IT-Sicherheit

Einführung

Prof. Dr. Dominik Merli, Prof. Dr. Lothar Braun

Sommersemester 2020

Hochschule Augsburg - Fakultät für Informatik

Vorstellungsrunde

Prof. Dr.-Ing. Dominik Merli

Hochschule Augsburg
Fakultät für Informatik

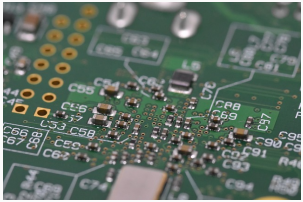
Campus am Roten Tor
Gebäude J, Raum J1.06
Sprechstunde: nach Absprache per E-Mail

Telefon: +49 (0)821 5586-3459
E-Mail: dominik.merli@hs-augsburg.de

Forschungs- und Interessengebiete

Industrial Security

- Sicherheit industrieller Anlagen
- Safety-Security-Schnittstelle



Embedded Security

- FPGA & µC Security
- Reverse Engineering und Angriffe

Prof. Dr. Lothar Braun

Hochschule Augsburg
Fakultät für Informatik

Campus am Roten Tor
Gebäude J, Raum J2.03
Sprechstunde: nach Absprache per E-Mail

E-Mail: lothar.braun@hs-augsburg.de

Forschungs- und Interessengebiete

Industrial Security

- Sicherheit industrieller Anlagen
- Industrielle Netzwerksicherheit

Netzwerksicherheit

- Sichere Netzwerk-Kommunikation
- Fuzzing von Netzwerk-Protokollen

Hochschule Augsburg
University of Applied Sciences

HSA_innos
Institut für innovative Sicherheit

- Themengebiete
  - Sicherheit industrieller Anlagen und Komponenten
  - Sicherheit eingebetteter Systeme
  - Security Monitoring und Digitale Forensik
  - Risikomanagement

- Abschlussarbeiten, HiWi, MAPR, Promotion, … ⇒ **`www.hsainnos.de`**

Wer sind Sie?

In welchem Semester sind Sie?

Was interessiert Sie an IT-Sicherheit?

Was erwarten Sie von dieser Veranstaltung?

Kurs: IT-Sicherheit


gP
gefragte
Persönlichkeiten

Spezifische Positionen

- Security Engineer
  - Hersteller von Produkten für Consumer- und Industrie-Branchen
  - Solide Kenntnisse über Kryptographie und Sicherheitskonzepte notwendig
  - Praktische Erfahrungen in Entwicklung und Test von Schutzmaßnahmen

- Security Architect
  - Betreiber von IT-Infrastrukturen, Integratoren von System-Lösungen
  - Wissen über Sicherheitsarchitekturen und -konzepte unabdingbar
  - Fokus auf Zusammenspiel und Schnittstellen verschiedener Systeme

- Security Consultant
  - Beratungsfirmen, In-house Beratungsabteilungen
  - Knowhow bzgl. Sicherheitsprozessen und -konzepten erforderlich
  - Begleitung eines Kunden bei der Verbesserung seiner IT-Sicherheit

Themen

1) Grundlagen der IT-Sicherheit
   - Sicherheitsstandards
   - Relevante Organisationen
   - Typische Angriffe
   - Sicherheitsprozesse
2) Kryptographische Grundlagen
   - Symmetrische Kryptographie
   - Hashfunktionen, MACs und Authenticated Encryption
   - Asymmetrische Kryptographie
   - Schlüsselverwaltung
3) Anwendungsbezogene IT-Sicherheit
   - Anwendungen kryptographischer Protokolle
   - Netzwerksicherheit
   - Sicherheit von Web-Anwendungen

Organisation

- Vorlesung und praktische Übungen
  - 6 Semesterwochenstunden
  - 7,5 ECTS Credits
  - Mo, 08:00 - 13:10, (M2.03 oder virtueller Hörsaal)
- Unterlagen
  - https://moodle.hs-augsburg.de
- Prüfung
  - 90 Minuten, Fragen zur Vorlesung und zu den Übungen
  - Zusätzlich für Masterstudierende: Vortrag, 20 Minuten

