Konzept für einen berufsbegleitenden Bachelor-Studiengang Informatik/IT-Sicherheit an der FAU

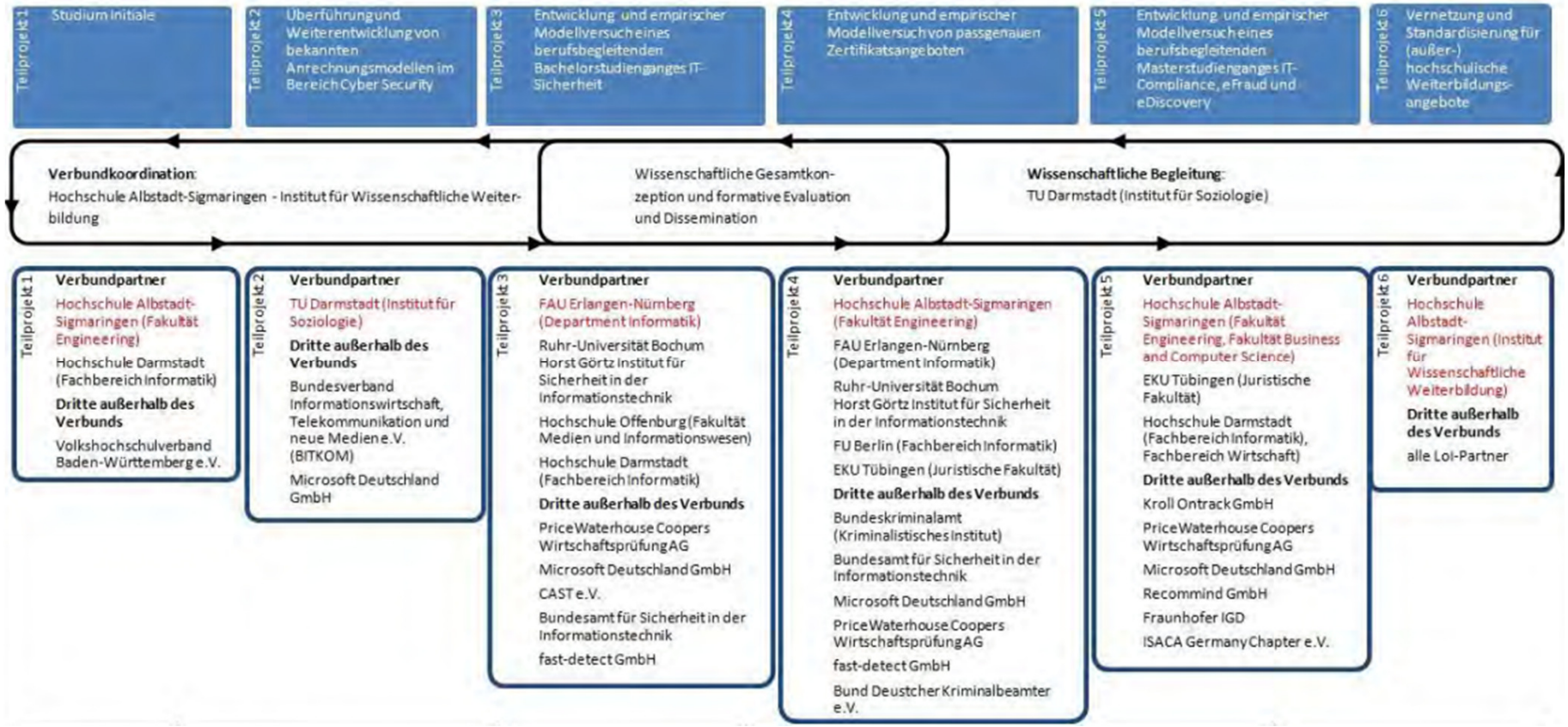
Prof. Dr. Felix Freiling
Dr. Zinaida Benenson
Lehrstuhl für Informatik 1 (IT-Sicherheitsinfrastrukturen)

Stand: 13.12.2011
(Druckoptimierte Version der Folien)

Kontext

- Förderung im Rahmen des **BMBF-Förderprogramms** „Aufstieg durch Bildung“
- Verbundvorhaben „**Open Competence Center for Cyber Security**“ (Open C^3S)
- Verbundprojekt-**Koordinator**:
  - Herr Prof. Dr. Martin Rieger, **Hochschule Albstadt-Sigmaringen**
- Weitere **Partner**:
  - FAU
  - Technische Universität Darmstadt
  - Hochschule Darmstadt
  - Ruhr-Universität Bochum
  - Hochschule Offenburg
  - Freie Universität Berlin
  - Eberhard-Karls-Universität Tübingen
- Gesamtziel: Entwicklung eines hochschuloffenen transdisziplinären **Programms Wissenschaftlicher Weiterbildung** im Sektor Cyber Security
- Zwei Förderphasen: 3,5 Jahre + 2,5 Jahre

