Master of Science-Studiengang IT-Sicherheit

am Fachbereich Informatik der TU Darmstadt

Studiengangskoordinator: Prof. Dr. Stefan Katzenbeisser

Motivation:

Informationstechnologie ist bereits heute eine Schlüsseltechnologie für viele Lebensbereiche und Wirtschaftszweige wie Gesundheit, Mobilität, Unterhaltung, Produktion, Logistik und Finanzen. IT ist der Schlüssel für Innovationen in einer Zukunft, in der wir umgeben sind von unzähligen eingebetteten Systemen, in der grenzenlose Kommunikation möglich ist und ein großes Wertschöpfungspotential durch die Verlagerung von Geschäftsprozessen und Dienstleistungen in das Internet besteht. Der IT-Sicherheit kommt in diesem Prozess eine Schlüsselrolle zu. Nur eine sichere IT-Infrastruktur wird Innovation ermöglichen; gleichzeitig verhindert IT-Sicherheit enorme wirtschaftliche Schäden etwa durch Hacker-Angriffe oder Wirtschaftsspionage, aber auch Schäden an Leib und Leben durch manipulierte oder unzuverlässige eingebettete Systeme.

Im Design- und Implementierungsprozess zukünftiger IT-Systeme werden daher fundierte Kenntnisse über den Schutz und die Zuverlässigkeit von Hardware- und Software eine enorme Rolle spielen. Umfassende Kenntnisse im Bereich der IT-Sicherheit erfordern unter anderem Wissen in den folgenden Teilbereichen:

- *Kryptographie:* Moderne Verschlüsselungsverfahren sowie andere kryptographische Basisprimitiven
- *Systemsicherheit:* Sicherheit von eingebetteten Systemen und Netzwerken
- *Softwaresicherheit:* Sicherheit und Zuverlässigkeit von Software, Konzeption von Sicherheitsarchitekturen für große IT-Systeme

Darüber hinaus erfordert die Konzeption moderner Sicherheitssysteme gute Kenntnisse in verschiedenen Bereichen der klassischen Informatik, wie Betriebssysteme, Software-Engineering, Datenbanksysteme oder Netzwerke.

Arbeitsmarktperspektiven:

Für Absolventen des Studiengangs bestehen vielfältige Einsatzmöglichkeiten sowohl im akademischen Bereich als auch in der Industrie. Dies wird durch vielfältige Referenzen belegt:

- Laut dem Branchenverband BITKOM gibt es zu wenig Lehrveranstaltungen an deutschen Hochschulen zur IT-Sicherheit[1]. Die Einführung des Masterstudiengangs würde das Problem mindern und die Bedeutung

[1] http://www.bitkom.org/de/presse/57465_54538.aspx

Darmstadts in der IT-Sicherheit stärken.

- In Deutschland wird die Bedeutung der Ausbildung IT-Sicherheit durch den Berufsverband „Gesellschaft für Informatik“ ebenfalls klar herausgestellt[2], im Oktober 2006 legte das Präsidium der GI das Papier „IT-Sicherheit in der Ausbildung“ (Empfehlung der Gesellschaft für Informatik e.V. (GI) zur Berücksichtigung der IT-Sicherheit in der schulischen und akademischen Bildung) vor.
- Nach Meinung des IT-Verbandes Comptia besteht ein weltweiter Mangel an IT-Fachkräften[3]. Kenntnisse in IT-Sicherheit erhöhen den Marktwert von IT-Fachkräften erheblich.
- Die Studie „2006 Global Information Security Workforce Study“ von IDC vom Dezember 2006[4] vertritt den Standpunkt, dass der Personalbedarf in der IT-Sicherheitsdomäne stark wächst („The number of information security professionals worldwide in 2006 is estimated to be 1.5 million, an 8.1% increase over 2005“), zeigt die Bedeutung des IT-Sicherheitspersonals auf („On average, more than 41% of information security budgets is spent on personnel, including salaries and benefits, and education and training) und betont die Wichtigkeit von Bildung speziell in diesem Bereich („Security professionals are asking for additional education and training in the areas of information risk management, business continuity/disaster recovery planning, and forensics.“).
- Eine regionale Studie über den Personalbedarf und die Perspekiven im Bereich der IT-Sicherheit[5] kommt zu folgendem Schluss: “Derzeit werden Arbeitskräfte für den Bereich IT-Security dringend gesucht. Knapp drei Viertel der Befragten schätzen den Fachkräftemangel als gravierend oder sehr gravierend ein. Ein Viertel der Stellen kann bereits heute schon nicht besetzt werden. Dieser wachstumshemmende Trend wird sich in Zukunft fortsetzen. Die Unternehmen planen eine Personalaufstockung bis 2010 um 65%, d.h. auf 330 Mitarbeiter. Von den Befragten, die die Engpasssituation als „gravierend“ oder „sehr gravierend“ einschätzen, ist die Hälfte der Meinung, dass sich die Situation bis 2010 nicht entspannen wird.”

