

Prerequisites for “Systems Security”

For the course “Systems Security”, you should have already participated in the following courses or in courses that roughly teach an equivalent topic:

- Language based Security (CS4105) or Software Security (UT201600051) and
- Security and Cryptography (IN4191) and
- Network Security (ET4397IN) or Internet Security (192654000) and
- A bachelor level Operating Systems course

Should you miss one or more of the courses, we recommend that you do a self study in the relevant topics. To assist you with that, we have compiled a list of useful books which should support you with that. Of course, you are free to choose a different way to studying the relevant topics.

Language/Software security

- General security bug hunting (**BugHunter**)

Security and Cryptography

- Signatures (**Applied Cryptography** chapters 1,2,3,4,11)
- Hash functions (**Applied Cryptography** chapters 1,2,3,9)
- Symmetric key algorithms (**Understanding Cryptography**, chapters 4,5)

Network Security or Internet Security

- The TCP/IP protocol family (**TcpIp**)
- HTTP (**TcpIp**)
- TLS (**TlsBook**)
- Network sniffers such as wireshark and tcpdump (**WireShark**)
- Attacking networking protocols (**AttackNet**)
- General Hacking (**ArtExploitation**)

Operating Systems

- A good understanding of the general structure of the Linux operating system. (**OpSys** chapters 1,2,3)
- The C programming language (**OpSys**)
- The networking API (**NetProg**)
- The permission model as well as authorization and authentication (**OpSys** chapter 15)

Books

- **OpSys** Operating Systems: Internals and Design Principles by William Stallings
<https://www.amazon.de/Operating-Systems-Internals-Design-Principles/dp/0134670957/>
- **NetProg** The Definitive Guide to Linux Network Programming by Nathan Yocom
<https://www.amazon.de/Definitive-Guide-Network-Programming-Experts/dp/1590593227/>
- **TcpIp** TCP/IP Guide - A Comprehensive, Illustrated Internet Protocols Reference - by Charles M. Kozierok
<https://nostarch.com/tcpip.htm>
- **WireShark** Wireshark Network Analysis (Second Edition): The Official Wireshark Certified Network Analyst Study Guide by Laura Chappell <https://www.amazon.de/Wireshark-Network-Analysis-Second-Certified/dp/1893939944/>
- **Applied Cryptography** Handbook of Applied Cryptography by Alfred J. Menezes, Paul C. van Oorschot and Scott A. Vanstone <http://cacr.uwaterloo.ca/hac/>
- **TlsBook** Implementing SSL/TLS by Joshua Davies <https://www.amazon.de/Implementing-SSL-TLS-Joshua-Davies/dp/0470920416/>
- **AttackNet** Attacking Network Protocols - A Hacker's Guide to Capture, Analysis, and Exploitation by James Forshaw <https://nostarch.com/networkprotocols>
- **ArtExploitation** Hacking, 2nd Edition - The Art of Exploitation by Jon Erickson
<https://nostarch.com/hacking2.htm>

- **BugHunter** Bug Hunter's Diary - A Guided Tour Through the Wilds of Software Security by Tobias Klein
<https://nostarch.com/bughunter>
- **Power Analysis Attacks: Revealing the Secrets of Smart Cards.** Stefan Mangard, Elisabeth Oswald, and Thomas Popp. Springer-Verlag New York, Inc., Secaucus, NJ, USA, 2007.
<https://www.springer.com/de/book/9780387308579>
- **Understanding Cryptography.** Christof Paar. Springer, 2009.
<https://www.springer.com/de/book/9783642041006>