mögliche gesellschaftliche Auswirkungen von aktuellen und neuen Entwicklungen im Quantencomputing für die IT-Sicherheit erkennen, bewerten und mit Laien- und Fachpublikum diskutieren. [Kommunikation, 7]

Selbstständigkeit
Die Studierenden können neue Anwendungen für Post-Quatum Cryptography und Quantum Key Distribution selbstständig identifizieren und erforschen sowie mit der Fachcommunity diskutieren. [Eigenständigkeit/Verantwortung, 7]</td></tr>
</table>

	Die Studierenden können neue Aufgabenstellungen und Probleme aus den Bereichen Post-Quatum Cryptography und Quantum Key Distribution selbstständig anhand der aktuellen Forschungsergebnisse erarbeiten. [Eigenständigkeit/Verantwortung, 7]
4	**Inhalte*:*** Vorlesung, Praktikum Post-Quantum Cryptography: • Auffrischung relevanter Grundlagen der Kryptologie, IT Sicherheit und Mathematik • Einführung in Quantum Computing • Gefahren durch Quantencomputer für etablierte Verschlüsselungsverfahren • Prinzipien für Post-Quantum Cryptography • Implementierung konkreter Post-Quatum-Verschlüsselungsverfahren Vorlesung Quantum Key Distribution: • Auffrischung relevanter Grundlagen der Kryptologie und IT Sicherheit • Grundlagen der Quantenmechanik • Quantum Key Distribution • Angriffsszenarien
	Empfohlene Literaturangaben: Daniel J. Bernstein, Johannes Buchmann, Erik Dahmen (ed.). *Post-quantum cryptography.* Springer, Berlin, 2009. ISBN 978-3-540-88701-0 Ramona Wolf. *Quantum Key Distribution*. Springer International Publishing, 2021. ISBN 978-3-030-73990-4
5	**Teilnahmevoraussetzungen:** Grundlagen der Kryptologie (insbesondere Public Key Cryptography), IT-Sicherheit, Programmierkenntnisse
6	**Prüfungsformen***:* Wissenschaftliche Ausarbeitung inkl. Kurzpräsentation, benotet Referat 20 min., Diskussion, benotet
7	**Voraussetzungen für die Vergabe von Kreditpunkten:** Ausreichend bewertete Ausarbeitung Ausreichend bewertetes Referat
8	**Verwendbarkeit des Moduls:** Advanced IT Security M.Sc., Business and Security Analytics M.Sc., Systems Engineering M.Eng. (Für SE-Studieremde ergibt sich durch das Belegen des Moduls ggf. ein höherer Workload als in StuPO vorgesehen)
9	**Modulverantwortliche(r):** Prof. Dr. Henrich.
10	**Optionale Informationen:** Studiengangsspezifische, zusätzliche Informationen zum Modul

3.1.8 51400 – Semantic Web

Studiengang: INF
StuPO-Version: 21.2

Semester: WS 2021/22
Letzte Bearbeitung: 15.09.21

<table>
<tr><td colspan="8">Modul: Semantic Web</td></tr>
<tr><td colspan="2">Kennnummer
51400</td><td>Workload
180 h</td><td>Modulart
WPM</td><td colspan="2">Studiensemester
1</td><td>Dauer
1</td><td>Häufigkeit
WS</td></tr>
<tr><td>1</td><td colspan="3">Lehrveranstaltung(en)
a. 51405 Semantic Web
b. 51420 Proj. Semantic Web</td><td>Sprache
a.,b., deutsch oder englisch</td><td>Kontakt-zeit
4 SWS / a. 30 h b. 30 h</td><td>Selbst-studium
120 h</td><td>Credits (ECTS)
6</td></tr>
<tr><td>2</td><td colspan="7">Lehrform(en) / SWS:
a. Vorlesung, b. Projektarbeit (4 SWS)</td></tr>
<tr><td>3</td><td colspan="7">Lernergebnisse (learning outcomes), Kompetenzen:

Kompetenz Wissen
Vertieftes verstehen formaler Logiken und Reasoning-Aufgaben [Wissen, 7]
Vertieftes Verstehen von Semantic Web -Technologien als Instrument für interoperable Wissensbeschreibung [Wissen, 7]

Kompetenz Fertigkeiten
Die Studierenden können Ontologien mit Hilfe von Tools wie Editoren und Reasoner entwickeln und Anwenden [Instrumentelle Fertigkeiten, 6]

Die Studierenden können Wissensstrukturen von komplexen Wissensdomains analysieren und formal beschreiben [Systemische Fertigkeiten, 7]

Sozialkompetenz
Die Studierenden sind in der Lage komplexe Formalismen zu kommunizieren und Diskussion auf Grundlage der Formalismen und mit Anwendung des formallogischen Vokabular zu führen [Kommunikation, 7]

Selbstständigkeit
Die Studierenden sind in der Lage, komplexe Fragestellungen selbständig zu bearbeiten und den eigenen Fortschritt adäquat zu bemessen.
[Lernkompetenz, 7]</td></tr>
<tr><td>4</td><td colspan="7">Inhalte:
Die Grundlagen:
- Definition und Begriffsklärung
- Security Analytics Use Cases
- Data Sourcess und Methoden der Datensammlung
- Real time Data Harvesting
- Anwendung der Security Analytics Ergebnissen und ihr Impact
- Basic Security Analytics Costs
- Advanced persistent threats
- Security Analytics und Digitale Forensics</td></tr>
</table>

