Inhalte der Vorlesung

„IT-Sicherheit für Geistes- und Gesellschaftswissenschaften“

Sommersemester 2017

http://emsec.rub.de/teaching/courses/799/

Zielgruppe: Studenten nichttechnischer Fächer, z. B. Geistes- und Gesellschaftswissenschaften, Jura, Pädagogik

Lernziele: Es soll eine grundlegendes Verständnis für die Begriffe und Techniken der modernen IT-Sicherheit gelegt werden. Inhaltlich werden Grundlagen der Computertechnik, Klassifizierung der IT-Sicherheit, Grundlagen der Kryptographie, Benutzerauthentifizierung und der Schutz der Privatsphäre eingeführt.

Veranstaltungsform: 2 SWS Vorlesung + 2 SWS Übung, 5 ECTS

Zeiten: Vorlesung: Mittwoch, 12:15-13:45, ID 03/445
Übung: Mittwoch, 14:00-15:30, ID 03/445

Lehrende: Prof. Markus Dürmuth
Prof. Christof Paar (Verantwortlicher)
Dr. Bertram Poettering (Prof. Eike Kiltz)

Prüfungsform: Übungszettel (1-2wöchentlich), Klausur

Anmeldung: per Email an emsec+office@rub.de (Anmeldung ist obligatorisch)

Beschreibung Modulhandbuch:

Die Veranstaltung gibt eine Einführung in moderne IT-Sicherheit für Studenten ohne technisch-mathematische Vorbildung.

Die Veranstaltung ist in drei Themenblöcke gegliedert. Zunächst werden technische Grundlagen der Informatik in Form einer kompakten Einführung in Computer und Netze vermittelt. Im zweiten Teil werden grundlegende Begriffe der IT-Sicherheit und eine Einführung in die Kryptografie gegeben. Der dritte Teil beschäftigt sich mit der Privatsphäre und Benutzerauthentifizierung.

Die Benotung erfolgt anhand von regelmäßigen Übungszetteln und einer Abschlussklausur.

Inhalte

Block 1: Computer und Netze (BP/EK) 4 Wochen

Woche 1

- Information und ihre Darstellung:
- bits/bytes/strings/unicode
- Binärsystem, Dezimalsystem, Hex-Kodierung
- Rechnerstrukturen
- CPU / Hauptspeicher / Massenspeicher / Peripherie
- wie “rechnet” man damit (Zusammenspiel CPU/RAM)?

Woche 2

- Programmierkonzepte
- was ist ein Programm, Prozess? Was ist source code, binary code, compiler?
- Einfache Programmierbeispiele in imperativer Sprache (python?)
- Vergleich C vs. Python in hinblick auf Programmiersicherheit
- Beispiel: Notwendigkeit von range checks

Wochen 3+4

- Betriebssysteme
- Resourcenverwaltung, Userverwaltung und access control
- use cases: Windows/Linux/Android
- Netzwerke
- Client/server, peer-to-peer
- OSI-Modell, speziell Einordnung von Ethernet, IP, TCP
- DNS
- Beispiel-Sitzungen in HTTP, SMTP, ...
- sniffing, firewalls, network-based intrusion detection
- Web-basierte Angriffe via CSRF oder session-id stealing via Referer field

Block 2: Kryptographie und IT-Sicherheit

Grundlagen Kryptographie (CP) 4 Wochen

- Begriffserklärung: Kryptografie, IT-Sicherheit und „Privacy“
- Klassifizierung Kryptologie: Kryptografie und Kryptanalyse, symmetrische vs. asymmetrische Kryptografie
- Wie sicher können kryptografische Verfahren sein?
  Beweisbare Sicherheit, praktische Sicherheit, vollständige Schlüsselsuche, Langzeitsicherheit
- One-Time Pad
- Advanced Encryption Standard (die wichtigste symmetrische Chiffre)
- RSA (die wichtigste asymmetrische Chiffre)

Sicherheitsziele und deren Umsetzung (CP) 2 Wochen

- Sicherheitsziele: Geheimhaltung, Integrität, Authentizität, Beweisbarkeit, Identifikation
- Digitales Signaturen
- Message Authentication Codes (MACs)
- Hashfunktionen

Block 3: Schutz der Privatsphäre und Benutzerauthentifizierung (MD) 4 Wochen

Schutz der Privatsphäre (MD) ca. 2 Wochen

- Warum Privacy?
- Definition(en) von Privacy
- Angriffe gegen unsere Privatheit
- Anonymität im Web/TOR/BitCoin

Das Internet: Funktion und Angriffe (MD) ca. 1 Woche

- Wie funktioniert das Internet?
- Infrastruktur, TCP/IP, HTTP, DNS
- Angriffe gegen das Internet (DDoS, IP hijacking, DNS redirection)

Benutzerauthentifizierung (MD) ca. 1 Woche

- Sicherheit von Passwörtern
- Passwort Alternativen
- PGP/TrueCrypt