Cybersecurity/CNS exam

14th July 2022

Syllabus 2021-22

Please write in a large and understandable handwriting, using a pen. Any pencil portions will be skipped. If necessary, use capital or block letters.

1. Write the name of the exam, first name, surname, matriculation and number of homeworks done in the top line of the first page.

2. Define *weak collision resistance*. Is it needed for making a hashing function of cryptographic quality? What is the difference with *second preimage resistance*? [3pt]

3. Why do we want hashing *fingerprints* longer than 160 bits? [3pt]

4. Compare *keyed hashing functions* to *digital signatures*: pros and cons. [3pt]

5. Explain how *authenticity* is a strengthening of *integrity*. [3pt]

6. What are the differences between *integrity verification* and *digital signature verification*? Discuss in depth. (Superficial approaches will be penalised). [3pt]

7. Define Shamir's secret sharing technique (n, k), where n is the number of participants and $1 < k \leq n$, where k is the threshold. Given three points, will these be sufficient for $k = 3$? Discuss. [3pt]

8. Public keys checking.

   8.1. Define OCSP. How is it better than CRLs? [2pt]

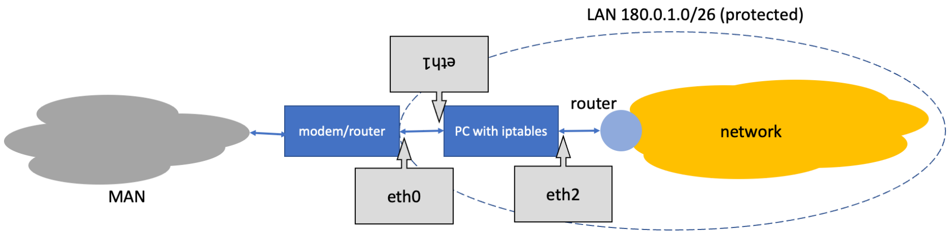
   8.2. Why does OCSP cause privacy issues? [2pt]

9. RSA: What happens if we exchange public and private keys? [2pt]

10. Firewalls

    10.1. What is the difference between packet filtering and session filtering? [2pt]

    10.2. You are a home user with a strong Internet connection, however the modem/router - offering only wired connection - is not providing any firewall/NAT. Carefully check the figure.



Default iptables policy is ALLOW and you are asked to protect ALL the LAN blocking bidirectional http/https traffic to/from site 140.11.201.23. Write the corresponding iptables rules. [4pt]

    10.3. Can a session filtering firewall help confidentiality? (It cannot guarantee it, but some policies may help). Discuss. [2pt]