	Security Analytics Tools and Services, u.a.: - Blue Coat Security Analytics Platform, - Lancope Stealth Watch System - JuniperNetworks JSA Series Secure Analytics - EMC RSASecurity Analytics NetWitness - FireEye Threat Analytics Platform - Arbor Networks Security Analytics - Click Security Click Commander - Hexis Cyber Solutions' NeatBeat MON - Sumo Logics' cloud service. - Security Onion - Splunk - Elastic Stack
	Empfohlene Literaturangaben: Lehto, Martti, and Pekka Neittaanmäki, eds. Cyber security: Analytics, technology and automation. Vol. 78. Springer, 2015. Talabis, Mark, et al. Information Security Analytics: Finding Security Insights, Patterns, and Anomalies in Big Data. Syngress, 2014. THOMAS, TONY P. VIJAYARAGHAVAN, Athira P. Vijayaraghavan, and Sabu Emmanuel. MACHINE LEARNING APPROACHES IN CYBER SECURITY ANALYTICS. SPRINGER VERLAG, SINGAPOR, 2020.
5	**Teilnahmevoraussetzungen:** Kenntnisse in IT Security (DQR 6), Praktische Fertigkeiten in Netzwerken und Programmierung (DQR 6)
6	**Prüfungsformen***:* Klausur 90 Min. (Modulprüfung)
7	***Voraussetzungen für die Vergabe von Kreditpunkten:*** Bestandene Klausur
8	***Verwendbarkeit des Moduls:*** Advanced IT Security M.Sc., Business and Security Analytics M.Sc., Systems Engineering M.Eng.(Für SE-Studieremde ergibt sich durch das Belegen des Moduls ggf. ein höherer Workload als in StuPO vorgesehen)
9	***Modulverantwortliche(r):*** Prof. Dr. German Nemirovski
10	***Optionale Informationen:*** Studiengangsspezifische, zusätzliche Informationen zum Modul

3.1.9 XXXXX – Tutorials

Studiengang: INF
StuPO-Version: 21.2

Semester: WS 2021/22
Letzte Bearbeitung: 15.09.21

<table>
<tr><td colspan="7">Modul: Tutorials</td></tr>
<tr><td colspan="2">Kennnummer
XXXX</td><td>Workload
90 h</td><td>Modulart
WPM</td><td colspan="2">Studiensemester
1, 2</td><td>Dauer
1</td><td>Häufigkeit
WS</td></tr>
<tr><td>1</td><td colspan="3">Lehrveranstaltung(en)
a. Tutorial
b. Seminar Didaktik der Informatik</td><td>Sprache
a.,b., deutsch oder englisch</td><td>Kontakt-zeit
2 SWS / 30</td><td>Selbst-studium
60 h</td><td>Credits (ECTS)
3</td></tr>
<tr><td>2</td><td colspan="7">Lehrform(en) / SWS:
a. Tutorial 1,5 SWS,
b. Seminar Didaktik der Informatik, 0,5 SWS</td></tr>
<tr><td>3</td><td colspan="7">Lernergebnisse (learning outcomes), Kompetenzen:

Kompetenz Wissen
Die Studierende kennen und verstehen die Grundsätze des Wissensvermittlung und sind insbesondere mit den didaktischen Ansätzen in den MINT-Disziplinen vertraut. [Wissen, 7]

Kompetenz Fertigkeiten
Die Studierenden können für sich vertraute Inhalte vertiefen, diese in angemessener Zeit geeignet strukturieren, didaktisch aufbereiten, und an die betreuten Gruppen weitergeben. [Systemische Fertigkeiten, 7]

Sozialkompetenz
Die Studierenden sind in der Lage komplexe sowie abstrakte und formal dargestellte Inhalte zu kommunizieren und eine Diskussion auf Grundlage der Inhalte zu führen. [Kommunikation, 7]

Selbstständigkeit
Die Studierende sind in der Lage, in der Fachliteratur Forschungsansätze selbständig zu suchen, diese zu verstehen und verständlich zu kommunizieren. [Lernkompetenz, 7]</td></tr>
<tr><td>4</td><td colspan="7">Inhalte:
- Unterrichtsmethoden im Kontext didaktischer Theorie
- Einsatz von Unterrichtsmethoden in der Präsenzlehre
- Einsatz von Unterrichtsmethoden in der Distanzlehre
- Beispiele von Lehr/Lern-Methoden im Informatikunterricht
- Conceptmapping
- Entdeckendes Lernen
- Experimentmethode
- Fallstudie</td></tr>
</table>

	- Modellmethode - Planspiel
	Empfohlene Literaturangaben: A. Zendler. Unterrichtsmethoden für den Informatikunterricht: Mit praktischen Beispielen für prozess- und ergebnisorientiertes Lehren. Springer Vieweg; 1. Aufl. 2018 Edition (18. März 2018). ISBN 3658206748 E. Modrow, K. Strecker, Didaktik der Informatik (De Gruyter Studium). De Gruyter Oldenbourg; 1. Edition (Juni 2016), ISBN 9783486716221.
5	**Teilnahmevoraussetzungen:** Bachelor Abschluss
6	**Prüfungsformen***:* Referat 25 Min.
7	***Voraussetzungen für die Vergabe von Kreditpunkten:*** Bestandenes Referat
8	***Verwendbarkeit des Moduls:*** Advanced IT Security M.Sc., Business and Security Analytics M.Sc., Systems Engineering M.Eng. (Für SE-Studieremde ergibt sich durch das Belegen des Moduls ggf. ein höherer Workload als in StuPO vorgesehen)
9	***Modulverantwortliche(r):*** Prof. Dr. German Nemirovski
10	***Optionale Informationen:*** Studiengangsspezifische, zusätzliche Informationen zum Modul