Aufbau des Studiums:

Das Studium umfasst 120 CP in 4 Semestern; der Studienbeginn ist sowohl im Sommer- als auch im Wintersemester möglich. Die 120 CP sind auf die folgenden Prüfungsleistungen verteilt:

- 30 CP Masterarbeit

[2] http://www.gi-ev.de/fileadmin/redaktion/empfehlungen/GI-Empfehlung-IT-Sicherheit-in-der-Ausbildung-2006.pdf
[3] http://www.computerwoche.de/job_karriere/arbeitsmarkt/1865980/
[4] https://www.isc2.org/download/workforcestudy06.pdf
[5] http://pc50461.uni-regensburg.de/NR/rdonlyres/D0D7632A-F549-420D-8306-75D2173554B0/0/806_Studie_ITSicherheit_Ostbayern_Langfassung_v100.pdf

- 75 CP Lehrveranstaltungen aus 4 verschiedenen Bereichen:
    1. Cryptography
    2. System Security
    3. Software Security
    4. Selected Complementary Topics

    Die folgenden Veranstaltungen (jeweils 6CP) stellen Pflichtveranstaltungen dar:
    - *Introduction to Cryptography* im Bereich 1
    - *Embedded System Security* im Bereich 2
    - *Introduction to IT-Security* im Bereich 3

    Die weiteren Vorlesungen (insgesamt 57CP) können frei aus dem Lehrangebot gewählt werden, wobei aus den Bereichen 1-4 jeweils mindestens 6 CP gewählt werden müssen.

- 15 CP Studienbegleitende Leistungen
  Die studienbegleitenden Leistungen können wahlweise in einer der folgenden Formen erbracht werden:
    - Ein Projekt über 15 CP. Hier wird eine konkrete wissenschaftliche Fragestellung theoretisch und praktisch bearbeitet. Die Themen des Projekts sollten möglichst eng an aktuellen Forschungsarbeiten der Mitglieder des Fachbereichs orientiert sein.
    - Besuch von Seminaren, Praktika, Projekten (mit weniger als 15 CP), Praktika in der Lehre, Semester- oder Studienarbeiten in einem Gesamtumfang von 15CP. Es müssen mindestens zwei der genannten Formen gewählt werden.

Aufbau der 4 Wahlbereiche:

Die Lehrveranstaltungen der 4 Bereiche bestehen aus den Angeboten des FB Informatik, sowie anderen Fachbereichen der TU Darmstadt. Im Folgenden sind beispielhaft bestehende bzw. Geplante Vorlesungen den Bereichen zugeordnet:

1. Wahlbereich A: Cryptography
    - Public Key Infrastructures (Buchmann)
    - Cryptographic Protocols (Manulis, Fischlin)
    - Public-Key Kryptanalyse (Buchmann)
    - Introduction to Quantum Informatuon Theory: Communication, Cryptography and Computing (Renes, FB Physik)

2. Wahlbereich B: System Security
    - Sicherheit in Netzwerken (N.N.)
    - Dependable Systems (Suri)
    - Intrusion Detection (N.N.)

- Implementation of Cryptographic Primitives (N.N.)

3. Wahlbereich C: Software Security
   - Privacy Enhancing Technologies (Katzenbeisser)
   - Multimedia Security (Steinebach)
   - Biometrics (Busch)
   - Formal Methods of Information Security (Mantel)
   - Specification and Verification (Veith)
   - Analysis of Software (Mantel)
   - Type Systems (Mezini)
   - Software Quality (Schürr)

4. Wahlbereich C: Selected Complementary Topics
   - Database Systems (A. Buchmann)
   - Operating Systems (Suri)
   - Computer Networks (Steinmetz)
   - Programming Language Concepts (Mezini)
   - Complexity Theory (Veith)
   - Machine Learning (Schiele, Fürnkranz)
   - Computer Vision (Schiele)
   - Real-Time Systems (Schürr)
   - IT-Security Managament (Böhmer)
   - Legal Issues in the Information Society (Schmid, FB1)
   - E-Business (Bixmann, FB1)