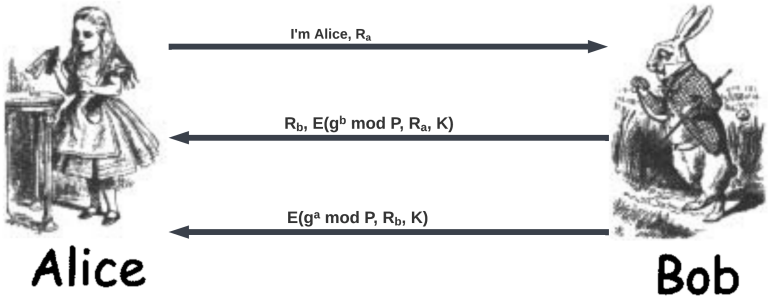
Homework 4

Antonio Zea Jr

November 9, 2022

1 Design a secure mutual authentication protocol based on a shared symmetric key. We also want to establish a session key, and we want perfect forward secrecy. Solve for a protocol that can establish this in 2 to 3 messages

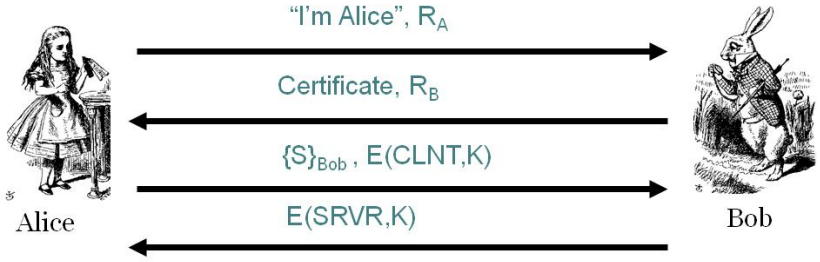


2 Consider the following mutual authentication protocol, where K_{ab} is a shared symmetric key.

Give an attack Trudy can use to convince Bob that she is Alice.

Trudy could use a replay attack by sending "I'm Alice", $R+1$ to Bob he would receive $E(R+1, K_{AB})$. He could then send "I'm Alice", R to Bob after which he would respond to Bob with $E(R+1, K_{ab})$.

3 Consider the following protocol, where CLNT and SRVR are constants and session key $K = h(S, R_A, R_B)$



1. Does Alice authenticate Bob? Justify your answer
   Yes, Alice authenticated Bob because she sent $\{S\}_{\text{Bob}}$, which could only be decrypeted by Bob. Bob decrypts this to get S. Bob then uses the hash of S, R_A, R_B to arrive at the session key. He then responds with the encryption of SRVR which only he could do given the need for S.

2. Does Bob authenticate Alice? Justify your answer
   No, Bob does not authenticate Alice because neither of her responses contain anything that only Alice could compute. Trudy could provide their own S, encrypt it for Bob, they could produce their session key since $R_A$and R_B were transmitted in the clear.

4 Kerberos

1. Why can Alice not remain anonymous when requesting a TGT from the KDC?

   (a) A Ticket Granting Ticket acts a users credentials. The KDC needs to know exactly who is making the request for the TGT to correctly provided it. The will TGT contain a session key and Alice's user ID amongst its contents. This is how the KDC maintains the state of Alice's authentication since the KDC is stateless in that the KDC does not maintain which users are logged in to the KDC.

2. Why can Alice remain anonymous in the sense of not needing to use her private key when requesting a ticket to Bob (what does she use instead and why is this sufficient)?

   (a) The TGT and the authenticator are enough to request a ticket to Bob. The TGT contains Alice's session key and user ID while the authenticator contains a timestamp and Alice's session key. Most of the information the KDC needs is in the TGT while the authenticator helps verify that the communication is fresh.

3. Why can Alice remain anonymous (not needing her private key) when she sends the "ticket to Bob" to Bob?

   (a) The ticket to Bob contains Alice's user ID and the shared key they will use in their communication. That is enough to for Bob to establish who Alice is and how to comminicate with Alice securely.

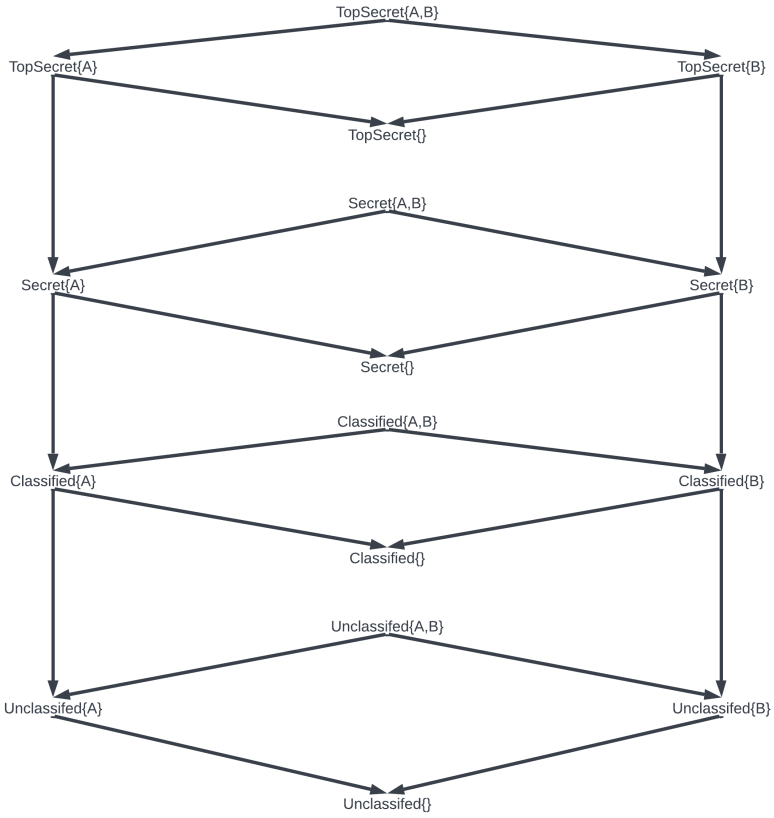
5 Describe what the confused deputy problem is and what types of authorization approach would be susceptible to it.

The confused deputy problem is a security issue where an entity that doesn't have permission to perform an action can coerce a more priveleged entity to perform the action. Access Control Lists, in particular, are susceptible to this approach.

6 Authorization - MLS compartments

Draw the full tree and indicate which files Alice and Bob each can read (don't forget Unclassified)

- Alice has the following clearances TopSecret, Secret{A}, Classified{B}
- Bob has the following clearances TopSecret{A}, Secret{B}



Alice can read TopSecret{}, Secret{A}, Secret{}, Classified{A}, Classified{B}, Classified{A,B}, Classified{}, Unclassified{A}, Unclassified{B}, Unclassified{A,B}, Unclassified{}

Bob can read TopSecret{A}, TopSecret{}, Secret{A}, Secret{B}, Secret{A,B}, Secret{}, Classified{A}, Classified{B}, Classified{A,B}, Classified{}, Unclassified{A}, