IT-Sicherheit

Prof. Dr. Claudia Eckert

Organisatorisches: 4 Std. Vorlesung und 1Std. Übung (2-wöchig)

- **Umfang 5 SWS**: 7 ECTS: Vorlesungszeiten

  Di 12:15 – 13:45 Uhr, Präsenz (MW0001) und Live-Stream

  Mi 16:15 – 17:45 Uhr, Präsenz (MI HS1) und Live-Stream

- Übungsaufgaben in Tutorübungen: begleitend und vertiefend
- Modul im Gebiet: Sicherheit und Datenschutz (SP)
- Leistungsnachweis: Klausur: Inhalt: Vorlesung und Übungen
- Materialien zur Vorlesung:
  - Folien und Literaturhinweise über Moodle
  - Vorlesungsaufzeichnungen, annotierte Folien Feb 2022

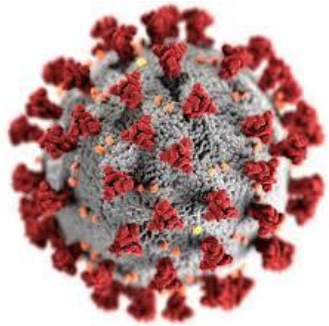
Die Verantwortlichen

Vorlesung: Prof. Claudia Eckert

- Lehrstuhl für Sicherheit in der Informatik, I20 Fakultät für Informatik
- Direktorin des Fraunhofer Instituts für Angewandte und Integrierte Sicherheit (AISEC), München/Garching

Übungsleitung:

- Fabian Franzen



Präsenzvorlesung:

- 3G Regel, mind 10% werden jedes mal stichprobenhaft geprüft, Verstoß wird gemeldet
- Raumbelegung: Bitte einen Sitzplatz Abstand einhalten
- Maskenpflicht**:** auch während der Vorlesung
- Kontaktnachverfolgung: Bitte über QRONITON-QR-Code am Eingang des Hörsaal
- Tweedback als Rückkanal während der Vorlesung
  - Moderation durch die Übungsleitung
  - Chat für Fragen der Studenten an Dozenten
  - Antwortkanal für interaktiv gestellte Fragen des Dozenten

https://tweedback.de

tweedback
We love feedback

- Live-Stream: Verfügbar unter **https://live.rbg.tum.de**

Übungsbetrieb

flag{66e94bd4ef8a2c3b884cfa59ca342b2e}

- 6 Übungsblätter mit Hausaufgaben + 2 Bonusblätter
- **Nicht verpflichtend, aber Punktebonus auf Klausur!**
- Ausgabe der Übungsblätter auf **Moodle**
  - Abgabe über **Scoreboard: https://scoreboard.sec.in.tum.de**
  - In Gruppen à 2 Studenten
  - Plagiatsversuche werden geahndet!
- Programmieraufgaben
  - CTF-Stil (Flagge bei erfolgreicher Lösung)
  - Verbesserungen des praktischen Verständnisses von Angriffen
  - Hinführend zu den Aufgaben der Praktika

Termine für Übungen

Alle Übungen finden im 2-Wochen-Rhythmus statt!

Wochentag	Uhrzeit	Raum	Erster Termin
Mo	12-14 Uhr	01.11.018	25.10. / 15.11.
Mo	14-16 Uhr	00.08.059	25.10. / 15.11.
Mo	16-18 Uhr	Online	25.10.
Mo	17-19 Uhr	00.13.008	25.10. / 15.11.
Di	17-19 Uhr	00.08.059	26.10. / 02.11.
Do	14-16 Uhr	Online	28.10. / 04.11.
Do	16-18 Uhr	00.13.009A	28.10. / 04.11.
Fr	12-14 Uhr	00.13.008	29.10.
Fr	14-16 Uhr	00.13.036	29.10.

01.11. ist Allerheiligen!

Anmeldung ab sofort bis spätestens So, 24.10. über TUMOnline!

Präsenztermine für Übungen

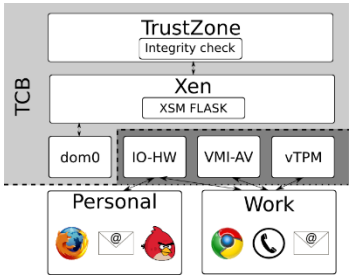
- Teilnahme nur mit Fixplatz in TUM-Online!
- Umwandlung in Online-Termine entsprechend der Nachfrage und der aktuellen Lage
- Während den Terminen:
  - Es gilt die 3G-Regel!
  - Bitte tragen Sie eine Mund-Nasen-Bedeckung!
  - Bitte scannen Sie die angebrachten QRONITON-QR-Codes!
- Informieren Sie sich regelmäßig: www.tum.de/corona
- Kommen Sie **nicht** bei COVID-19 typischen Symptomen!

