Themen zur Computersicherheit

Einleitung

PD Dr. Reinhard Bündgen
buendgen@de.ibm.com

Vorlesungsvoraussetzung

- allgemeine Informatik & Mathematikkenntnisse äquivalent zu Bachelor Informatik
- Grundlagen Betriebsysteme hilfreich
- Einige Bespiele im Rahmen von Unix / Linux
- zum Nachvollziehen bestimmter Stoffe ist der Zugang zu einem Linux System vorteilhaft.
  - zur Not Linux in VirtualBox installieren

Organisatorisches

- 22.11.2019: Vorlesung fällt voraussichtlich aus
- Prüfungstermin: Freitag 21.2.2020
- Prüfungsanmeldung
  - formal: Anmeldung beim Prüfungsamt
  - real (Platz im Prüfungsraum, Anzahl der Klausurausdrucke):
    - Anmeldung beim Dozenten
      - ca 2 Wochen vor Vorlesungsende
    - dazu Einschreibung in Teilnehmerliste zur Vorlesung (während der ersten drei Termine)
      - Teilnehmer werden aufgefordert sich anzumelden
    - Teilnahme ohne Anmeldung bei Dozenten nur möglich, wenn jenseits der angemeldeten Teilnehmer noch Platz im Prüfungsraum und Klausurausdrucke übrig – also besser anmelden :-)

Attacken in den Nachrichten

- 11/2014: Sony Pictures Entertainment
- 02/2015: NSA/GCHQ hacked SIM manufacturer Gemalto
- 04/2015: AT&T to pay $25M
- 05/2015: Chinese breach: data of 4M fed workers
- 08/2015: Carphone Warehouse: 2,4M Kundendaten
- 08/2015: VW Hack: Wegfahrsperre
- 09/2015: Ashley Medison Seitensprungportal
- 03/2016: PKWs über Funk hackbar
- 03/2016: Digitaler Bankraub in Bangladesh
- 04/2016: Türkisches Wählerverzeichnis: 49M Wähler
- 06/2016: LinkedIn Hack 113M Passwort Hashes
- 09/2016: 800K klartext Passwörter bei Brazzers veröffentlicht
- 10/2016: Passwörter vom Dropbox Hack veröffentlicht
- 10/2016: DDoS auf Amazon, Twitter, Netfix, PayPal, Spotify ...
- 05/2017. WannaCry: Ransomware (Telefonica, NHS, Dt. Bahn ...)
- 06/2017: Not Petya Ransomware (Ukraine)
- 07/2017: Hacking Kampagne auf Atomkraftwerke
- 07/2017: Information von über 400 000 UniCredit-Kunden ausgelesen
- 09/2017: Equifax hack: Kreditkarten Daten (einschl. SSN)

2019: Winnti

2018: Facebook

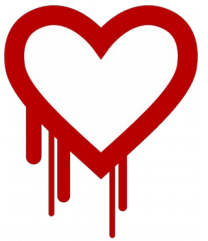
2018: Google+

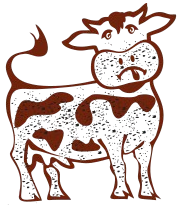
2019: Osiander

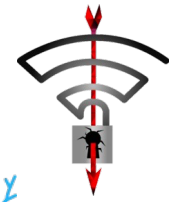
2019: Capital One
100M Personen

Attacken/Sicherheitslöcher mit Namen

- BEAST: SSL/CBC
- POODLE: SSL/Padding
- FREAK: SSL/short RSA keys
- ROWHAMMER: high frequency writes
- **Heart Bleed**: openSSL buffer overflow
- Logjam: small DH key, parameter reuse
- Shellshock: bash injection (string variables)
- Sweet32: birthday attack on 64 bit block ciphers
- Dirty Cow: Linux privilege escalation
- Krack: WPA2 Lücke im Handshake
- ROCA: schlechte RSA Implementierung
- Meltdown/Spectre 1/2: Seitenkanalangriffe die schlechtes Prozessor-Design für out-of-order Berechnung ausnützten







Wie wichtig ist IT Sicherheit?

