Cybersecurity/CNS exam

3 February 2023

- Don't use pencils
- Have a good (and big) handwriting
- Use English
- Answers without a motivation will be not considered

0. Write name, surname, matriculation and number of delivered homeworks in the top right corner of first page

1. *Authenticity* versus *authentication*. Does one contain the other? Or does the other contain one? Any differences? Carefully explain. [3 points]

2. **Symmetric encryption/decryption** [12.5 points]
   - 2.1. Describe the architecture of OFB, both for encryption and for decryption. [2 points]
   - 2.2. Does OFB need to use a randomly generated IV at any encryption? Why? [2 points]
   - 2.3. What is a KDF and why is it useful? [2 points]
   - 2.4. What is the effect of the following command line string?
     ```
     echo "SilverSurfer" -n | openssl enc -aes-128-cbc -p -out out.enc
     ```
     Carefully describe in detail. [3.5 points]
   - 2.5. If in CBC the attacker flips the third bit of the first ***ciphertext*** *block*, and no integrity mechanism is in place, what is the total effect of that in Bob's reconstructed **plaintext** message? Discuss. [2 points]
   - 2.6. If in the CBC it is Alice who inverts the third bit of the first ***plaintext*** *block*, and no integrity mechanism is provided, what is the total effect of this intervention in Bob's reconstructed **plaintext** message? Discuss. [1 points]

3. **Digital certificates** [5 points]
   - 3.1. Compare CRLs to OCSP. [2 points]
   - 3.2. What is OCSP stapling and why is it done? [1 point]
   - 3.3. Why don't we need the https protocol but can use plain http in retrieving a certificate? [2 points]

4. **Digital signatures** [6 points]
   - 4.1. Alice and Bob digitally sign the same document M, which is a contract. If Alice is the first signer is there a difference whether Bob signs M or M with Alice's signature? Discuss. [2 points]
   - 4.2. If the verification of a digital signature fails (without diagnostics, so we don't know the reason for the failure), what is it correct to infer? Discuss. [2 points]
   - 4.3. The following sentence contains a poorly posed (and therefore incorrect) question, written solely to confuse ideas.
     If Alice wants to digitally sign a document, but she doesn't know the public key, how should she do it?
     Discuss why such a question should not be asked. [2 points]

5. **Firewalls** [5.5 points]
   - 5.1. Compare blacklisting with whitelisting and discuss the impact of those policies on iptables. [2 point]
   - 5.2. Suppose iptables is running on host H, which is protecting a LAN. Write appropriate rules so that: a) H does not allow any incoming or outgoing network connections (can only be configured using the local console) b) H allows any connection from the LAN to the Internet, but does not allow opening connections from the Internet to the LAN. [3.5 points]