Lehrstuhl Sicherheit in der Informatik, I20

Einige Forschungsthemen:

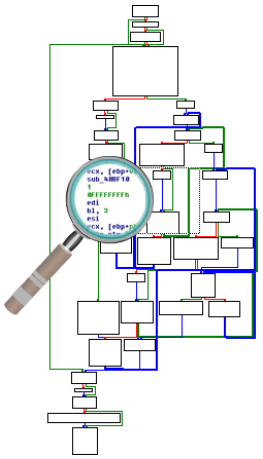
1. Methoden und Werkzeuge zur Angriffserkennung:

- Virtual-Machine Introspection (VMI)
- Malware-Analyse Framework
- Erweiterte maschinelle Lerntechniken



2. Unterstützung sicherer Ausführumgebungen:

- Sicherheitsarchitekturen eingebetteter Geräte
- Virtualisierung



3. Angriffsvektoren auf Sicherheitssysteme:

- App und Binary Hardening Systems
- Binary Analysis Systems (z.B. Intel PIN, z3)
- Protokollsicherheit (z.B. Bluetooth)

Fraunhofer AISEC: Angewandte und Integrierte Sicherheit

- Forschungsgelände Garching
- Lichtenbergstrasse 11

MitarbeiterInnen:

>180, weiter wachsend

Themen:

- Sicherheits-Testing, Embedded Security, KI & Security,
- Cloud-Sicherheit, System Security, ID-Management, Applied Privacy

Planung Januar (abhängig von Pandemie): AISEC-Studierendentag

Angebote für Studierende:

- HiWi-Tätigkeiten, Mitarbeit in laufenden Projekten, ….
- Bachelor- und Masterarbeiten, IDP mit E-Technik (Prof. Sigl)

Lehrveranstaltungen zum Themenfeld IT-Sicherheit

- IT-Sicherheit: jedes WS**, Hinweis:** ab WS22/23 mit 5 ECTS und als Vertiefung der ab WS2022/2023 neuen ITSec Vorl. im B.Sc.
- Sonstige sicherheitsbezogene Vertiefungsvorlesungen: u.a.
  - Sichere eingebettete, mobile Systeme (im SS)
  - Ausgewählte Themen: im WS21/22: ML und Sicherheit
  - Netzwerksicherheit (Carle), Security Engineering (Pretschner)
  - Kryptografie (Esparza)

Praktika: jedes Semester, in WS21/22: Binary Exploitation

Seminare: jedes Semester, in 2021/2022 u.a.

- Data Privacy Technology, Systems Hardening, Common Flaws in Protocol Security, Software Security Analysis, HW Security Extensions

Motivation: Bedrohungslage

BSI Lagebericht (Bundesamt für Sicherheit in der Informationstechnik)

- 2-jähriger Bericht: Aktueller Lagebericht vom September 2020
- **Fazit: Trends haben sich weiter fortgesetzt**
  - Schadprogramme: Ransomeware, Malware, Botnetze

    Frage: was ist Ransomeware?
  - Identitätsdiebstahl: Phishing, Maskierung
  - Advanced persistence threats (APT):

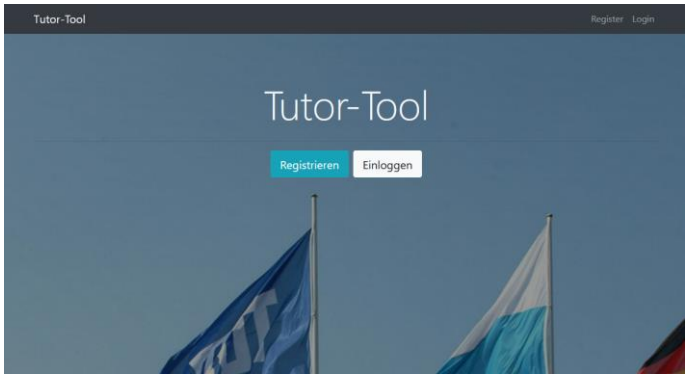
    Frage: was heißt das?
  - Distributed Denial of Service (DDos)
  - **Neu:** Covid 19 Konsequenzen

    Frage: Welche Probleme neu oder verstärkt?