- im Durchschnitt kostet ein Einbruch in ein IT System $11M
- im Durchschnitt bleibt ein Einbruch 8 Monate lang unentdeckt
- die NSA kann die Telekommunikation einzelner Länder vollständig aufzeichnen
- in den USA wurden 2013 3000 Firmen über Hackerangriffe aufgeklärt

Abzusichernde IT Systeme

- online Geldtransaktionen
  - online banking
  - Internethandel
  - digitales Geld
- sensible Systeme (Privatsphäre)
  - online Steuererklärung
  - Gesundheitswesen
- demokratische Einrichtungen
  - Wählerregister
  - Wahlautomaten
- Dokumente, Kommunikation die Betriebsgeheimnisse enthalten
  - Bilanzen
  - Strategien
  - Entwürfe/Erfindungen
- Steuerungen von Industrieanlagen
  - stuxnet
- Energieversorgung
  - Smart-Meter
- Verkehr
  - elektrische Schlösser
  - Diebstahlsicherung
  - Verkehrsleitsysteme
  - vernetzte Autos
- IoT
  - ...
- ...

Sicherheit: Die Haustüre

- kontrolliert Zugang zum Haus
  - sichert Privatsphäre
  - sichert Eigentum
  - Was ist erlaubt? Wo ist die Grenze?
- Schutzarten
  - Regelungen (Versicherungen)
  - gesetzlicher Schutz
  - physischer Schutz
    - keine absolute Sicherheit
    - abhängig vom Werkzeug und Zeit
- Sicherheitsfragen
  - Ist die Türe der einzige Zugang zum Haus?
  - Mit welcher Disziplin wird abgeschlossen?
  - Liegt der Schlüssel unter der Fußmatte
  - soziale Bedrohungen / Erpressungen

Bedrohungen

- Gefährdungsfaktoren
  - höhere Gewalt
  - Fahrlässigkeit
  - technisches Versagen
  - Vorsatz
  - organisatorische Mängel

Buffer overflow

Würmer **Bot-Netze**

(ERPRESSUNGS)TROJANER

DoS

Viren

OWASP Top 10

Open Web Application Security Project (OWASP)

- https://www.owasp.org/index.php/Main_Page
- sammelt die wichtigsten Bedrohungen für Web Applikationen

Top 10 für 2017

1) injection
2) broken authentication
3) sensitive data exposure
4) XML External Entities (XXE) -- new
5) broken access control
6) security misconfigurations
7) cross-site scripting (XSS)
8) insecure deserialization -- new
9) using components with known vulnerabilities
10) insufficient logging and monitoring -- new

Sicherheitstechnologien

Trusted Computing

Auditing

Kryptografie

Firewalls

SANDKÄSTEN

Secure Engineering

Zugriffskontrolle

Antiviren Programme

Verhaltensanalyse

Schutzziele

- Authentizität
  - Subjekt ist was/wer es vorgibt zu sein
- Datenintegrität
  - zu schützende Objekte werden nicht unerlaubt geändert
- Vertraulichkeit
  - Information ist nur Befugten zugänglich
- Verfügbarkeit
  - Daten oder Dienst sind immer verfügbar
- Verbindlichkeit
  - ein Subjekt kann für eine Tat verantwortlich gemacht werden
- Anonymität
  - ein Dienst kann anonym genutzt werden
- Vertrauen
  - ein Dienst verhält sich wie erwartet

Security Engineering ist schwer

Software Engineering

- positive Ziele (Funktion, Performanz, Nutzerfreundlichkeit, …)
- bekannte Schnittstellen
- Modularität
- SW Erweiterung → modulweise Kompatibilität

Security Engineering

- negative Ziele (was nicht passieren darf)
- potenziell unbekannte Angriffsflächen
- das schwächste Glied des Systems bestimmt seine Sicherheit → E2E Sicherheit
- SW Erweiterung → neue E2E Sicherheitsanalyse

