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

Exam of 11th January 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: HMAC is a cryptographic hash function
- Q1.2: SHA-3 is not vulnerable to the birthday paradox
- Q1.3: Diffie-Hellman Key Exchange (DHKE) is based on a trapdoor function
- Q1.4: RSA is based on a trapdoor function
- Q1.5: RSA is insecure and should not be used
- Q1.6: A password using 14 chars is always more secure than a password using 12 chars
- Q1.7: Kerberos v4 is based mainly on asymmetric ciphers
- Q1.8: AES can encrypt only a fixed amount of bits
- Q1.9: 3-DES can encrypt an arbitrary amount of bits
- Q1.10: Static DHKE in SSL is secure against a MITM attack

Q2: **RSA [6/30]**

- Q2.1 [2/30] Present in detail the main ideas behind RSA encryption/decryption.
- Q2.2 [2/30] Discuss in detail at least two attacks against a textbook implementation of a RSA encryption/decryption.
- Q2.3 [2/30] Discuss in detail how RSA can be used for implementing a digital signature scheme. Also, present the main ideas behind one standard of your choice for an RSA-based digital signature scheme.

Q3: **Cryptographic hash functions [5/30]**

- Q3.1 [2/30] Define and discuss the security requirements needed by a hash function in order to be considered suitable for security purposes.
- Q3.2 [3/30] Are these functions good candidates for a new cryptographic hash function?
    a. f(x) = XOR(x, r) || r
    b. f(x) = SHA-3(XOR(x, r)) || r

    where x is the message, r is a random number (same number of bits of x), XOR is the bitwise exclusive or operator, || means concatenation. Motivate your answer with respect to the security requirements presented in Q3.1.

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

- Q4.1 [2/30] Suppose that a web server is publishing a file that you want to download. To help you trust the content of the file, the web server is publishing also the SHA-3 checksum computed over the content of the file. Hence, you can easily locally compute the SHA-3 checksum of the file (after downloading it) and compare the obtained hash value with the one published by the web server. Discuss the security of this approach with respect to data integrity and data origin.
- Q4.2 [3/30] Suppose that a user chooses a secret key by randomly typing 16 times on a keyboard. Assume that each character typed in can be represented using 1 byte. Discuss the security of this secret key: e.g., is it secure as a 128-bit random number? is there any benefit with respect to a 128-bit random number when using the secret key as a password for authentication?
- Q4.3 [3/30] Suppose that Bob knows the public key pk(A) of Alice and that the private key pr(A) of Alice has not been compromised. Alice and Bob agreed on the special secret message X = "Bazinga!". For one-way authentication, Alice sends to Bob $\text{Enc}_{pr(A)}(X)$. Bob decrypts the message using the public key pk(A) of Alice, checks the validity of the message, and authenticates Alice. Discuss the security of the protocol and possible improvements.

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] Define suitable rules to allow an HTTP server running on the machine 192.168.0.55 to correctly serve requests from the Internet.
- Q5.2 [2/30] Explain the difference between the FORWARD, INPUT, and OUTPUT chains, presenting concrete examples (at least one for each chain) (you may consider at your choice host H, hosts from the internal LAN, and external hosts from the Internet).
- Q5.3 [2/30] Define suitable rules for allowing users of the LAN to browse the web only in the case of HTTPS connections (HTTP traffic running via the standard port should be not allowed) using a standard browser.