Cybersecurity

Cybersecurity/CNS exam

17th June 2022

Syllabus 2021-22

1. Write first name, surname, matriculation and number of homeworks done top-right on the first page.

2. Define strong collision resistance. Is it sufficient for making a hashing function of cryptographic quality? If not, what should we additionally require? (penalties for unnecessary additional requirements) [3pt]

3. Define the so-called birthday bound. Are strongly collision resistant hashing functions affected? Elaborate. [2pt]

4. Compare keyed hashing functions to unkeyed hashing functions: pros and cons. [3pt]

5. Forgeries against digital signatures
   - 5.1 Define the types of forgery adversaries can set up against digital signatures. [2pt]
   - 5.2 Describe a procedure based on the birthday bound to make a selective forgery. [3pt]

6. People often say that *integrity* is the requirement for not allowing unauthorised modifications in a document. This sentence is not completely exact. Formulate it more precisely, clarifying powers and limits of the recipient of a document subject to the integrity requirement. [2pt]

7. Recall the general architecture of the Kerberos protocol. Can it be used on whatever type of network (LAN, MAN, WAN)? [3pt]

8. Digital certificates.
   - 8.1. Discuss the necessity of a CRL. [1pt]
   - 8.2 What is OCSP and what issues does it create? [2pt]
   - 8.3 Why do digital certificates expiry? [1pt]

9. Firewalls
   - 9.1 What is an application level firewall? [1pt]
   - 9.2 You are a home user with a strong Internet connection, however the modem/router is not providing any firewall and NAT. The Internet provider assigned to you the IP range 180.0.1.0/26. In your iptables the default policy is accept. Filter incoming connections on ports 121,122, 123, but do not block conversations using these ports but locally initiated. [4pt]
   - 9.3 While using iptables what are the main differences between network protection and personal firewalling? [2pt]

10. Describe a case of use where both TLS and IPsec are used by the same host at the same time. [2pt]