2019 CWE Top 25 Most Dangerous Software Errors
http://cwe.mitre.org/top25/

[1]	CWE-119	Improper Restriction of Operations within the Bounds of a Memory Buffer
[2]	CWE-79	Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')
[3]	CWE-20	Improper Input Validation
[4]	CWE-200	Information Exposure
[5]	CWE-125	Out-of-bounds Read
[6]	CWE-89	Improper Neutralization of Special Elements used in an SQL Command ('SQL Injection')
[7]	CWE-416	Use After Free
[8]	CWE-190	Integer Overflow or Wraparound
[9]	CWE-352	Cross-Site Request Forgery (CSRF)
[10]	CWE-22	Improper Limitation of a Pathname to a Restricted Directory ('Path Traversal')
[11]	CWE-78	Improper Neutralization of Special Elements used in an OS Command ('OS Command Injection')
[12]	CWE-787	Out-of-bounds Write
[13]	CWE-287	Improper Authentication
[14]	CWE-476	NULL Pointer Dereference
[15]	CWE-732	Incorrect Permission Assignment for Critical Resource
[16]	CWE-434	Unrestricted Upload of File with Dangerous Type
[17]	CWE-611	Improper Restriction of XML External Entity Reference
[18]	CWE-94	Improper Control of Generation of Code ('Code Injection')
[19]	CWE-798	Use of Hard-coded Credentials
[20]	CWE-400	Uncontrolled Resource Consumption
[21]	CWE-772	Missing Release of Resource after Effective Lifetime
[22]	CWE-426	Untrusted Search Path
[23]	CWE-502	Deserialization of Untrusted Data
[24]	CWE-269	Improper Privilege Management
[25]	CWE-295	Improper Certificate Validation

Prinzipen für Security Engineering

- KISS: „keep it small and simple“
- erlaube viele Reviews
- keine „security by obscurity“
  - obskure Systeme
    - können unbekannte Sicherheitslöcher enthalten
    - können unerkannt manipuliert sein
  - *Kerckhoffs Prinzip*: Die Sicherheit eines kryptographischen Verfahrens darf nicht von der Geheimhaltung des Verfahrens abhängen
- Ferguson et al: professional paranoia

Beheben von Sicherheitslücken

Regelmäßige Wartung von

- Firmware,
- Betriebsysteme
- Programmen

Sicherheitskorrekturen anwenden

- SW hat ein Verfallsdatum

Unbekannte Sicherheitslücken: „zero days“

- CVEs
  - Common Vulnerabilities and Exposures
- CVSS
  - Common Vulnerability Scoring System
    - Base Metric:
      - exploitability
      - scope
      - impact
    - Temporal Metric
    - Environmental Metric

Hausaufgaben

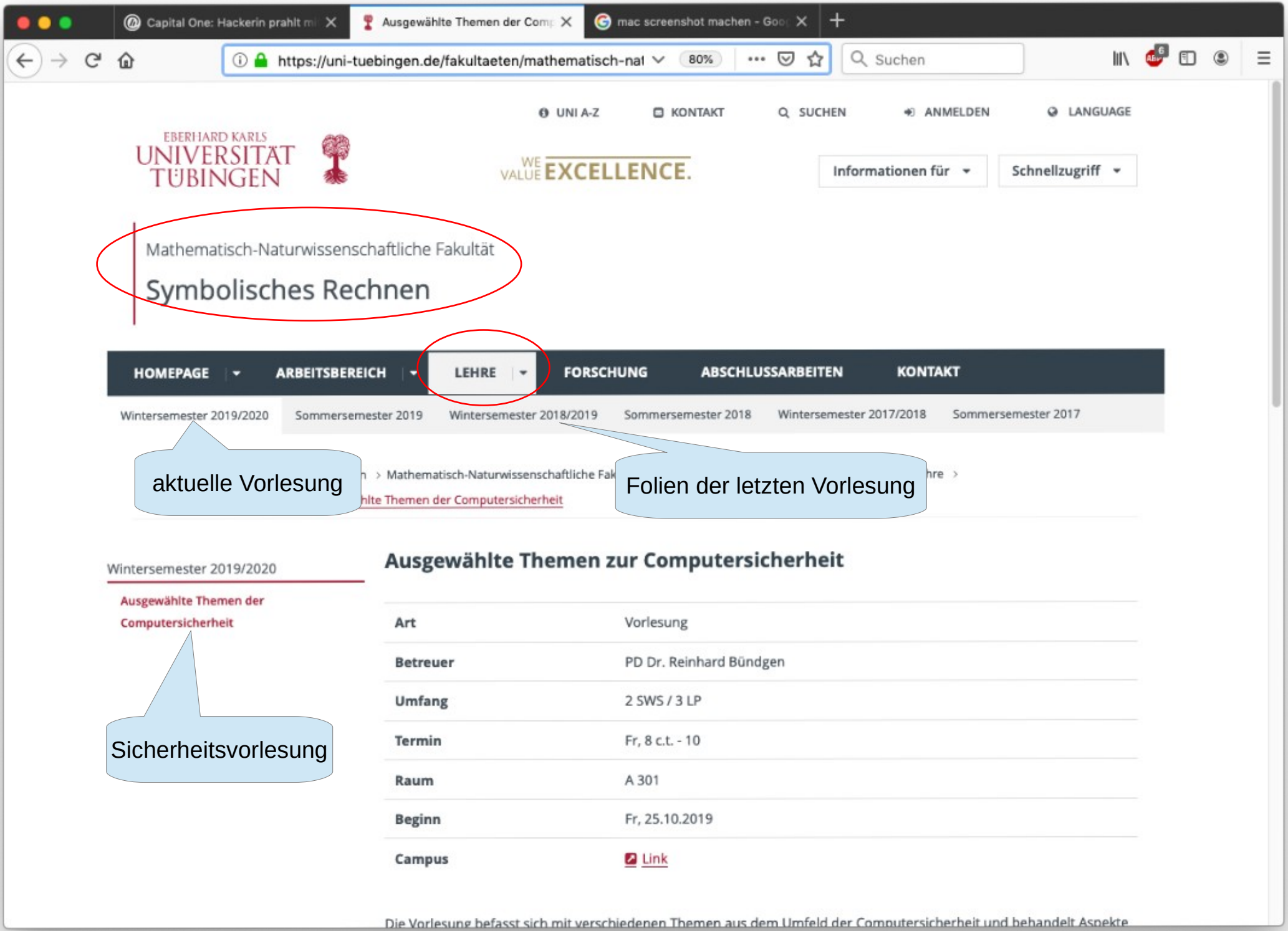
- Lesen Sie die OWASP Top 10 Vulnerabilities nach
- Lesen Sie die Beschreibungen von mindestens 5 der Top 25 CWE durch
- Schauen Sie sich Beispiele für CWE-78 „OS command injection“ an
- Betrachten Sie einen Sicherheitsmechnismus aus ihrem täglichen Leben und überlegen Sie gegen welche Angriffe er schützt und wie man ihn umgehen bzw „überlisten“ kann.