3.2 Sommersemester

3.2.1 52600 – Advanced Network and Internet Security

Studiengang: Advanced IT Security M.Sc. **Semester**: WS 2021/22
StuPO-Version: 21.2 **Letzte Bearbeitung**: 15.09.21

<table>
<tr><td colspan="7">Modul: Advanced Network and Internet Security (ANIS)</td></tr>
<tr><td colspan="2">Kennnummer
52600</td><td>Workload
180 h</td><td>Modulart
WPM</td><td>Studiensemester
2</td><td>Dauer
1 Semester</td><td>Häufigkeit
WS und SS</td></tr>
<tr><td>1</td><td colspan="2">Lehrveranstaltung(en)
Vorlesung, Seminar, Projekt</td><td>Sprache
Englisch</td><td>Kontakt-zeit
4 SWS / 60 h</td><td>Selbst-studium
120 h</td><td>Credits (ECTS)
6</td></tr>
<tr><td>2</td><td colspan="6">Lehrform(en) / SWS:
Vorlesung: 1 SWS
Seminar: 1,5 SWS
Projekt: 1,5 SWS</td></tr>
<tr><td>3</td><td colspan="6">Lernergebnisse (learning outcomes), Kompetenzen:

Kompetenz Wissen
Die Studierenden kennen den aktuellen Forschungsstand ausgewählter Forschungsbereiche in der Netzwerksicherheit [Wissen, 7]
Kompetenz Fertigkeiten
Die Studierenden können Forschungsfragestellungen der Netzwerksicherheit mit geeigneten Mechanismen und Methoden in Verbindung setzen und diese zur Bearbeitung der Fragestellung anwenden [Instrumentelle Fertigkeiten, 7]

Die Studierenden können eine Forschungsfragestellung bearbeiten und die erzielten Ergebnisse adäquat aufbereiten und präsentieren. [Systemische Fertigkeiten, 7]
Sozialkompetenz
Die Studierenden sind in der Lage die Ergebnisse ihrer Tätigkeit im Bereich Network Security auf einem Master-Niveau einem fachkundigen Experten zu erläutern. [Kommunikation, 7]
Selbstständigkeit
Die Studierenden können im Rahmen einer eigenständigen Arbeit neue Systeme im Bereich Netzwerksicherheit entwickeln und bestehende Systeme bewerten erweitern und analysieren [Eigenständigkeit/Verantwortung, 7]</td></tr>
<tr><td>4</td><td colspan="6">Inhalte:
Die Vorlesung gliedert sich in drei Teile auf, die z.T. zeitlich überlappend durchgeführt werden:
- Wiederholung und Vertiefung der Grundlagen und fortgeschrittenen Aspekte der Netzwerksicherheit. Dieser Teil wird im Rahmen einer Vorlesung absolviert und dient dazu, Informatik-Studierenden ohne spezifischen IT Security-Hintergrund die Grundlagen für die Bearbeitung des Referats und des Projekts zu vermitteln.</td></tr>
</table>

	- Ausarbeitung eines Referats über ein aktuelles Thema der Netzwerksicherheit (basierend auf aktuellen Konferenz- oder Journal Veröffentlichungen aus dem Bereich der Netzwerksicherheit). Dieser Teil dient dazu, an einem konkreten Beispiel den Aufbau einer wissenschaftlichen Arbeit zu erarbeiten und diese zu bewerten. Die Referate werden im Peer-Review Prozess von jeweils zwei Kommilitonen korrigiert und ähnlich zu einem Konferenzformat gehalten (1-tägige Blockveranstaltung). - Bearbeitung eines eigenen Projekts zu einer ausgewählten Forschungsfragestellung aus dem Bereich der Netzwerk- und Internetsicherheit. Dabei werden sowohl Ingenieursmethoden als auch analytische Methoden verwendet um die Fragestellung zu beantworten. Die Projektbearbeitung schließt mit einem Vortrag über die Ergebnisse ab (erneut im Konferenz-Format als Blockveranstaltung). Hier sollen selbständig wissenschaftliche Fragestellungen bearbeitet werden. Beispiele für die zu behandelnden Themen • Sicherheit moderner Kommunikationsprotokolle (HTTP/2, QUIC, P2P Protokolle, etc.) • Aktuelle Angriffe gegen Kommunikationsprotokolle • Protokolle zur Erreichung spezifischer Sicherheitsziele (Vertraulichkeit, Integrität, Verfügbarkeit, Anonymität, Pseudonymität) • Authentifikations- und Authorisierungsprotokolle • Sicherheit im industriellen Umfeld (Fertigung, Steuerung) • Analyse von Kommunikationsdaten zur Erkennung von Sicherheitsproblemen • Analyse verschlüsselter Verbindungen zur Klassifikation von Verkehr • Analyse von Log- Einträgen und anderweitig erfassten Ereignissen zur Erkennung und Klassifikation von Angriffen
	Empfohlene Literaturangaben: R. Anderson, Security Engineering, Wiley, 2009G. Schäfer, M. Roßberg, Netzssicherheit, dpunkt.verlag, 2014 Ausgewählte Literatur bekannter Top-Tier Konferenzen im Bereich Sicherheit und Netzwerksicherheit z.B. ACM CCS, Usenix Security, Defcon, Balckhat, etc.
5	**Teilnahmevoraussetzungen:** Bestandenes Referat
6	**Prüfungsformen***:* Referat 20 min. mit Ausarbeitung, benotet Laborarbeit, unbenotet
7	***Voraussetzungen für die Vergabe von Kreditpunkten:*** Bestandenes Referat und bestandene Laborarbeit
8	***Verwendbarkeit des Moduls:*** Systems Engineering M.Eng., Advanced IT Security M.Sc., Business and Security Analytics M.Sc.
9	***Modulverantwortliche(r):*** Prof. Dr. Christian Henrich Dozenten: Prof. Dr. Christian Henrich
10	***Optionale Informationen:*** Studiengangsspezifische, zusätzliche Informationen zum Modul

