

SENG2250/6250 System and Network Security

Self-Quiz Week 7, Semester 2, 2020

True/False Questions.

1. Remote procedure call (RPC) aims to make the procedure call on a remote machine to look like a local call.
True.
2. Asynchronous RPC (ARPC) is always better than synchronous RPC because the ARPC clients can perform other tasks during procedure execution.
False. It depends on the particular applications. They both have advantages and disadvantages that we may decide case by case.
3. Kerberos is an example of an Authentication and Authorisation Infrastructure (AAI).
True.
4. Kerberos version 4 is secure against eavesdropping because it encrypts sensitive information, such as session key, ID, etc.
False. As Kerberos V4 only uses DES, it is insecure under the current computing systems. An adversary can highly likely break the ciphertext. In Kerberos version 5, it allows any encryption method.
5. For inter-realm Kerberos authentication, a client (of Realm A) has to register in the destination realm (Realm B) before he can play authentication protocols with the server reside in Realm B.
False. The client does not need to register in Realm B. The Kerberos systems in Realm A and B share some secret that they can help the client and server. Please refer to the short video of L7S36 for details.

Short-Answer Questions

6. Kerberos version 4 does not provide the authentication forwarding service. What does it mean by authentication forwarding? Give an example.
Authentication forwarding allows a credential (e.g., secret token/ticket) issued to one client to be forwarded to another host (i.e. server). For example, a client issues a request to a print server that then accesses the client's file from a file server, using the client's credentials.