Common Security Fails @TUM

ARTEMIS

- Alte Kryptoverfahren
- Anmeldung mit leerem Passwort
- Privilege Escalation: Student zu Admin
- Remote Code Execution
- …



Hack des alten Tools (Juli 2021), Verlust von Tutorendaten

Neues Tool:

- Ungeschützte API Endpunkte
- Privilege Escalation: Student zu Admin
- …

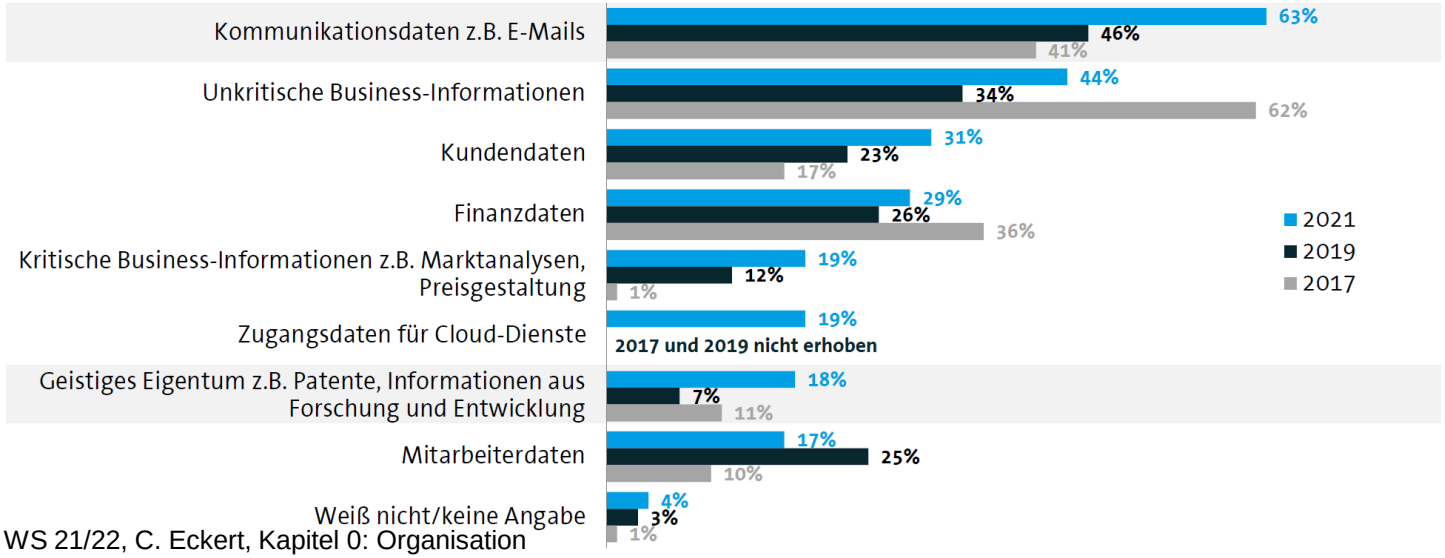
Weitere Zunahme an Angriffen in 2021 mit erheblichen Schäden

- Umfrage des Branchenverbands BitKom im August 2021,

Quelle: https://www.heise.de/downloads/18/3/1/4/8/7/4/1/bitkom-slides-wirtschaftsschutz-cybercrime-05-08-2021.pdf

  - 88% der befragten Deutschen Unternehmen waren in 2020/2021 Opfer von Attacken
- Cyber-Kriminalität ist Big Business
  - 220 Milliarden Euro Schaden durch Ransomware und andere Cyber-Angriffe in 2020/2021 allein in Deutschland

Ziele:



Lessons Learned:

- Angriffe entwickeln sich schneller als Verteidigungstechniken:
  - Verteidigung orientiert sich oft an einzelnen Angriffen, anstatt die Schwachstelle zu beseitigen
  - Secure Engineering und
  - Secure Programming Methoden sind erforderlich

- Angriffe sind zielgerichteter:
  - Differenzierte Schutz-Level, Authentisierung, Isolierung, Zero-Trust Paradigma erforderlich
- Starker Anstieg an Malware: Maßnahmen, wie
  - Signierte Binaries, Isolierung, Secure Boot sind unabdingbar
- Verfeinerte Angriffstechniken erfordern Sicherheitsmaßnahmen über gesamten Lebenszyklus: Design, Implementierung, Betrieb

Lessons Learned (Forts.)

Sicherheitsmaßnahmen über gesamten Lebenszyklus:

Design u.a.