3.2.2 52300 - Distributed Enterprise Applications

Studiengang: Advanced IT Security M.Sc. **Semester**: WS 2021/22
StuPO-Version: 21.2 **Letzte Bearbeitung**: 15.09.21

<table>
<tr><td colspan="7">Modul: Distributed Enterprise Applications</td></tr>
<tr><td colspan="2">Kennnummer
51300</td><td>Workload
180 h</td><td>Modulart
WPM</td><td colspan="2">Studiensemester
2</td><td>Dauer
1 Semester</td><td>Häufigkeit
WS und SS</td></tr>
<tr><td>1</td><td colspan="3">Lehrveranstaltung(en)
Vorlesung Distributed Enterprise Applications
Projekt Distributed Enterprise Applications</td><td>Sprache
Deutsch, bei Bedarf Englisch (muss vor Semesterbeginn geäußert werden)</td><td>Kontakt-zeit
4 SWS / 60 h</td><td>Selbst-studium
120 h</td><td>Credits (ECTS)
6</td></tr>
<tr><td>2</td><td colspan="7">Lehrform(en) / SWS:
Vorlesung: 2 SWS
Übungen: 2 SWS</td></tr>
<tr><td>3</td><td colspan="7">Lernergebnisse (learning outcomes), Kompetenzen:

Kompetenz Wissen
Die Studierenden kennen
die Bedeutung und Notwendigkeit der Betrachtung und Entwicklung von Software-Architekturen für komplexe und vor allem verteilter Software-Produkte,
Architekturmuster zur Implementierung verteilter Anwendungen,
Techniken zur Implementierung komponentenbasierter Software-Entwicklung auf Basis von Applikationsservern
[Wissen, 7]</td></tr>
<tr><td></td><td colspan="7">Kompetenz Fertigkeiten
Die Studierenden sind in der Lage
Komponenten im Sinne einer Applikationsserver-orientierten Architektur zu entwerfen und zu implementieren,
verteilte Transaktionsarchitekturen zu entwerfen und zu implementieren,
verschiedene Frontend- und Backend-Architekturen zu entwickeln und zu implementieren [Instrumentelle Fertigkeiten, 7]</td></tr>
<tr><td></td><td colspan="7">Sozialkompetenz
Nicht relevant</td></tr>
<tr><td></td><td colspan="7">Selbstständigkeit
Die Studierenden sind fähig selbständig komplexere Aufgabenstellungen im Sinne einer komponentenorientierten Software-Architektur zu modellieren und umzusetzen
[Eigenständigkeit/Verantwortung, 7]</td></tr>
</table>

