Exercise Questions
CS447-003 Networks and Data Communications
April 18, 2024

QUESTION

As we discussed in the classroom, the concept of “non-repudiation” consists of “sender non-repudiation” and “receiver non-repudiation”. The sender non-repudiation means, if a sender did sent a message to a receiver, and if the message was successfully received by the receiver, the sender can not deny that he sent that message to the receiver.

Given scenario: Suppose you are developing a network application. Your network application consists of two processes of the server-side and the client-side processes. The network application requires the server and the client processes communicate through the unreliable public Internet.

If your network application must guarantee the sender non-repudiation (senders can not repudiate their messages sent to receivers), how do you achieve it in your network application?

Question: Design and describe what we should do to guarantee “sender non-repudiation”.

Hint 1: Your solution should be a combination of multiple different security enhancing techniques and methods.

Hint 2: Anything that is not mentioned above is currently not implemented yet (your security design should take care of any possible security issues not explicitly mentioned above).

Requirements to your solution:

(1) Your description should be complete, meaning that any possible security issues (but only those related to “sender non-repudiation”) should be considered and you are expected to describe every single detail. For example, you may say, “do … (something) …”, but if there is anything can ruin the purpose of “doing (something)”, you need to design a solution to take care of such issues.

(2) At the beginning of the network application, all what the receiver know (and has) is the IP address (not the host name) of the sender. You can assume that the sender’s IP address the receiver has is always correct.

(3) If you need to have your own assumptions, please clarify (and clearly) state each of your assumption. Your assumptions must be reasonable and realistic. Any unreasonable or unrealistic assumption (e.g., assuming that the server and the receiver host computers are directly connected by single wire – logically it can happen in the Internet, but I really do not think it is realistic …) is subject to penalty.

(4) Please clearly identify each different technique you used in your solution.

(5) Ignore any problem other than “sender non-repudiation”.

Grading policy: Any solution that will not be positively contribute to preventing “sender non-repudiation” will be subject to some penalty even though it does not do any harm to your network application. Do not mention anything that is not related to the security issue of “sender non-repudiation”.