Revision Part 1

Exam process

- Exam weight: 40%
- Answer THREE questions from FOUR
- Each question is worth a total of 20 marks

Type of questions

- Knowledge-based
  - Target basic information
- Comprehension
  - Target the understanding of what information means
- Application
  - Target the knowledge to problem solving

Topics Part 1

- Applied cryptography
- Systems and security engineering
- Information security goals
- Access control
- Network security
- OS security
- Foundations of model checking

+ All topics covered in labs

Cryptography

- Symmetric and asymmetric encryption
  - How do they work?
  - What do they offer?
  - When do we use them?
- We also had a look at hashes, MACs, digital signatures
- Attacks on cryptosystems

References

- William Stallings, Cryptography and Network Security, Principles and Practise, 5th edition
- All in one - CISSP, 5th edition, Chapter on Cryptography
- Security Engineering, Chapter on Cryptography, https://onesearch.lancaster-university.uk/permalink/f/fvnevo/TN_cdi_proquest_ebookcentral_EBC6412239

Security fundamentals

- Common information security goals (CIA)
- Security engineering is '… about building systems to remain dependable in the face of malice, error or mischance' [1]
- Security principles to achieve the information security goals

References

[1] Security Engineering: https://onesearch.lancaster-university.uk/permalink/f/fvnevo/TN_cdi_proquest_ebookcentral_EBC6412239

[2] Security in Computing, 5th Edition, By Charles P. Pfleeger, Shari Lawrence Pfleeger, Prentice Hall, Chapter 1, https://ptgmedia.pearsoncmg.com/images/9780134085043/samplepages/9780134085043.pdf

[3] All In One – CISSP Exam Guide, 5th Edition by Shon Harris. ISBN 978-0-07-160217-4 – Chapter 5 (Available from the library)

[4] Systems Engineering Fundamentals, DoD, January 2001, https://ocw.mit.edu/courses/aeronautics-and-astronautics/16-885j-aircraft-systems-engineering-fall-2005/readings/sefguide_01_01.pdf

[5], J. Saltzer and M. Schroeder, Proceedings of the IEEE, The Protection of Information in Computer SystemsVol. 63, No. 9, September 1975. https://web.mit.edu/Saltzer/www/publications/protection/State.html

[6] William Stallings, Network and Internetwork Security: Principles and Practice. Englewood Cliffs, NJ: Prentice-Hall International, 1999. (Available from the library)

AAA

- Identification
  - Identity management
- Authentication
  - Ways of authenticating
  - Techniques to improve security against attacks
- Authorisation
- Accountability
- Access control (models and policies)

References

- Security Engineering, Chapter on Access Control, https://onesearch.lancaster-university.uk/permalink/f/fvnevo/TN_cdi_proquest_ebookcentral_EBC6412239
- All in one - CISSP, 5th edition, Chapter on Access Control
- NIST SP 800-162 https://nvlpubs.nist.gov/nistpubs/specialpublications/NIST.SP.800-162.pdf
- NIST SP 800-178 https://nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.800-178.pdf
- ANSI INCITS 359-2004 https://www.cs.purdue.edu/homes/ninghui/readings/AccessControl/ANSI+INCITS+359-2004.pdf

Network Security

- OSI
- Firewalls
- Security protocols
- Overlay anonymity protocols

References

- CISSP All in One. Chapter 7 Telecommunications and Network Security.
- Internet Protocol RFC 791
- Transmission Control Protocol RFC 793
- IPSec
- The TOR Network

OS security

- OS and ways of protection
- Trusted Platforms Modules (TMP)
- Processes/threads
- Technical attacks

References

- Andrew S. Tanenbaum, “Modern Operating systems”. Chapter 9
- Shon Harris, All in one CISSP, Chapter 5 on Security Architecture and Design.
- Lampson, B. W. (1973). A note on the confinement problem. Communications of the ACM, 16(10), 613-615.

Foundations of model checking

- The model checking process
- Transitions system
- Type of properties
- LTL

Reminder!

+ All topics covered in labs

Example questions