4	**Inhalte*:*** Aufbau eines komponentenorientierten, TP-Monitor-basierten Applikationsservers Implementierung komplexer (Datenbank-) Anwendungen auf Basis der Java Persistence Architektur
	Empfohlene Literaturangaben: https://www.tutorialspoint.com/software_architecture_design/component_based_architecture.htm Syperski, C.: Component Software: Beyond Object-Oriented Programming (Addison-Wesley Component Software), 2011 Andresen, A.: Komponentenbasierte Softwareentwicklung mit MDA, UML 2 und XML. Hanser, 2. Auflage, 2004,ISBN-13: 978-3446229150 Eilebrecht, K., Starke, G.: Patterns kompakt: Entwurfsmuster für effektive Software-Entwicklung. Spektrum Akademischer Verlag, 3. Auflage, 2010, ISBN-13: 978-3827425256 Erl, T.: SOA: Design Patterns. Prentice Hall International, 2008, ISBN-13: 978-0136135166Erl, T.: SOA: Entwurfsprinzipien für service-orientierte Architektur. Addison-Wesley, 2008, ISBN-13: 978-3827326515 Fowler, M. et al.: Patterns of Enterprise Application Architecture. mitp, 2003, ISBN-13: 978-3826613784 Gamma et al.: Entwurfsmuster: Elemente wiederverwendbarer objektorientierter Software. Addison-Wesley, Neuauflage, 2010, ISBN-13: 978-3827330437 Gharbi, M.: Basiswissen für Softwarearchitekten: Aus- und Weiterbildung nach iSAQB-Standard zum Certified Professional for Software Architecture - Foundation Level. dpunkt.verlag, 1. Auflage, 2012, ISBN-13: 978-3898647915 Wieken, J.-H.: SQL -Einstieg für Fortgeschrittene, Addison Wesley, 2008 Kroenke, D.M.; Auer, D.: Database Processing, Prentice Hall, 2010 Wehr, H., Müller, B.: Java Persistence API mit Hibernate, Addison Wesley, 2007 Bauer, Chr.; King, G.: Hibernate in Action. Manning Pub., 2004 http://jbossts.blogspot.de/2014/01/narayana-transaction-analyser-100alpha1.html http://www.redhat.com/products/jbossenterprisemiddleware/data-grid/
5	**Teilnahmevoraussetzungen:** Teilnahmevoraussetzungen: Zulassung zu einem Master-Studiengang an der HS Albstadt Sigmaringen
6	**Prüfungsformen***:* Mündliche Prüfung 20 min., benotet Praktische Arbeit, unbenotet
7	***Voraussetzungen für die Vergabe von Kreditpunkten:*** Erfolgreiche Teilnahme an der mündlichen Prüfung
8	***Verwendbarkeit des Moduls:*** Systems Engineering M.Eng., Advanced IT Security M.Sc., Business and Security Analytics M.Sc.
9	***Modulverantwortliche(r):*** Prof. Dr. J. Röhrle Dozenten: Prof. Dr. J. Röhrle
10	***Optionale Informationen:*** Studiengangsspezifische, zusätzliche Informationen zum Modul

3.2.3 XXXXX - File System Forensics

Studiengang: Advanced Internet Security M.Sc. **Semester**: WS 2021/22

StuPO-Version: 21.2 **Letzte Bearbeitung**: 16.03.21

Modul: Dateisystemforensik / File System Forensics					
52600	**Workload** 180 h	**Modulart** WPM	**Studiensemester** 2	**Dauer** 1 Semester	**Häufigkeit** SoSe

1	**Lehrveranstaltung(en)** Vorlesung Dateisystemforensik Praktikum Dateisystem-forensik	**Sprache** Deutsch oder Englisch (Literaturstudium in Deutsch und Englisch erforderlich)	**Kontakt-zeit** 4 SWS / 60 h	**Selbst-studium** 120 h	**Credits (ECTS)** 6
2	**Lehrform(en) / SWS:** Vorlesung, Übungen, Seminar: 2 SWS Praktikum: 2 SWS				
3	Lernergebnisse (learning outcomes), Kompetenzen: Kompetenz Wissen Die Studierenden verfügen über ein breites Wissen über die technischen Grundlagen des Aufbaus von Dateisystemen. [Wissen, 7] Die Studierenden verfügen über ein tiefes Wissen über ausgewählte und relevante Dateisysteme. [Wissen, 7] Kompetenz Fertigkeiten Die Studierenden können Werkzeuge nutzen um Partitions- und Dateisysteme forensisch zu analysieren. [Instrumentelle Fertigkeiten, 7] Die Studierenden können den Aufbau von Dateisystemen vergleichen und somit auch unbekannte Dateisysteme einordnen. [Beurteilungsfähigkeit, 7] Sozialkompetenz Studierende können sich auf tiefer Expertenebene mit der Fachcommunity unterhalten, Erkenntnisse und Methoden diskutieren und Ergebnisse für forensisches Zielpublikum (z.B. Juristen) darstellen. [Kommunikation, 7] Selbstständigkeit Studierende können selbstständig Dateisysteme analysieren, die Ergebnisse analysieren und das Ergebnis zielgruppengerecht darstellen. [Eigenständigkeit/Verantwortung, 7]				
4	**Inhalte*:*** Vorlesung, Praktikum • Auffrischung relevanter Grundlagen der IT-Sicherheit und der digitalen Forensik • Technische Grundlagen und Sicherungsprozess • Grundlagen ausgewählter Partitionssysteme (z.B. MBR) • Grundlagen der Dateisystemforensik • Detaillierte Betrachtung ausgewählter Dateisysteme (z.B. NTFS und FAT) • Weitere aktuelle Inhalte aus dem Bereich der Dateisystemforensik				

	Empfohlene Literaturangaben: Carrier, Brian (2005). File System Forensic Analysis. Boston/USA: Addison Wesley. Casey, Eoghan (2011). Digital Evidence and Computer Crime. London: Elsevier/AP. Dewald, Andreas und Felix Freiling (2015). Forensische Informatik. Norderstedt: BoD (Books on Demand). Weitere Literatur wird in der Vorlesung vorgestellt.
5	**Teilnahmevoraussetzungen:** Grundlagen IT Sicherheit und Digitaler Forensik, Programmierung in einer Skriptsprache
6	**Prüfungsformen***:* Klausur 90 min., benotet Laborarbeit, unbenotet
7	**Voraussetzungen für die Vergabe von Kreditpunkten:** Mindestens ausreichend bewertete Klausur Erfolgreiche Teilnahme am Praktikum
8	**Verwendbarkeit des Moduls:** Systems Engineering M.Eng., Advanced IT Security M.Sc., Business and Security Analytics M.Sc.
9	**Modulverantwortliche(r):** Prof. Dr. Fein Prof. Morgenstern Dozenten: Prof. Morgenstern, Prof. Dr. Fein
10	**Optionale Informationen:** Studiengangsspezifische, zusätzliche Informationen zum Modul