- Risiko- und Bedrohungsanalyse (**Bem**. starke Industrie-Nachfrage)
- Sicherheitskonzept (**Bem.** häufig schon kaputt)

Implementierung u.a.

- Sichere Programmierung (**Bem.** nach wie vor viele Fehler)
- Korrekte Umsetzung von Krypto-Protokollen (**Bem.** erhebliche Schwachstellen, u.a. falsche Nutzung von Krypto-Schlüsseln)

Betrieb u.a.

- Zugangs- und Zugriffskontrollen (**Bem**. häufig fehlerhaft)
- Kontinuierliches Monitoring/Intrusion Detection (**Bem**. fehlt meist)
- Sicheres Update/Patch-Management (**Bem.** meist ohne Kontrolle)

Bsp: Sicherheitsprobleme: alt aber ähnliche Probleme heute überall

(1) **Apple Goto Fail**

- Implementierung von SSL/TLS : Server2Client Authentisierung
- Problem in Zertifikatsprüfung (ID-Bescheinigung) bei iOS Geräte
  - Darstellung != Inhalt
- Prüfung der Echtheit des Server-Schlüssels sollte über die Prüfung des Server-Zertifikats erfolgen!

```
...
if ((err = ReadyHash(&SSLHashSHA1, &hashCtx)) != 0)
    goto fail;
if ((err = SSLHashSHA1.update(&hashCtx, &clientRandom)) != 0)
    goto fail;
if ((err = SSLHashSHA1.update(&hashCtx, &serverRandom)) != 0)
    goto fail;
if ((err = SSLHashSHA1.update(&hashCtx, &signedParams)) != 0)
    goto fail;
    goto fail;
if ((err = SSLHashSHA1.final(&hashCtx, &hashOut)) != 0)
    goto fail;

err = sslRawVerify(ctx,
                   ctx->peerPubKey,
                   dataToSign,          /* plaintext */
                   dataToSignLen,       /* plaintext length */
                   signature,
                   signatureLen);
```

Problem:

- 2 goto Fail hinter einander: Signaturprüfung wird übersprungen,
- alle Schlüssel (d.h. alle Server-Identitäten) werden akzeptiert

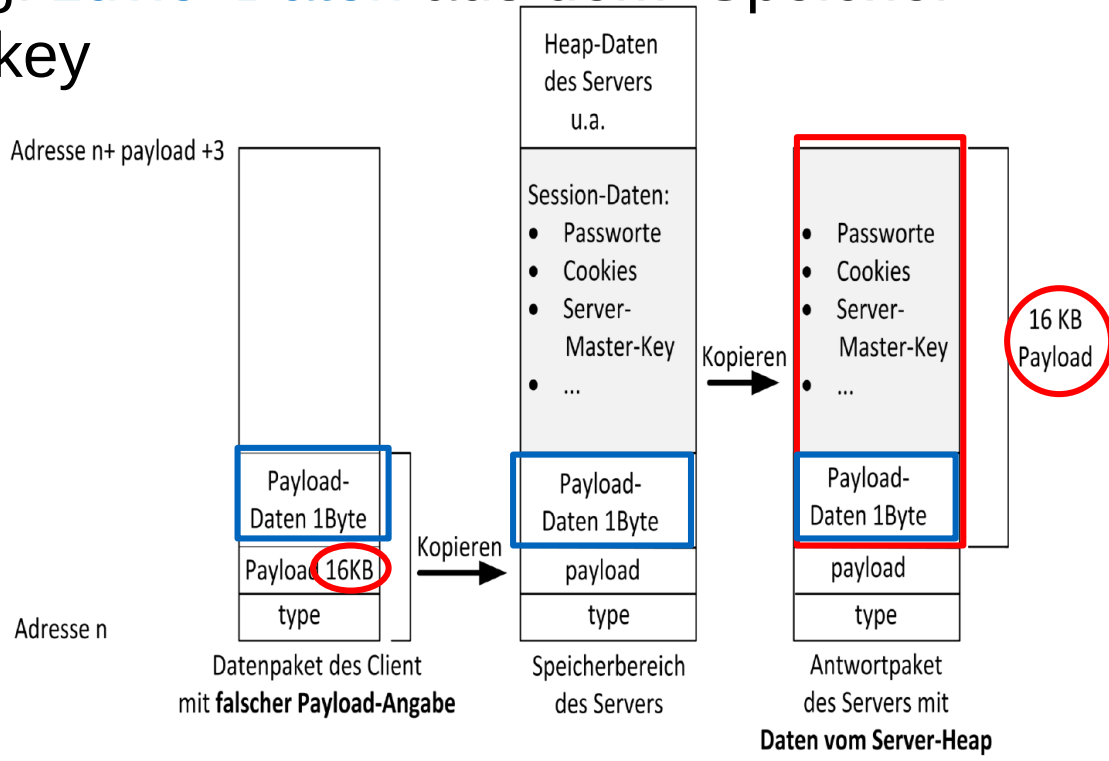
Ursache: fehlerhafte Programmierung führt zu Sicherheitslücken

