Answering COM-301 questions

In this document we provide guidelines to structure your answers in such a way that the security arguments are well supported. The goal of this document is not to provide technical insights on the content of the course, but to help you compose your answers in a structured manner.

Before jumping into explanations, here is some general advice when confronting an exam. They may seem trivial but checking the Most Repeated Error documents of the last years you can see how these are recurrent errors.

- **Answer the question**. Read the question and answer what is asked. First, make sure you answer all the parts of the question. Then, do not add extras that are not asked for. For instance, do not provide a mitigation to an attack if you are only asked about the attack, or do not provide two attacks if you are asked for one. When you answer extra non-asked elements, they will not count positively and, if the proposal is wrong, it will result in negative points. We need to grade everything that has been written in your answer, we cannot just select the parts that are correct (think of this as marking several answers in a multiple-choice question).

- **State your assumptions**. If you are uncertain about details, spell out your assumptions clearly in your answer. For example, if you are not sure what are the assumptions about the threat model in the question, state in your answer what kind of adversary (what are their capabilities and goals) you interpreted.

- **Be careful with terminology**. If the question uses some names or specific terminology, stick to the terminology in the question (e.g., use “security concern” and not worry, or problem, if the question asks about security concerns). This facilitates the grading as it leaves no room for misinterpretation. Do not worry about repeating a term multiple times; there is no need to find synonyms to technical terms.

- **Always justify your answer.** Even if we forget to add the “justify your answer” to the question, please justify your answer. It will ensure that we can assess that you actually know the content of the course.

Question

Part I. *Rita has heard the best coffee in town is served at Ricco's Cafe. She gets there and while she waits for her coffee, she wants to watch the new TikTok hits. It turns out that the WiFi network at Ricco's Caffe has no encryption. Ricco warns Rita that it is not safe to use this connection, but Rita disagrees. Rita connects to the WiFi, and tests that she has Internet connectivity by visiting https://cutestkittens.com. It loads without issues. Rita says to Ricco: "See, no problem! That access was totally safe!"*

If Rita is correct and the access to cutestkittens.com was safe, explain why she is correct. If she is not correct, provide a network attack against Rita.

Part II. *Now that she has tested her WiFi access, Rita decides to have the only muffin sold in the cafe. She does not remember whether she has enough money, so she tells Ricco: "Let me check if I have enough money in my bank account." and starts typing https://QuiteSecBan... on her phone's browser. The next client in line, Randy, also wants the muffin, so he decides to stop Rita from buying it and wants to prevent her from checking her bank account.*

Describe a network attack that Randy can do to prevent Rita from checking whether she has enough money in her account. For each attack, describe clearly (in one or two sentences) how Randy performs this attack and what capabilities he needs to have to perform the attack.

These are sample answers. There are many more answers (other attacks, other justifications) that would be awarded whole grade

Answer Part I

Part I. Assuming safe access means that she is connected to the actual cutestkitten.com website and no adversary has tampered with the content on transit, Rita is correct. There is no adversary that could have interfered with this connection due to the use of HTTPS, which indicates that the HTTP connection was done via TLS.
Thanks to the TLS handshake, the client can check the authenticity of the server by checking the server's public key. After the handshake client and server share a secret key that they use to ensure confidentiality and integrity of the communication. When Rita reads the page, she knows it comes from the actual server and it has not been altered.

Analysis of the answer
Structure your answer well. If there are two questions, indicate what the answer to each question is.
State your assumptions about the question. The question says "safe" access. If you think this is ambiguous, map this to an adversarial model and goal so that the rest of your security argument has a context.
Answer the question. Make sure there are clear answers to the direct questions.

Justify the answer, in this case explain why Rita is correct under the adversary model you have set up using your knowledge about the concepts of the course

Answer Part II

Part II. Randy can run a Denial of Service attack on the router, for instance, *sending a lot of connections to the router*. To run this attack **Randy needs access to the router Rita is connecting to**. As Randy is in the same café, he is in the same network and can run this attack.

Analysis of the answer

Structure your answer well. If there are two questions, indicate what the answer to each question is.

Answer the question. Make sure there are clear answers to the direct questions. The question has three: what attack, *how it is performed* and **what capabilities the adversary needs**.

Justify the answer, in this case explain why Randy is in a position to run the attack and why he has the capabilities needed.

Note that the answer does not propose countermeasures, and only provides one attack, as this is what the question asks for.

Alternative answer Part II

Part II. Randy can run a DNS hijacking attack on Rita's connection. Randy *needs to capture the DNS reply to Rita's DNS request to find the IP of https://QuiteSecBank.com and substitute the IP by another that will not let Rita access the bank*. **Randy needs access to the traffic between Rita and the DNS resolver (anywhere in the path).** As Randy is in the same café, he is in the same network, can capture packets and run this attack.

Analysis of the answer

Structure your answer well. If there are two questions, indicate what the answer to each question is.

Answer the question. Make sure there are clear answers to the direct questions. The question has three: what attack, *how it is performed* and **what capabilities the adversary needs**.

Justify the answer, in this case explain why Randy is in a position to run the attack and why he has the capabilities needed.