3.2.4 52400 – Financial Risks and Financial Management

Studiengang: Advanced IT Security M.Sc. **Semester**: WS 2021/22
StuPO-Version: 21.2 **Letzte Bearbeitung**: 15.09.21

<table>
<tr><td colspan="8">Modul: Financial Risks & Financial Management</td></tr>
<tr><td colspan="2">Kennnummer
52400</td><td>Workload
180 h</td><td>Modulart
WPM</td><td colspan="2">Studiensemester
2</td><td>Dauer
1 Semester</td><td>Häufigkeit
WS und SS</td></tr>
<tr><td>1</td><td colspan="2">Lehrveranstaltung(en)
Vorlesung; Übungen & Fallstudien Financial Risks & Financial Management</td><td>Sprache
Deutsch und Englisch (deutsches und englisches Literatur-studium erforderlich)</td><td>Kontakt-zeit
4 SWS / 60 h</td><td>Selbst-studium
120 h</td><td>Credits (ECTS)
6</td></tr>
<tr><td>2</td><td colspan="7">Lehrform(en) / SWS:
Vorlesung: 2 SWS
Übungen / Fallstudien: 2 SWS</td></tr>
<tr><td>3</td><td colspan="7">Lernergebnisse (learning outcomes), Kompetenzen:

Kompetenz Wissen
Die Studierenden:
• sind mit zentralen Aspekten des Kapitalstrukturmanagements und der Ableitung der relevanten Kapitalkosten vertraut
• kennen die Portfoliotheorie und das CAPM und deren Anwendungsgebiete im Risikomanagement und der Kapitalkostenableitung
• kennen die wesentlichen Verfahren der Unternehmens- sowie der Anleihebewertung
• sind mit den zentralen finanzwirtschaftlichen Risiken vertraut und kennen die gängigen Verfahren des Risikomanagements
• kennen in Grundzügen das Wesen von Derivaten und deren Anwendungs-möglichkeiten im Management von finanzwirtschaftlichen Risiken [Wissen, 7]</td></tr>
<tr><td></td><td colspan="7">Kompetenz Fertigkeiten
Die Studierenden:
• können marktgestützt Kapitalkosten von Unternehmen ableiten
• können die gängige Verfahren zur Unternehmensbewertung anwenden und selbständig Unternehmenswerte ableiten
• können Anleihen bewerten
• können die unterschiedlichen finanzwirtschaftlichen Risiken identifizieren und voneinander abgrenzen
• können gängige Verfahren zum Management finanzwirtschaftlicher Risiken (Value at Risk, Hedging mittels Derivaten, etc.) anwenden
[Instrumentelle Fertigkeiten, 7]</td></tr>
</table>

	Sozialkompetenz Die Studierenden können Fallstudien im Team bearbeiten und sind in der Lage die Teams selbst zu organisieren; beherrschen Methoden der Präsentation und Dokumentation und können diese zielgruppenorientiert einsetzen *[Team-/Führungsfähigkeit, 7]* Die Studierenden beherrschen Methoden der Präsentation und Dokumentation und können diese zielgruppenorientiert einsetzen *[Kommunikation, 7]*
	Selbstständigkeit Die Studierenden können im Rahmen von Fallstudien Problemstellungen des Finanz- und Risikomanagements selbständig erkennen, nach Lösungen recherchieren, auf das Wesentliche abstrahieren und in einem gestalteten Prozess Aufgaben bezogen lösen *[Eigenständigkeit/Verantwortung, 7]* Durch die fortlaufende Vertiefung des Stoffes durch die selbständige Bearbeitung von Übungsaufgaben und Fallstudien, sind die Studierenden in der Lage, sich ein realistisches Bild ihrer eigenen Kompetenzentwicklung zu machen und entsprechend darauf zu reagieren. *[Lernkompetenz, 7]*
4	**Inhalte*:*** Grundlagen des Finanzmanagements, Finanzanalyse, Value Management und Unternehmenswert, Fremdkapitalmanagement, Finanzielle Risiken und Risikomanagement.
	Empfohlene Literaturangaben: Becker, H. P.: Investition und Finanzierung –Grundlagen der betrieblichen Finanzwirtschaft, 7. Auflage, Springer Verlag, 2015, Brealey, R. A./ Myers, St. C., 2003, Principles of Corporate Finance, 7th. Ed., New York et. al. (Mc Graw Hill International Ed.), Elton, E., Gruber, M., Brown, S. und Goetzmann,W., 2002, Modern Portfolio Theory and Investment Analysis, 6. Aufl., John Wiley and SonsKruschwitz, L.;Husmann, S.: Finanzierung und Investition, 6. Auflage, Oldenbourg Verlag, 2009Hull, J.C.: Options, Futures, and Other Derivatives, 9th Edition, Pearson, 2015Higgins, R.: Analysis for Financial Management, 10thEdition, McGraw-Hill/Irwin, 2011Perridon, L.; Steiner, M.;Rathgeber, A.: Finanzwirtschaft der Unternehmung, 15. Auflage, Vahlen Verlag, 2009Zantow, R.;Dinauer, J.: Finanzwirtschaft der Unternehmens:Die Grundlagen des modernen Finanzmanagements, 3. Auflage,PearsonStudium, 2011
5	**Teilnahmevoraussetzungen:** Empfohlen: Grundlagen der Investition und Finanzierung, Grundlagen der Statistik
6	**Prüfungsformen***:* Klausur 90 min.
7	***Voraussetzungen für die Vergabe von Kreditpunkten:*** Bestandene Klausur
8	***Verwendbarkeit des Moduls:*** Systems Engineering M.Eng., Advanced IT Security M.Sc., Business and Security Analytics M.Sc.