(2) **Heartbleed:** 2014, OpenSSL-Heartbeat-Funktion: still alive

- Client kopiert einen Datenblock (z.B. 1 Byte) in Server-Speicher und gibt die Länge x des Datenblocks an, z.B. 1 Byte.
- Server sendet Datenblock der Länge x (z.B. 1 Byte) zurück
- **Problem:** Server sendet ggf zuviel Daten aus dem Speicher zurück, z.B. Server-Masterkey

Ursache: Server prüft nicht, ob die Längenangabe x gleich der Länge der Eingabedaten des Clients ist!

Bsp: Angreifer sendet 1Byte, behauptet aber 16KB Serverantwort: 16KB



(3) Shellshock, Unix Shell Bash:

- Wert einer Variablen kann Funktionsaufruf sein (Daten und Code sind nicht getrennt)
- Code der aufgerufenen Funktion wird bei Werte-Auswertung ausgeführt, wenn die Variable einen bestimmten Präfix besitzt.
- Über Umgebungsvariablen können Variablen und Funktionen exportiert werden, gekennzeichnet durch Präfix
- **Problem:** Funktionsdefinition wird nicht geprüft, z.B.

  (var = “() { :;}; rm –rf / ; echo ‘Ups…‘ “)

  var: Umgebungsvariable

  Ausgeführter Code: rm –rf / ; echo ‘Ups…‘

Ursache: unsichere Programmierung

Begriffliche Abgrenzung: Safety versus Security

Safety: Funktions- und Betriebssicherheit, Zuverlässigkeit

- **Ziel:** Erkennen und Abwehr von Störungen, die die korrekte Funktionalität, die Betriebssicherheit beeinträchtigen.
- **Störungen**: von Innen, durch das technische System
  - in Software: durch Programmierfehler, oder
  - u.a. durch Material-Ermüdung, Hardware-Fehler etc.

- **Vorgehen zur Gewährleistung der Safety:**
  - Spezifikation der gewünschten Funktionalität und
  - Erkennen und - falls möglich- Beheben von Abweichungen vom gewünschten Verhalten

Begriffliche Abgrenzung: Safety versus Security

Safety: Funktions- und Betriebssicherheit, Zuverlässigkeit

Frage: Welche Safety-Maßnahmen, Mechanismen sind bekannt?

Security: Daten und Informations-Sicherheit, Cyber-Security

- **Störungen** von Außen**:** gezielte oder unabsichtliche Angriffe: Manipulation, Datenmissbrauch, Funktionsstörung,
- **Ziel:** nach ISO/IEC 2382-1:
  - Minimierung der Verwundbarkeit von Werten u. Ressourcen,
  - Bewahren eines Systems vor Beeinträchtigung und Missbrauch
- **Vorgehen zur Gewährleistung der Security:**
  - Spezifikation von zulässigen Zugriffen/Aktionen (was, durch wen, wann),
  - Spezifikation von erwartetem Verhalten,
  - Erkennen u. Abwehr von unzulässigen Zugriffen, Aktionen

Security: Daten und Informations-Sicherheit, Cyber-Security

Frage: Welche Security-Maßnahmen, Mechanismen sind bekannt?

Einordnung und Ziele der Vorlesung IT-Sicherheit

Vorkenntnisse:

- Grundlagenkenntnisse zu Betriebssystemen, Rechnernetzen und Verteilte Systeme sind erforderlich

Ziele der Vorlesung:

- Kennenlernen der wichtigsten Bedrohungen und Schwachstellen
- Überblick über gängige Techniken, Methoden und Konzepte zur Erhöhung der IT-Sicherheit
- Verständnis für Ursachen von Sicherheitsproblemen
- Fähigkeit zur kritischen Bewertung der Qualität und Grenzen von Sicherheitslösungen
- Fähigkeit zur kritischen Reflektion von Medienberichten