Termine

Datum	Thema
23.03.2020	Einführung (Profs. Merli & Braun)
30.03.2020	Sicherheitsprozesse (Prof. Merli)
06.04.2020	Symmetrische Kryptographie (Prof. Merli)
13.04.2020	*Ostermontag*
20.04.2020	Hash Funktionen, MACs und Authenticated Encryption (Prof. Merli)
27.04.2020	Asymmetrische Kryptographie (Prof. Merli)
04.05.2020	Schlüsselverwaltung (Prof. Merli)
11.05.2020	Angreifer-Typen und typischen Angriffe (Prof. Braun)
18.05.2020	Anwendungen kryptographischer Protokolle (1) (Prof. Braun)
25.05.2020	Anwendungen kryptographischer Protokolle (2) (Prof. Braun)
01.06.2020	*Pfingstmontag*
08.06.2020	Netzwerksicherheit (Prof. Braun)
15.06.2020	Sicherheit von Web-Anwendungen (1) (Prof. Braun)
22.06.2020	Sicherheit von Web-Anwendungen (2) (Prof. Braun)
29.06.2020	Master-Vorträge und Fragestunde (Profs. Merli & Braun)

Vorträge der Masterstudierenden

- Zusatzleistung nötig!
  - Aufarbeitung einer aktuellen Veröffentlichung im Bereich IT-Sicherheit
  - 20 Min. Präsentation für alle Kommilitonen
  - Geht zu 20% in Note ein

- Details und Liste zum Eintragen
  - https://moodle.hs-augsburg.de

Literatur

- A. Shostack: ”Threat Modeling: Designing for Security”, Wiley, 2014
- C. Paar, J. Pelzl: ”Understanding Cryptography: A Textbook for Students and Practitioners”, Springer, 2010
- I. Ristić: ”Bulletproof SSL and TLS”, Feisty Duck, 2015
- C. Eckert: ”IT-Sicherheit: Konzepte - Verfahren - Protokolle”, Oldenbourg, 2012

Einverstanden? Gibt es noch Fragen?

Was ist IT-Sicherheit?

Sicherheit

Sicherheit =

- safety
- security
- certainty
- assurance
- immunity
- guarantee
- dependability
- ...

Sicherheit vs. Risiken

”Sicherheit bezeichnet allgemein den Zustand,
der für Individuen, Gemeinschaften [...] und Systeme
frei von unvertretbaren Risiken ist
oder als gefahrenfrei angesehen wird.”

Deutsche Wikipedia, März 2020

Es gibt keine 100%ige Sicherheit!

IT-Sicherheit (engl. IT security)

- **Schutz von Daten**, z.B. Dateien oder Datenbanken
- **Schutz von Software**, z.B. Applikationen oder Betriebssysteme
- **Schutz von Hardware/Geräten**, z.B. Smartphones, Laptops, Smartcards
- **Schutz von Kommunikation**, z.B. zwischen Geräten
- **Schutz von Netzwerken und Systemen**, z.B. Firmennetzwerke und Industrieanlagen
- **Schutz von Infrastrukturen**, z.B. das Stromnetz
- **Schutz von Benutzern**, z.B. deren Identitäten und Daten

Verwandte Begriffe

- Funktionssicherheit bzw. Funktionale Sicherheit (engl. safety)
  - Schutz von Menschen und Umwelt vor Schäden, notfalls durch Einnahme eines sicheren Zustands
- Datenschutz (engl. privacy / data protection)
  - Schutz von natürlichen Personen bei der Verarbeitung personenbezogener Daten

Fakt:

IT-Sicherheit kostet Geld!

Diskussion:

Was motiviert Einzelpersonen und Unternehmen in ihre IT-Sicherheit zu investieren?

Gesetze, Standards und Institutionen

Gesetze und Standards

- Schutz aus nationalem/internationalem Interesse
  - Gesetze ermöglichen national/international verpflichtende Sicherheitsmaßnahmen
  - Verfehlung von Schutzmaßnahmen kann von Staat(en) bestraft werden
- Einigung auf vergleichbare Sicherheitsmaßnahmen
  - Lieferkette wird zunehmend komplexer
  - Zusammenarbeit und einheitliche Sicherheitsstandards unerlässlich
- Kundenanforderungen und Ausschreibungen
  - Nachweis von Sicherheitsniveau oft auf Basis einer Zertifizierung
  - Normen und Standards ermöglichen vergleichbare Zertifizierung

Institutionen

- Verantwortlichkeiten
  - Welche Institutionen tragen Verantwortung bzgl. IT-Sicherheit?
- Ansprechpartner und Unterstützung
  - Welche Institutionen können beim Thema IT-Sicherheit unterstützen und wie?
- Beschwerde-/Meldestelle
  - An welche Institutionen müssen Vorfälle/Schwachstellen gemeldet werden?

Fakt:

Es gibt viele verschiedene IT-Sicherheits-Organisationen!

Aufgabe:

1) Jede/r Studierende für sich

2) Analyse einer Institution

3) Erstellung einer Antwort im Forum

4) Enthält Mission und Angebote der Organisation