Note that the answer does not propose countermeasures, and only provides one attack, as this is what the question asks for.

Answer without full points

Part 1 : Rita is not correct, just because she can access cutestkittens.com doesn't mean that her connection is secure. A Man-in-the-middle (MITM) can intercept her packets and change them how he wants / follow them where he wants. To do that, he can hijack the TCP connection.

Correction: (0/2) The question specifies that the connection is through HTTPS, which means that the browser is using TLS. In TLS, the server is authenticated so there cannot be a MITM attack.
Even if it was correct, “Hijack the TCP connection” is not enough to define the attack. How is the attack performed? Why is it possible?

Part 2 : Randy can perform a DNS hijacking, that means he will be a MITM and corrupt the DNS responses with fake pairs (IP, domain) before following the packets to Rita. This way, he can redirect Rita to another website and Rita cannot access her bank account. If Rita's phone server already know the IP of the bank server, Randy can perfom an IP spoofing, being a MITM and redirect Rita on a web page "not disponible yet"

Correction: (1/2) Hijacking is correct, and the explanation is explicit enough to know that the student understands the concept.
0.5 points were subtracted for not answering the part of the question about Randy’s capabilities. What enables Randy to launch a DNS hijacking attack?
0.5 points were subtracted for proposing a second attack (IP Spoofing) without indicating capabilities and without providing details of the attack (what IP is spoofed? How does the redirection happen? What are the capabilities needed to perform this attack?). As this answer would have not received points if it was incorrect, it subtracts from the correct answer.

Question

The TAs for COM-301 are frequently meeting in their coffee lounge to discuss the upcoming quizzes for the class and their solutions. To prevent curious students from listening to their conversations, the TAs have set up a simple authentication scheme to control who can enter the lounge.
The TAs have a Signal group and every morning send around the name of a new song to the group. To get entry to the lounge, you have to sing the first few lines of the current day's song. The people in the room will listen and if it is the correct melody you will be let in.

Part I. Is this a secure way to prevent students from entering the lounge? If you think the scheme is secure, justify what properties make it a secure authentication scheme. If you think the scheme could be broken, describe how and make a suggestion about how the TAs could prevent this attack from happening.

Part II. The TAs also discussed adding a second step to the authentication process where you would not only have to sing the correct song but also name the title of the song before entry. Would adding this second step change anything about your answer to the first part of the question? Justify.

These are sample answers. There are many more answers (other countermeasures, other justifications) that would be awarded whole grade

Answer Part I

Part I. No, the proposal is not a secure way to prevent students from entering the room. A student that wishes to learn the password of the day, just needs to hear the password from one TA. The student could just be around the corridor and wait for a TA to enter the lounge using the song. Then, the student can repeat the song and the TAs would let them in.

To fix the problem, the TAs could discard the song every time a TA comes in the room and use a different one the next time, e.g., by instead of agreeing on one song, agreeing on a list of songs. This way, a student listening will not have enough information to enter the room.

Analysis of the answer
Structure your answer well. If there are two questions, indicate what the answer to each question is.
Answer the question. Make sure there are clear answers to the direct questions.
Justify the answer, in this case explain why the scheme is not secure using your knowledge about the concepts of the course

Answer Part II

Part II. No, the addition does not increase the security of the mechanism. A student that can hear the TA singing, can also hear the name and title of the song and repeat it afterwards..

Analysis of the answer
Structure your answer well. If there are two questions, indicate what the answer to each question is.
Answer the question. Make sure there are clear answers to the direct questions.
Justify the answer, in this case explain why the additional step does not make the scheme more secure using your knowledge about the concepts of the course

Answer without full points

Part 1: This authentication scheme is not secure at all. By a simple eavesdropping technique, the attacker can know the song and so reproduce it to get access.

The attacker could know it by hacking or getting access to the WhatsApp conversation (which can be hard) or with a much more simpler way, by hearing it in the hall or next to the lounge itself.

A good next step to the authentication process would be to add a Challenge , a random number (from a large space, to ensure that there are no repetitions and cannot be predicted) .

Correction: (1/3) The answer correctly says that the scheme is not secure and explains why and how it could be broken.
However, the amendment is not well explained. The student mostly paraphrases the course slides regarding how Challenges work, without applying the concepts to this particular use case. How would a random number be used? If it is from a large space how would the TAs remember it? Or be able to parse it correctly? This answer does not demonstrate understanding of how challenge-response protocols work, just that the student read the course material.

Part 2 : The next step suggested by the TA-s does not make the scheme more secure as it can be derived and known after eavesdropping the song lyrics and hence it would add a bit more work to the attacker but really not that much and won't let the system more secure, hence it is completely useless. A fix would be to have a song per TA, and each morning they decide who's going to sing what (every TA a different music).

Correction: (1/2) The first part of the answer is correct, the modification does not improve security. However, the fix is incorrect. Having one song per TA does not solve the problem, as TAs may return in a day (the question specifies that the TAs meet there frequently) and thus a student could still eavesdrop. This wrong statement subtracts 1 point from the answer. (Note that this part of the question DID NOT ask for a countermeasure, just if the

modification would change the response to part 1. By adding something that was not asked, the student lost points).