Network Security (ROL) - Exam: June 2021

ONLINE EXAM - General instructions

1. Submit the exam via Moodle before the deadline: **June 13rd, 10:00**.

    - Submitting the exam correctly is strictly in your responsibility.
    - Submit in time, do NOT wait for the last minutes to submit. You can continuously submit before the deadline, and only the last submitted document is considered for grading. No reason (e.g., technical problems, clock desynchronization) will be accepted as an excuse if you do not submit in time.
    - The students that do not submit the exam are considered absents.

2. Your answer must be a **.pdf file, submitted via Moodle** in the corresponding section and named **group_surname_firstname.pdf**. The first page of the exam file must contain your name, group, and a list of unsolved exercises (e.g.,: *Unsolved exercises: 1(a), 1(c), 3(b).* or -).

    - It is up to how you write the exam: scan of hand-written papers (easily readable!), Word / LaTeX export to pdf, etc.
    - Take care to have a valid final .pdf file, and all exercises to be easily identifiable!

3. Partial scores are awarded. For wrong answers at the written exam you will NOT be subtracted any extra points.

4. To pass the exam, **it is mandatory to participate in both the written and oral exam and obtain minimum 22.5 points in the final exam and minimum 45 points as the final grade** (this includes the points granted for the activities during the year but excludes the bonus, which will only be granted in case of passing the exam).

5. For the oral exam:

    - It is your responsibility to check the schedule for the oral exam (day / approx. hour) and any other information regarding the oral exam.
    - You must connect **audio-video using your institutional account in Teams**.
    - You must present **an identification document** (preferably the university card, with a photo). It is your responsibility to hide other data available on the document if you do not want to make them public!
    - Every exercise that you are granted points for at the written exam but you cannot explain at the oral exam will cause a **subtraction of the doubled allocated points for the exercise**.
    - The students that submit the written exam and are absent at the oral exam will have the final grade 4.
    - If for special reasons you cannot connect with video, you have to announce in time before the oral exam via e-mail (*ruxandra.olimid@fmi.unibuc.ro*).
    - Write on the first page of the written exam if you have restrictions wrt the hours to participate in the oral exam.

Post any questions you might have during the exam on the forum - *Exam* section. Follow up the forum for answers. **Do NOT post solutions or hints!**

Good luck!

ONLINE EXAM - Exercises

1. **True of False**

   Respond with true or false. If the claim is false, make it true by enforcing a minimal change (keep the same context, but do not simply negate).

   Example: RC4 is used as a building block in CCMP.
   Expected answer: False. AES is used as a building block in CCMP.

   (a) 0x5468617473206D79204B756E67204675 can be a valid packet sequence number[1] for WPA/TKIP. **(2p)**

   (b) In a WPA2-Personal (WPA2-PSK) network of 25 hosts there exist 25 distinct CCMP encryption keys. **(2p)**

   (c) The MAC header in WPA2/CCMP is input for the computation of the MIC. **(2p)**

   (d) A direct purpose of the Packet Number in the CCMP header is to protect against impersonation attacks. **(2p)**

   (e) SAE in WPA3 is a direct measure of protection against offline dictionary attacks. **(2p)**

   (f) 208014829537140 can be an IMSI issued by a Romanian mobile operator. **(2p)**

   (g) In GSM, there are 2^{256} possible distinct permanent subscriber keys. **(2p)**

   (h) The keys used for AS protection can be refreshed without the need of changing the keys used for NAS protection.**(2p)**

   (i) Both the UE and the eNodeB know the value of K_{ASME} in a successful run of AKA. **(2p)**

   (j) Public-key cryptography is used in 5G to sign the response of the UE to the authentication challenge in 5G-AKA. **(2p)**

2. **WPA2 Security**

   You are applying for a network security expert position at the well-known company *UB Networks*. At the interview, some of the questions refer to WPA2/CCMP security. Argue about each of them independently (e.g., question (b) is independent of (a)).

   (a) Briefly explain the consequences of the Pairwise Master Key (PMK) leakage (1-2 paragraphs). **(5p)**

   (b) Briefly explain the consequences of the EAPOLMICKey leakage (1-2 paragraphs). **(5p)**

   (c) Assume that the AP has a bug such that any randomization it can produce is up to 32-bits of entropy. How does this affect WPA2 security? **(5p)**

   (d) *UB Networks* is worried about the consequences that KRACK attack might have had against devices used within its network or by its employees, in the terms of CVE-2017-13080. Choose a specific vendor (e.g., Android, Apple, Alcatel, Intel), then briefly state the past and present impact of CVE-2017-13080 with respect to your choice. Refer to online sources for more information. **(5p)**

[1] also known as a counter, or IV

3. **Mobile Consultant**

You work as a security consultant for the telecom company *PrivTel Ro*. The company wants to learn more about the security and privacy of their subscribers because they do not want to lose their customers' credibility. That is why they ask you to write a short report.

(a) To write the report, you classify possible adversaries into *insiders* and *outsiders*. Explain what actions each of the two adversarial types can perform and give examples of possible attacks in the given context. **(2x3p)**

PrivTel Ro wants to improve the Authentication and Key Agreement (AKA) mechanism so that it does not allow the IMSI transmission in clear. They propose the following solution:

1. Each subscriber owns a public-private key pair (pk_i, sk_i)
2. The home network itself owns a public-private key pair (pk_{HN}, sk_{HN})
3. The home network stores the IMSI and the corresponding public key $(IMSI, pk_i)$ for each subscriber in the HLR
4. The UE stores (in a tamper-resistant way) the public key of the home network pk_{HN} in the USIM

Every time a subscriber asks to register to the network and the TMSI is not available (or it is not recognized by the network), the following protocol takes place:

1. The UE sends its IMSI encrypted using a secure (thus randomized) asymmetric scheme, using the public key of the home network: $Enc(pk_{HN}, IMSI)$
2. The home network decrypts, it finds the IMSI and responds with a challenge $rand$, where $rand$ is a 256-bit randomly-chosen value
3. The UE uses its private key to sign this value concatenated to the IMSI and responds with $Sign(sk_i, IMSI||rand)$, where $Sign$ is a strong signature scheme and $||$ is the concatenation
4. The home network verifies the signature and if the verification holds it continues with the normal AKA procedure

(b) As given, the scheme fails when the UE is in roaming. Explain why and propose a fix. **(2x2p)**

(c) Moreover, the scheme still exposes the IMSI. Explain why. **(5p)**

(d) Briefly compare the method proposed by *PrivTel Ro* to protect the IMSI with the SUPI concealment as it is performed in 5G (1-2 paragraphs). Why is the approach adopted in 5G a better choice? **(5p)**

TOTAL available: 60p