Übersicht des Verbundvorhabens



Teilprojekt 3

- FAU ist **Koordinator** von Teilprojekt 3: „Entwicklung eines berufsbegleitenden Bachelorstudiengangs IT-Sicherheit“
  - Designierte Koodinatorin: Dr. Zinaida Benenson (Informatik 1)
- **Kenndaten** (gemäß Akkreditierungsvorgaben):
  - **Teilzeitstudiengang** von **9 Semestern** Dauer. Die Regelstudienzeit orientiert sich an den Bedürfnissen Berufstätiger. Durch Anrechnung kann die Studienzeit verkürzt werden.
  - Der **Gesamt-Workload** beträgt **180 ECTS** (pro Modul i.d.R. 6 ECTS).
    - pro Studiensemester ein Workload von **20 ECTS** nicht überschritten
  - Der Studiengang ist **modularisiert und flexibel**, d.h. die Module werden Studienlevels zugeteilt und können innerhalb dieser in nahezu unabhängiger Reihenfolge und separat studiert werden.
  - Für den Erwerb des Bachelors können auch im Rahmen einer berufspraktischen Tätigkeit erworbene Kompetenzen nach individueller Prüfung im Umfang von maximal 50 % des Studiums **angerechnet** werden.
  - **Studienabschluss**: „Bachelor of Engineering“ (stärker anwendungsorientiert) oder alternativ „Bachelor of Science“
- **Zielgruppe**: IT-Sicherheitsberater, Beschäftigte in Rechenzentren, Sicherheits- oder Ermittlungsbehörden, der Mobilfunkindustrie, Telekommunikationsunternehmen, in der IT-Branche allgemein
  - Sowohl beruflich Qualifizierte ohne Hochschulzugangsberechtigung (sog. Senior High Potentials) gemäß gesetzlichen Vorgaben, als auch alle Personen mit Hochschulzugangsberechtigung

Konzeption

- Studiengang an der FAU
  - Abschluss der FAU
  - Akkreditiert an der FAU
  - Qualitätssicherung primär durch die FAU
    - beteiligte Partner können ggf. in Studien- oder Zulassungskommissionen aufgenommen werden
  - Nicht (notwendigerweise) kapazitätswirksam
    - Weiterbildungsstudiengang
    - Lehrleistung kann im Nebenamt erbracht werden
    - Vorgabe ist Kostendeckung
- Aufnahme pro Jahr: 30 Studierende
  - Beginn des Studiums nur zum Wintersemester
- Module können auch einzeln belegt werden
  - Um noch freie Studienplätze zu belegen
  - Abschluss Hochschulzertifikat
- Weitere beteiligte Partner:
  - Ruhr-Universität: Prof. Jörg Schwenk
  - Hochschule Darmstadt: Prof. Harald Baier
  - Hochschule Offenburg: Prof. Daniel Hammer
  - FAU (assoziiert, d.h. ohne Förderung): Prof. Kimmelmann (Berufspädagogik)
- Kooperationsvertrag regelt Rechte und Pflichten

Lehr- und Betreuungskonzept

- Lehrkonzept ist hybrid:
  - Online-Selbstlernphasen und Präsenzphasen wechseln sich ab im Verhältnis 70:30.
- Das Betreuungskonzept ist zweistufig:
  - Der 1st level support erfolgt durch einen Online-Tutor
  - Der 2nd level support durch den modulverantwortlichen Dozenten.
- Präsenzveranstaltungen:
  - an Wochenenden (alle 4-6 Wochen) und im Block (modul-spezifisch)
  - dienen dem Wissensaustausch und der Diskussion aktueller, praxisrelevanter Problemstellungen, können Gruppen- oder Laborarbeit enthalten
  - Auch die Prüfungen werden in Präsenz durchgeführt
- Online-Phasen:
  - Zentrales Element: der didaktisch aufbereitete Studienbrief
  - Umfangreicher Übungsanteil
  - Lernmanagementsystem StudOn / ILIAS.
  - Web-Conferencing-Werkzeug Adobe Connect

