Cybersecurity/CNS exam

8th September 2022 - Syllabus 2021-22 - 120 minutes

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

0. Write the name of the exam, first name, surname, matriculation and number of homeworks done in the top line of the first page. (I will save time).

1. Collision resistance

1.1. Define *strong* and *weak collision resistance*. [2pt]

1.2. Why does the strong one imply the weak one? [2pt]

1.3. Consider the mod *s* function (% *s*), where *s* is a large random prime number. Why isn't it cryptographic? Provide **all** reasons. [2pt]

2. RSA

2.1. When is RSA normally used for confidentiality and why? [1pt]

2.2. What are the keys (private and public) used for RSA and what relationship binds them? [2pt]

2.3. What is OS2IP? Describe it in detail. [3pt]

3. Authentication

3.1. Define SPEKE and all parameters/options that occur in it. [2.5pt]

3.2. In a web application, authentication is made by requesting username and password to the user, who connects via https. Design the details of authentication, clarifying how the server checks the user's credentials. [3.5pt]

4. Explain the difference between a key and a password. [1pt]

5. A VPN is based on IPSec tunnelling. What partial (meta)information is available to an eavesdropper that intercepts the packets? [2pt]

6. Describe strengths and limits of inserting a timestamp within a message of some cryptographic protocol. [2pt]

7. Timestamp Authority

7.1. What is a Timestamp Authority (TSA) and what function does it perform? [1pt]

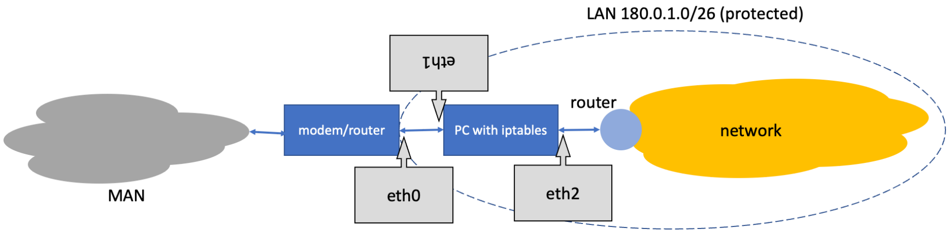
7.2. Illustrate a way of timestamping a digitally signed message. [2pt]

7.3. Illustrate a way of timestamping a message without digital signature but with integrity. [2pt]

8. Firewalls

8.1. What is the difference between a personal firewall and a perimeter firewall? [1pt]

8.2. 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 block all connections to the pc running iptables (and vice versa) except those initiated inside the LAN. Write the corresponding iptables rules. [3pt]