Hochschule **RheinMain**
University of Applied Sciences
Wiesbaden Rüsselsheim

SECURITY

Übersicht und Organisation

April 14, 2023

Marc Stöttinger

ÜBERSICHT UND ORGANISATION

- → Einordnung der Veranstaltung
- → Organisation der Veranstaltung
- → Materialien

EINORDNUNG DER VERANSTALTUNG IN DAS STUDIUM

- → Pflichtveranstaltung im Studiengang ITS und AI
- → Voraussetzung:
  - → Erfolgreicher Abschluss aller Module gemäß der semesterweise aufbauenden Fortschrittsregelung
- → Empfohlene Grundlagen
  - → Diskrete Strukturen / Analysis & Numerik / Lineare Algebra / Statisitik & Wkt.-Rechnung
  - → Rechnernetze & Telekommunikation / Betriebsysteme
- → Ergänzende LVen des 4. Semesters:
  - → Embedded IT-Security
  - → IT-Forensik
- → Listenfächer, z.B.:
  - → Embedded Systems

WORUM GEHT ES?

- → Wie kann ich Bedrohungen erkennen und abwehren?
- → Welche Sicherheitsmaßnahmen zum Erhalt des Schutzniveaus müssen ergriffen werden?
- → Welche kryptographischen Verfahren/Protokolle kann ich sinnvoll gegen welche Bedrohung einsetzen?
- → Wie wende ich kryptographische Primitiven korrekt an?

ZIELE DER VERANSTALTUNG (MODULHANDBUCH)

- → Einführung in die IT-Sicherheit
- → Spezielle Bedrohungen
- → Security Engineering
- → Monoalphabetische Chiffren und deren Analyse
- → Symmetrische und asymmetrische Kryptoverfahren
- → Public-Key-Infrastruktur
- → Kryptographische Protokolle und Anwendungen
- → Sicherheit in Netzen

ANGESTREBTE LERNERGEBNISSE (ZIELSETZUNG)

Nach Absolvieren dieser Kurseinheit sollten Sie:

- → Verfahren zur Authentifizierung von Teilnehmern verstanden haben und auswählen können,
- → Methoden der Informationsverschlüsselung einordnen, in ihrer Wirkung analysieren und in der Praxis anwenden können,
- → Vorkehrungen zur Datenintegrität und Geheimhaltung sensibler Dateninhalte beurteilen und sicherstellen können,
- → Konzepte für einfache kryptographische Primitiven, wie z.B. Einweg- und Hashfunktionen verstanden haben sowie Probleme beim Schlüsselaustausch behandeln können.

TYPISCHE FRAGESTELLUNGEN

Aus Sicht eines Anwenders ergeben sich die Fragen:

- → Warum ist Sicherheit nötig (IT-Sicherheitsgesetz, kritische Infrastrukturen) und wie ist sie erreichbar?
- → Mit welchen Kosten ist Sicherheit verbunden?
- → Was ist für ein erfolgreiches E-Business (IT-gestützter Arbeitsablauf) nötig?
- → Wie ist die Risikolage (Gefahrenlage, Angreifer und Täter, Konsequenzen)?

KAPITEL DER VORLESUNG

- → Motivation
- → Grundbegriffe
- → Standards
- → Risko Management
- → Kryptographie
- → Sicherheitsprotokolle
- → Plattformintegrität/Hardwaresicherheit
- → Softwaresicherheit
- → Netzwerksicherheit
- → Ausblick: Post-Quanten Kryptographie

ORGANISATION DER VERANSTALTUNG I

- **Vorlesung:**
  - Freitag 08:15 - 09:45; B002
  - Dozent: Marc Stöttinger
  - Beginn: 14.04.2023
- **Übung:**
  - 4 Übungsgruppen:
    - A: Freitag 10:00 - 11:30; C035
    - B: Mittwoch 14:15 - 15:46; C407
    - C: Mittwoch 16:00 - 17:30; C407
    - D: Mittwoch 17:45 - 19:15; C407
  - Betreuer: Marc Stöttinger
  - Beginn: 19./21.04.2023

ORGANISATION DER VERANSTALTUNG II

- **Leistungsnachweis:**
  - Klausur 90 Minuten
  - Prüfung findet in der Prüfungszeit statt
  - Geprüft wird der Inhalt der Vorlesung und der Übung
  - 100% der Modulnote

MATERIALIEN

- **Folien zur Vorlesung**
  - als pdf-datei in Stud.IP
- **Übungsblätter**
  - für Programmier- und Papierübungen der Übung
  - werden als .pdf-Dateien kapitelweise in Stud.IP bereitgestellt

LITERATUR & ONILNE-QUELLEN

- **Bücher**
  - Patrick Horster: Kryptologie - BI-Reihe Informatik/47, 1988
  - Wolfgang Ertel: Angewandte Kryptographie, Fachbuchverlag, 2007
  - Bruce Schneier: Applied Cryptography, John Wiley & Sons, 1996
  - Claudia Eckert: IT-Sicherheit, Oldenbourg Verlag, 2008
  - Christoph Paar, Jan Pelz: Understanding Cryptography, 2010, Springer
  - Christoph Paar, Jan Pelz: Kryptografie verständlich, 2016, Springer - als PDF verfügbar
  - Adam Shostack: Threat Modeling - Designing for Security, 2014, John Wiley & Sons Inc