Finanzierung

- Bedarf: 4 Stellen E13 + 0,5 Stellen E10
  - Davon FAU 1 Stelle E13, 0,5 Stellen E10
    - Beitrag **aus eigenen Ressourcen**: Lehrstuhl für Informatik 1 stellt Studiengangskoordinatorin (Dr. Benenson)
  - Bedarf besteht solange Studiengang läuft
  - Ressourcen werden auf Partnerhochschulen abhängig von der Zahl der beigetragenen Module verteilt
- Während der Förderphase (3,5 + 2,5 Jahre) Finanzierung durch das BMBF
- Später Vollkostenfinanzierung über Studiengebühren
  - Kalkulation:
    - ca. 17.500 EUR für das gesamte Studienprogramm.
    - Einzelmodule kosten ca. 1000 EUR.
  - Die Kosten beinhalten u.a. Studienmaterial, Zugang zu Fachliteratur, Nutzung der Lernplattform, Betreuung im Selbststudium, Prüfungsgebühren.
- Geplant: Modellversuch während der Förderphase
  - keine Kosten für Teilnehmer

Curriculum

- Curriculum wird im Rahmen der ersten Förderphase im Detail ausgearbeitet.
  - Es orientiert sich am folgenden Entwurf, der auf drei Säulen basiert.
  - Die Module haben soweit nicht anders angegeben einen Umfang von jeweils 6 ECTS.
  - Die Module werde von den unterschiedlichen Projektpartnern angeboten
    - Die FAU übernimmt 6 der 29 Module
- Im Wahlpflichtbereich können ggf. auch weitere Lehrveranstaltungen der FAU integriert werden
  - Voraussetzung: Tauglichkeit für die Fernlehre
- Ergänzt wird das Angebot durch
  - ein studienbegleitendes Projekt (Praxissemester) sowie
  - zwei studienbegleitenden Seminare zum wissenschaftlichen Arbeiten.

Übersicht

Ruhr-Universität

Semester /Säule	Grundlagen	Programmierung	IT-Sicherheit
begl.	Projekt (11)	Seminar (5)	Seminar (5)
9	Bachelorarbeit (12) und Kolloquium (3)		
8	Wahlpflichtbereich		Sicherheitsmanagement
7	(5 aus 10 Modulen)		Netzsicherheit 3
6		Softwaretechnik 3	Netzsicherheit 2
5	Einf. Forensik	Softwaretechnik 2	Netzsicherheit 1
4	Theor. Informatik	Softwaretechnik 1	Systemsicherheit 2
3	Kryptographie	Systemprogrammierung	Systemsicherheit 1
2	Mathematik 2	Programmierung 2	Rechnerstrukturen
1	Mathematik 1	Programmierung 1	Einf. in die IT-Sicherheit

Hochschule Darmstadt

FAU

Hochschule Offenburg

Modellversuch

- Während der Förderphase soll ein voller Jahrgang einmalig aufgenommen werden
  - Evaluation der Konzeption im laufenden Betrieb
- Dazu notwendig:
  - **Einrichtung des Studiengangs zum WS 2013/2014**
    - Studienordnung, Prüfungsordnung, Modulhandbuch
    - Studiengang wird anschließend gleich wieder geschlossen
  - Keine Kosten für die Teilnehmer
  - Studienangebot ab 5. Semester abhängig vom Zuschlag zur 2. Förderphase

Zeitplan

- Winter 2011/2012:
  - Meinungsbildung innerhalb des Departments
- Sommer 2012:
  - Meinungsbildung in der Fakultät
- Herbst 2012:
  - Senat, Hochschulrat, Ministerium
- Wintersemester 2013/2014:
  - Aufnahme des Versuchsjahrgangs
- Frühjahr 2015:
  - Versuchsjahrgang ist dann im 4. Semester
  - Antragstellung für 2. Förderphase
    - Ende 2. Förderphase wäre September 2017
    - Versuchsjahrgang käme dann ins 9. Semester
- Öffnung eines ggf. modifizierten Studiengangs zum Wintersemester 2017/2018

Langfristige Planung

- Studiengang Teil der „Marke“ **Open C3S**
  - Kurse können darin auch zweitverwertet werden, z.B. in Form von Weiterbildungsangeboten für die Industrie
- **Marketing zentral** durch Open C3S
  - Institut für wissenschaftliche Weiterbildung (IWW), Hochschule Albstadt-Sigmaringen und International School of IT Security (isits), Ruhr-Universität
- CWW organisiert den Studiengang an der FAU
  - Dozentenmanagement, finanzielle Abwicklung
- FAU erhält **dauerhafte, nicht-exklusive Nutzungsrechte** für alle im Rahmen des Projekts entwickelten Inhalte
  - **FAU verantwortlich für den Bestand des Studiengangs**, auch wenn Dozenten wechseln
  - FAU schließt im Anschluss an die Förderung weiterführende Kooperationsverträge mit Hochschulen bzw. Dozenten
- Studiengang besteht, solange Finanzierung durch Studiengebühren gesichert ist

