# 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]

1 AUTHENTICATION IS THE PROCESS OF VERYFING THE IDENTITY OF A SUBJECT, TYPICALLY THROUGH CREDENTIALS OR CRYPTOGRAPHIC PROTOCOLS. AUTHENTICITY IS THE PROPERTY THAT A MESSAGE OR DOCUMENT IS GENUINE.

SUCCESSFUL AUTHENTICATION PROVIDES AUTHENTICITY. THE FIRST ONE IS THE PROCESS, WHILE THE SECOND THE RESULTING PROPERTY.

2.1 IN OFB, THE BLOCK CIPHER IS USED TO GENERATE A KEYSTREAM THAT IS XORED WITH THE PLAINTEXT.

FOR ENCRYPTION, THE IV IS ENCRYPTED WITH THE SECRET KEY TO PRODUCE THE FIRST KEYSTREAM BLOCK, WHICH IS XORED WITH THE PLAINTEXT TO FORM THE CIPHERTEXT. THE SAME OUTPUT (NOT THE CIPHERTEXT) IS FED BACK INTO THE BLOCK CIPHER TO PRODUCE THE NEXT KEYSTREAM BLOCK. FOR DECRYPTION WE USE THE SAME PROCESS, BUT THE KEYSTREAM BLOCK IS XORED WITH THE CIPHERTEXT TO OBTAIN THE PLAINTEXT.

SINCE ENCRYPTION AND DECRYPTION USE THE SAME PROCESS, OFB WORKS AS A SYNCHRONOUS STREAM CIPHER.

2.2 YES, BECAUSE THE IV DETERMINES THE KEYSTREAM. IF TWO ENCRYPTIONS USE THE SAME KEY AND IV, THE SAME KEYSTREAM IS PRODUCED.

$$C_1 \oplus C_2 = (K \oplus P_1) \oplus (K \oplus P_2) = P_1 \oplus P_2$$

2.3 A KEY DERIVATION FUNCTION (KDF) IS A CRYPTOGRAPHIC FUNCTION THAT DERIVES ONE OR MORE SECRET KEYS FROM AN INITIAL SECRET. IT TYPICALLY USES HASH FUNCTIONS AND MAY INCLUDE A SALT.

KDFs ARE USEFUL BECAUSE THEY TRANSFORM ARBITRARILY SIZED SECRETS INTO STRONG, UNIFORMLY DISTRIBUTED KEYS OF THE REQUIRED LENGTH. THEY CAN ALSO GENERATE MULTIPLE INDEPENDENT KEYS FROM THE SAME SECRET.

2.4 THE COMMAND TAKES THE STRING "SILVERSURFER" (WITHOUT APPENDING A NEW LINE) AND ENCRYPTS IT WITH AES-128 IN CBC MODE USING OPENSSL. THE CIPHER TEXT IS WRITTEN INTO THE FILE OUT.ENC.

2.5 THIS HAS TWO EFFECTS. THE FIRST PLAINTEXT BLOCK WILL BE COMPLETELY CORRUPTED, SINCE DECRYPTION OF A MODIFIED CIPHERTEXT BLOCK IS UNPREDICTABLE. THE SECOND PLAINTEXT BLOCK WILL DIFFER IN EXACTLY THAT SINGLE BIT POSITION, BECAUSE WE USE $C_1$ TO OBTAIN $P_2$.

2.6 THE ENCRYPTION PROCESS SIMPLY ENCODES THIS MODIFIED BLOCK, AND BOB RECONSTRUCTS THE ALTERED PLAINTEXT BLOCK EXACTLY AS MODIFIED BY ALICE, WITH NO ERROR PROPAGATION.

3.1 CRLs ARE LISTS ISSUED PERIODICALLY BY A CA, CONTAINING THE SERIAL NUMBERS OF CERTIFICATES THAT HAVE BEEN REVOKED. CLIENTS MUST DOWNLOAD AND CHECK THE CRL TO VERIFY CERTIFICATE VALIDITY.

OCSP, INSTEAD, ALLOWS CLIENTS TO QUERY AN ONLINE RESPONDER IN REAL TIME TO OBTAIN THE REVOCATION STATUS OF A SPECIFIC CERTIFICATE. IT PROVIDES FRESHER INFORMATION AND AVOIDS LARGE DOWNLOADS.

3.2 OCSP STAPLING IS AN OPTIMIZATION OF OCSP IN WHICH THE WEB SERVER, INSTEAD OF THE CLIENT, QUERIES THE OCSP FOR A CERTIFICATE VALIDITY. THE SERVER THEN STAPLES THE RESPONSE TO THE TLS HANDSHAKE AND SENDS IT TO THE CLIENT.

3.3 A CERTIFICATE IS NOT SECRET INFORMATION: IT CONTAINS A PUB KEY AND IDENTITY DATA SIGNED BY A TRUSTED CA. DURING THE TLS HANDSHAKE, SERVERS SEND THEIR CERTIFICATES IN CLEAR TEXT TO ANY CLIENT. THEREFORE, USING PLAIN HTTP IS SUFFICIENT.

4.1 IF BOTH SIGN M INDEPENDENTLY, WE GET TWO VALID SIGNATURES ON THE SAME DOCUMENT, BUT BOB'S SIGNATURE DOESN'T CONFIRM ALICE'S. IF BOB SIGNS $(M \| S_A)$, HE CERTIFIES BOTH THE DOCUMENT AND ALICE'S SIGNATURE, PROVING ORDER AND ACKNOWLEDGMENT.

4.2 THE ONLY CORRECT INFERENCE IS THAT THE AUTHENTICITY AND INTEGRITY OF THE MESSAGE CANNOT BE GUARANTEED.

4.3 ALICE ONLY NEEDS HER PRIV KEY TO SIGN THE DOCUMENT. THE PUB KEY IS REQUIRED FOR THE VERIFICATION.

5.1 BLACKLISTING ALLOWS ALL TRAFFIC (DEFAULT POLICY ACCEPT) EXCEPT WHAT IS EXPLICITLY DENIED (DROP), WHILE WHITELISTING BLOCKS ALL TRAFFIC (DEFAULT POLICY DROP) EXCEPT WHAT IS EXPLICITLY ALLOWED (ACCEPT).

5.2 a
```
IPTABLES -P INPUT DROP
IPTABLES -P OUTPUT DROP
IPTABLES -P FORWARD DROP
```

b
```
IPTABLES -P INPUT DROP
IPTABLES -P OUTPUT DROP
IPTABLES -P FORWARD DROP

IPTABLES -A FORWARD -i eth1 -o eth0 -j ACCEPT
IPTABLES -A FORWARD -i eth0 -o eth1 -m STATE --CTSTATA
  ESTABLISHED, RELATED -j ACCEPT
```