Computer and network security
Sicurezza nelle reti e nei sistemi informatici
Crittografia e sicurezza delle reti

Exam of 5th February 2021, a.y. 2020-21. Time: 2 hours
Outcomes will be sent via email within three weeks

1. ***Write the answers in the text area from Exam.net***
2. ***TEXT IN NON-ENGLISH: 2 penalty points***
3. ***UNREADABLE WRITING will be skipped***
4. ***All questions of an exercise must be answered with no more than one page of text. Be concise and focus on what a question is asking.***

Q1: **General concepts [5/30]**

Evaluate the truth of the following assertions [correct: +0.5; wrong: -0.25; no answer: 0]. The answer should be “True” or “False”: e.g, write “Q1.X True” to answer “True” to the X-th question. Write one answer for each line. Assertions:

- Q1.1: All operations modes for symmetric block ciphers require to have an input with a size that is multiple of the cipher block size.
- Q1.2: 2-DES is significantly more secure than DES
- Q1.3: 3-DES is significantly more secure than 2-DES
- Q1.4: Given $\{(x_1, y_1), (x_2, y_2)\}$, where x_j is a plaintext message and y_j is the encrypted message of x_j using a fixed symmetric key k, i.e., $y_j = enc_k(x_j)$, and j in [1,2], then if we find a key k’ such that $y'_1 = enc_{k'}(x_1) = y_1$ then we are sure that k’ = k and thus $y'_2 = enc_{k'}(x_2) = y_2$
- Q1.5: In RSA, if we reuse the same private and public keys across different sessions then we can achieve forward secrecy
- Q1.6: Differently from the Diffie-Hellman Key Exchange algorithm, the Elgamal encryption scheme is not vulnerable to a MITM attack.
- Q1.7: In real-world, we only use protocols that have mathematical proofs of their security, i.e., we know that no attack will ever exist
- Q1.8: DSA is based on RSA
- Q1.9: DSS provides both message authentication and message confidentiality
- Q1.10: IPSec only handles TCP traffic, leaving UDP traffic unprotected.

Q2: **Symmetric ciphers [6/30]**

- Q2.1 [2/30] Define the main steps performed by AES when encrypting a block. Be concise: do not write more than half of a page.
- Q2.2 [2/30] During encryption, the steps performed by AES are conceptually more complex than the steps performed by RSA. Hence, why do we say that AES is generally faster than RSA?
- Q2.3 [2/30] Consider AES128-CBC:
    a. Why do we use an Initialization Vector (IV)?
    b. Given (k, y, IV) where y = AES128-CBC-Encrypt$_k$(x) and IV is the initialization vector used during CBC, then what would happen during decryption if an attacker is able to manipulate the IV but not (k, y)?

Q3: **Random Number Generators [5/30]**

- Q3.1 [2/30] Define and discuss the main types and desired properties of Random Number Generators.

- Q3.2 [3/30] Are these functions good candidates for CSPRNG?

    a. XOR(S, X) where S is obtained by calling a secure CSPRNG and X is a public fixed value equal to 0xCAFECAFE. Discuss two scenarios: (1) a new value S is generated at each invocation of the function, and (2) the value S is kept fixed across different invocations.

    b. $AES_K(X)$ where X is a value generated by calling a secure CSPRNG and K is a public value initially equal to 0xCAFECAFE that is incremented by 1 after each invocation of the function. Discuss two scenarios: (1) a new X is generated at each invocation of the function, and (2) X is kept fixed across different invocations.

Q4: **Data integrity, data origin, and authentication [8/30]**

- Q4.1 [2/30] Suppose you receive (x, s) where x is a message and s is the signature of x generated by a user that is claiming to be Bob. The user is also sending to you his public key. How can you be sure that the message was actually generated by Bob and not by an attacker? Present a technical solution that may prevent this attack.
- Q4.2 [3/30] Explain what is a ticket in the context of authentication protocols. Discuss how tickets are used in Kerberos v4.
- Q4.3 [3/30] Alice and Bob have available a secure cryptographic hash function and a shared secret key. Additionally, their clocks are synchronized. Design a scheme that allows Alice to authenticate with Bob, i.e., one-way authentication. Carefully discuss the requirements of your scheme and possible weaknesses that your approach may have.

Q5: **Iptables [6/30]**

Assume that the iptables firewall is running on host H, having a network interface eth1 (IP: 192.168.0.1) connected to an internal LAN (IP: 192.168.0.0/24: the LAN is protected by H) and a network interface eth2 (IP: 151.100.5.5) connected to Internet. Assume that the default policy for all built-in chains is DROP.

- Q5.1 [2/30] What is the difference between chains and tables?
- Q5.2 [2/30] Explain the difference between these two rules:

    - `iptables -A FORWARD -o eth2 --dport 443 -p tcp -m state --state NEW,ESTABLISHED,RELATED -j ACCEPT`
    - `iptables -A OUTPUT -o eth2 --dport 443 -p tcp -m state --state NEW,ESTABLISHED,RELATED -j ACCEPT`

- Q5.3 [2/30] Explain the effect of the following rule:

    - `iptables -A INPUT -p tcp -i eth1 --dport 1024:65535 --sport 22 -m state --state ESTABLISHED -j ACCEPT`