Anhang

Grobe Inhalte der Module

Module 1.-3. Semester

- **1. Semester**
  - Mathematik 1: Mengen, Beweisverfahren, Aussagenlogik, Zahlenräume, Lin. Alg.: Vektoren / Vektorräume, Funktionen und Folgen, Differentialrechnung
  - Programmierung 1: Java etc. (objects first); BlueJ. Listen (Stacks, Queues) und Bäume
  - Einführung IT-Sicherheit: Grober Überblick: Sicherheitsmanagement, Gefahrenanalyse, Zertifizierungen, z. B. Fallstudien, physische Sicherheit, Fehlertoleranz, Verfügbarkeit, RAID
- **2. Semester**
  - Mathematik 2: Numerik, Wahrscheinlichkeitsrechnung, Diskrete Strukturen, Zahlentheorie
  - Programmierung 2: maschinennäher, C/Assembler (Intel? MMIX?)
    (hier vielleicht Exploits, Shell-Code? → Intel?)
    Graphen und Graphalgorithmen
  - Rechnerstrukturen: Prozessor, Speicher, Peripherie, Schaltnetze/Schaltwerke, Floating-Point-Operationen (oder: Mathe 2)
- **3. Semester**
  - Kryptographie: Lit.: Christof Paar: „Understanding Cryptography“,
    Stromchiffren, DES, AES, Blockchiffren allg., RSA, diskreter Log., elliptische Kurven, digitale Signaturen, Hashfunktionen, MAC, Schlüsselvereinbarung → davon ca. ¼ , 1/3 kürzen
  - Systemprogrammierung: Shell-Skripte (auch Perl, Python), Unix-Baukasten, PowerShell (?)
    z. B. Brute-Force-Skripte schnell selbst schreiben, reguläre Ausdrücke
  - Systemsicherheit 1/Betriebssysteme: Prozesse/Threads, virtueller Speicher, Scheduling + Context Switch, Architektur (monolith. / Mikrokernel), Dateisysteme, Synchronisation

Module 4.-8. Semester

- **4. Semester**
  - Theoretische Informatik: Automatentheorie, abstrakte Rechnermodelle (Register- und Turingmaschinen), Komplexitätstheorie, Kompl.-Klassen (P, NP, Co-NP, …), NP-vollständige Probleme (Knapsack, TSP), Laufzeiten O(n)..., Bewertung der Effizienz von Algorithmen, Berechenbarkeit, formale Sprachen, Chomsky [Teile davon]
  - Softwaretechnik 1-3: Modellierung, UML, Software-Entwicklungs-Vorgehensmodelle (V-Modell, Wasserfallmodell, …), Sichere Software-Entwicklung – Secure Development Lifecycle (SDL, Microsoft), statische/dynamische Code-Analyse, Web-Applikationen (clientseitig und serverseitig), Fuzzing, Application Server, Dienste, SOAP, XML, JavaScript, PHP, Code Injection; Parser: lex, yacc. SQL/Datenbankprogrammierung
  - Systemsicherheit 2: Absicherung eines Einzelrechners. Malware, Anti-Malware, Integritätsmanagement, sicheres Booten, aktuelle Fallbeispiele, Passwörter.
- **5. Semester**
  - Compilerbau: Einführung in die Forensik: Vorgehensmodelle, digitale Spuren, Definitionen, Einbettung in die klassische Forensik, post-mortem- und Live-Analyse (Dateisysteme, Speicher), Anwendungsforensik
  - Softwaretechnik 2: siehe SWT 1
  - Netzsicherheit 1/Rechnernetze: Ethernet, IP, TCP/UDP, VPN (IPSec, PPTP), SSL, WLAN (WEP, WPA2)
- **6. Semester**
  - Softwaretechnik 3: Testen und Dokumentation, siehe SWT 2
  - Netzsicherheit 2: Anwendungen: E-Mail, S/MIME, PGP, X.509, Kerberos
- **7. Semester**
  - Netzsicherheit 3: Sicherheit von Webanwendungen und Webservices: HTTP, Soap
- **8. Semester**
  - Sicherheitsmanagement: Governance im Bereich der Informationssicherheit, Grundlagen des Risikomanagements, Entwicklung/Management eines Programms zur Informationssicherheit, Grundlagen Incident Management, Informationssicherheitsmanagement auf Basis BSI-IT-Grundschutz. Datenschutz.

Wahlpflichtbereich

- Der Wahlpflichtbereich besteht voraussichtlich aus folgenden Modulen:
  - Modellbildung
  - Sicherheitsprotokolle (TLS, IPSec, PACE, DNSsec, etc.)
  - Elektronische Identitäten
  - Netzwerk- und Mobilfunkforensik
  - Ethisches Hacking
  - Incident Management
  - Security Trends/Cloud Security
  - Internetforensik
  - Implementierung kryptographischer Protokolle
  - Sicherheit von Webanwendungen