Inhaltsverzeichnis – Grobüberblick

1. Einleitung
   - Grundlegende Begriffe, Schutzziele, Bedrohungen, Risiken
   - Ausgewählte Angriffe: u.a. OWASP TOP-10, Buffer-Overflow, Return-oriented-Programming (ROP)
2. Kryptografische Grundlagen
   - Symmetrische Verfahren (AES) und deren Betriebsmodi
   - Asymmetrische Verfahren: RSA, Elliptische Kurven (ECC)
   - Hashfunktionen, Signaturverfahren
   - Fortgeschrittene Konzepte: u.a.
     - Post-Quantum u. Homomorphic Crypto, Attribute-based

Inhaltsverzeichnis – Grobüberblick

3. Schlüsselmanagement

- Schlüsselaustausch- und Schlüsselvereinbarungsverfahren: u.a. mit Trusted-Third-Party; Diffie-Hellman-Protokoll
- Public Key Infrastruktur (PKI): Zertifikate, CA, Validierung

4. Digitale Identität

- Klassifikation, Mehrfaktor-Authentisierung
- Wissensbasierte Authentisierung: Challenge-Response, OTP
- Besitzbasierte Authentisierung: Token, U2F (FIDO), PA
- Biometrie-basierte Authentisierung: u.a. Gesichtserkennung
- Authentifikationsprotokolle: Kerberos, OAuth
- Self-Sovereign Identity (SSI)

Inhaltsverzeichnis – Grobüberblick

5. Netzwerksicherheit

- Überblick über gängige Konzepte: Firewalls, VPNs
- Protokolle zur Kommunikationssicherheit:
  - TLS, IPSec (nur kurze Wiederholung)
  - DNSSec

6. Anwendungssicherheit

- Protokolle:
  - Messenger: Signal (auch bei WhatsApp), Telegram
  - Mail: OpenPGP
  - RDP

Inhaltsverzeichnis – Grobüberblick

7. System-Sicherheit

- Sicherheitsmodelle
- Betriebssystemsicherheit:
  - Architekturen, Dienste, Virtualisierung, Speicherschutz
- Fallbeispiele: Linux, Windows

8. Hardware-gestützte Sicherheit

- Trusted Computing:
  - TPM, Trusted und Secure Boot, DICE
- Secure Enclave, Confidential Computing
  - Intel SGX/TDX, AMD-SEV

Inhaltsverzeichnis – Grobüberblick

9. Sicherheitsanalyse

- Code-Analysen
- Fuzzing
- Reverse Engineering

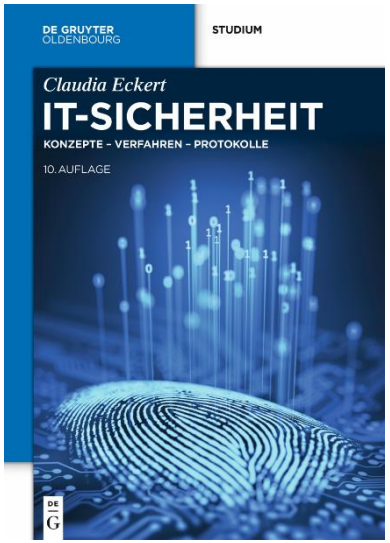
10. Secure Engineering

- Design-Prinzipien,
- Systematik: u.a. Bedrohungs-, Risikoanalyse
- Sicherheitsevaluierung
  - Bsp Common Criteria

Zeitplan Übungsbetrieb

#	Datum	Thema	Bonus
1	25.10. – 7.11.	Web Application Security	
2	8.11. – 21.11.	Kryptografie	Common Security Fails @TUM
3	22.11. – 5.12.	Hashfunktionen	
4	6.12. – 19.12.	Netzsicherheit	
5	20.12 – 16.01	Binary Exploitation	Reverse Engineering
6	17.01. – 30.01.	Systemsicherheit	
7	31.01. – 13.02	Klausurvorbereitung, TBA …	

Literatur



1. C. Eckert *IT-Sicherheit, De Gruyter* Verlag, 2018, 10. Auflage
   Das Buch ist auch als eBook verfügbar
2. Christof Paar: Understanding Crytography, Springer, 2016
3. M. Bishop: *Introduction to Computer Security* , Addison-Wesley, 2004
4. B. Schneier, Applied Cryptography, John Wiley & Sons, 1996
5. W. Stallings, Lawrie Brown: Computer Security: Principles and Practice, 3rd Edition, Published Jul 8, 2014 by Pearson
6. G. Hoglund und G. McGraw, Exploiting Software, how to break code, Addison Wesley, 2004