Inhalt der Vorlesung

1. Einleitung
2. Authentisierung
3. Autorisierung
   - theoretische Modelle
   - HW Konzepte
   - Unix Konzepte
4. Verschlüsselung
5. MACs & Signaturen
6. Schlüsselverwaltung
7. HSMs
8. PKCS #11
9. SSL/TLS
10. Sicherheit in der Cloud
11. Bitcoins
12. Quanten Computing

Literatur (Auswahl)

- C. Eckert: IT-Sicherheit, Oldenburgverlag
- N. Ferguson, B. Schneier, T. Kohno: Cryptography Engineering, Wiley 2010
- R. Anderson: Security Engineering, Wiley
- A. Beutelsbacher, H. Neumann, T. Schwarzpaul: Kryptographie in Theorie und Praxis, Teubner+Vieweg, 2010
- Neuigkeiten
  - Linux Weekly News (lwn.net)
  - Heise news
  - Schneiers news letter
  - Ars Technica


Capital One: Hackerin prahlt mi
Ausgewählte Themen der Comp
mac screenshot machen - Goo
https://uni-tuebingen.de/fakultaeten/mathematisch-nat
80%
Suchen
UNI A-Z
KONTAKT
SUCHEN
ANMELDEN
LANGUAGE
EBERHARD KARLS
UNIVERSITÄT
TÜBINGEN
WE VALUE EXCELLENCE.
Informationen für
Schnellzugriff
Mathematisch-Naturwissenschaftliche Fakultät
Symbolisches Rechnen
HOMEPAGE
ARBEITSBEREICH
LEHRE
FORSCHUNG
ABSCHLUSSARBEITEN
KONTAKT
Wintersemester 2019/2020
Sommersemester 2019
Wintersemester 2018/2019
Sommersemester 2018
Wintersemester 2017/2018
Sommersemester 2017
aktuelle Vorlesung
Folien der letzten Vorlesung
Mathematisch-Naturwissenschaftliche Fak
hlte Themen der Computersicherheit
Wintersemester 2019/2020
Ausgewählte Themen der Computersicherheit
Sicherheitsvorlesung
Ausgewählte Themen zur Computersicherheit
Art
Vorlesung
Betreuer
PD Dr. Reinhard Bündgen
Umfang
2 SWS / 3 LP
Termin
Fr, 8 c.t. - 10
Raum
A 301
Beginn
Fr, 25.10.2019
Campus
Link
Die Vorlesung befasst sich mit verschiedenen Themen aus dem Umfeld der Computersicherheit und behandelt Aspekte