9	***Modulverantwortliche(r):*** Prof. Dr. Philipp Lindenmayer Dozenten: Prof. Dr. Philipp Lindenmayer
10	***Optionale Informationen:*** Studiengangsspezifische, zusätzliche Informationen zum Modul

3.2.5 XXXXX - Highly Optimized Hardware Cryptography

Studiengang: INF
StuPO-Version: 21.2

Semester: WS 21/22
Letzte Bearbeitung: 15.09.21

<table>
<tr><td colspan="8">Modul: Highly Optimized Hardware Cryptography</td></tr>
<tr><td colspan="2">Kennnummer
z.B. 15100</td><td>Workload
180 h</td><td>Modulart
WPM</td><td>Studiensemester
1</td><td>Dauer
1 Semester</td><td colspan="2">Häufigkeit
SS</td></tr>
<tr><td>1</td><td colspan="2">Lehrveranstaltung(en)
Vorlesung Highly Optimized Hardware Cryptography
Projekt Highly Optimized Hardware Cryptography</td><td>Sprache
Deutsch oder Englisch</td><td>Kontakt-zeit
Vorlesung 2 SWS / 30h
Projekt 2 SWS / 30h</td><td>Selbst-studium
120 h</td><td>Credits (ECTS)
6</td></tr>
<tr><td>2</td><td colspan="6">Lehrform(en) / SWS:
Vorlesung Highly Optimized Hardware Cryptography (2 SWS)
Projekt Highly Optimized Hardware Cryptography (2 SWS)</td></tr>
<tr><td>3</td><td colspan="6">Lernergebnisse (learning outcomes), Kompetenzen:

Kompetenz Wissen
Die Studierenden verstehen verschiedene Optimierungs-Strategien für die effiziente Implementierung von kryptografischen Algorithmen in Hardware. [Wissen, 7]
Kompetenz Fertigkeiten
Die Studierenden können kryptografische Algorithmen effizient in Hardware umsetzen und auf bestimmte Zielvorgaben hin optimieren. [Instrumentelle Fertigkeiten, 7]
Die Studierenden können die Auswirkungen von Optimierungen auf Systeme bzgl. unterschiedlichen Kriterien, wie z.B. Gesamtsystemperformance, Kosten, oder Angriffs-Anfälligkeit beurteilen und geeignete Maßnahmen herleiten und umsetzen. [Beurteilungsfähigkeit, 7]
Sozialkompetenz
Die Studierenden können komplexe Themenfelder der Hardware-Kryptografie mit anderen Experten diskutieren und im Team weiterentwickeln. [Team-/Führungsfähigkeit, 7]
Selbstständigkeit
Die Studierenden können selbstständig und anwendungsorientiert Entscheidungen zur Optimierung komplexer Sachverhalte treffen.
[Eigenständigkeit/Verantwortung, 7]</td></tr>
</table>

4	**Inhalte*:*** Vorlesung - Einführung in die RTL-Programmierung mit VHDL - Grundlagen zur Programmierung von FPGAs und ASICs - Optimierungsstrategien für hochperformante, ressourcensparende, oder energiesparende Implementierungen - Optimierungs-Strategien mit Software/Hardware Co-Design - Anwendung der Optimierungsstrategien für unterschiedliche kryptgrafische Algorithmen - Effiziente Algorithmen für Public Key Kryptografie Projektarbeit - Einführung in die FPGA-Programmierung mit VHDL - Implementierung und Optimierung eines Algorithmus auf einem FPGA - Erprobung unterschiedlicher Optimierungsstrategien --- **Empfohlene Literaturangaben:** Koç, C. K. - Cryptographic Engineering, Springer-Verlag, 2010 Ashenden, J. P. - The Designer's Guide to VHDL, Morgan Kaufmann, 2010
5	**Teilnahmevoraussetzungen:** Grundlagen der Kryptologie, Programmierkenntnisse (C, optional ARM Assembly oder VHDL)
6	**Prüfungsformen***:* Wissenschaftliche Ausarbeitung zur Projektarbeit, benotet Referat 20 min., Diskussion, benotet
7	***Voraussetzungen für die Vergabe von Kreditpunkten:*** Ausreichend bewertete Ausarbeitung Ausreichend bewertetes Referat
8	***Verwendbarkeit des Moduls:*** Advanced IT Security M.Sc., Business and Security Analytics M.Sc.,Systems Engineering M.Eng. (Für SE-Studieremde ergibt sich durch das Belegen des Moduls ggf. ein höherer Workload als in StuPO vorgesehen)
9	***Modulverantwortliche(r):*** Prof. Dr. Bernhard Jungk
10	***Optionale Informationen:*** Studiengangsspezifische, zusätzliche Informationen zum Modul

3.2.6 52500 – Innovation and Transfer Competence

Studiengang: Advanced IT Security M.Sc. **Semester**: WS 2021/22
StuPO-Version: 21.2 **Letzte Bearbeitung**: 15.09.21

<table>
<tr><td colspan="8">Modul: Innovation and Transfer Competence</td></tr>
<tr><td colspan="2">Kennnummer
52500</td><td>Workload
180 h</td><td>Modulart
WPM</td><td colspan="2">Studiensemester
2</td><td>Dauer
1</td><td>Häufigkeit
SS</td></tr>
<tr><td>1</td><td colspan="3">Lehrveranstaltung(en)
a. 52305 In. and Transfer Competence
b. 52320 Proj. In. and Transfer Competence</td><td>Sprache
a.,b., deutsch oder englisch</td><td>Kontakt-zeit
4 SWS / 60 h</td><td>Selbst-studium
120 h</td><td>Credits (ECTS)
6</td></tr>
<tr><td>2</td><td colspan="7">Lehrform(en) / SWS:
a. Vorlesung, Seminar (2 SWS)
b. Projektarbeit (2 SWS)</td></tr>
<tr><td>3</td><td colspan="7">Lernergebnisse (learning outcomes), Kompetenzen:
Kompetenz Wissen
Methoden zur Integration einen betrieblichen Innovationsmangements in bestehende Betriebe [Wissen, 7]
Planungs-, Organisations-und Qualitätsmanagementsmethoden aus Theorie und Praxis [Wissen, 7]

Kompetenz Fertigkeiten
Wissenschaftliche Grundlagen und neuere Forschungsergebnisse erfassen, auf deren praktischen Einsatz hin prüfen, ergänzen und zum Einsatz bringen. [Systemische Fertigkeiten, 7]
Zusammenhänge zwischen diversen Theorien und Konzepten zu sehen, diese zu umfassenderen integrierenden praxisorientierten Konzeptionen weiterzuentwickeln und in konkret entwickelten Anwendungen zum Einsatz zu bringen [Instrumentelle Fertigkeiten, 7]
Geschäftsideen entwickeln, diese bezügliche Realisierbarkeit prüfen und Strategien entwickeln, Forschungsergebnisse zu transferieren und als Innovation umzusetzen [Systemische Fertigkeiten, 7]

Sozialkompetenz
Projekte organisieren, umsetzen, steuern und die Einhaltung nach Gesichtspunkten des Qualitätsmanagements kontrollieren, überwachen. [Team-/Führungsfähigkeit, 7]

Selbstständigkeit
Sind in der Lage, in einem konkurrierendem Kontext eigene Ideen zu reflektieren, diese gegebenfalls anzupassen und durchzusetzen, oder sich Argumenten zu beugen und die Ideen der Wettbewerber zu akzeptieren.
[Eigenständigkeit/Verantwortung, 7]</td></tr>
</table>

4	**Inhalte*:*** Vorlesung: - Ideenmanagement - Betriebliches Innovationsmanagement - Transfer Wissenschaft - Praxis Projekt - Entwicklung eines ausführlichen Geschäftsszenarios, eines Qualitätsmanagementplans und einer Risikoabschätzung - Bestimmung, Suche und Auswahl der einzusetzenden wissenschaftlichen Forschungsergebnisse - Entwicklung einer Vermarktungsstrategie - Durchführen der Organisations-und Qualitätsplanung - Vornahme der Projektplanung (Aufgaben, Netzplan, Meilensteine) und Festlegung der Arbeitsverteilung (Rollen, Verantwortlichkeiten, Mitarbeit, Personalführung) - Leitung und Durchführung des Projekts - Betreiben des Projekt-und Risikomanagements - Durchführung von Produkttest, Endfertigung und Qualitätskontrolle
	Empfohlene Literaturangaben: Al-Laham, Andreas. Organisationales Wissensmanagement: Eine strategische Perspektive. Vahlen, 2016. Mertins, Kai, Ina Kohl, and Ronald Orth. "Ein Referenzmodell für Wissensmanagement." Wissensmanagement im Mittelstand. Springer Gabler, Berlin, Heidelberg, 2016. 31-40. Kamiske, Gerd F., and Jörg-Peter Brauer. Qualitätsmanagement von A-Z: Wichtige Begriffe des Qualitätsmanagements und ihre Bedeutung. Carl Hanser Verlag GmbH Co KG, 2016. Neumann, Alexander. Führungsorientiertes Qualitätsmanagement. Carl Hanser Verlag GmbH Co KG, 2017.
5	**Teilnahmevoraussetzungen:** Wissenschaftliches Arbeiten (DQR 6), Projektmanagement (DQR 5)
6	**Prüfungsformen***:* Praktische Arbeit (benotet) als Modulprüfung
7	***Voraussetzungen für die Vergabe von Kreditpunkten:*** Bestandene Praktische Arbeit
8	***Verwendbarkeit des Moduls:*** Systems Engineering M.Eng., Advanced IT Security M.Sc., Business and Security Analytics M.Sc.
9	***Modulverantwortliche(r):*** Prof. Dr. German Nemirovski
10	***Optionale Informationen:*** Studiengangsspezifische, zusätzliche Informationen zum Modul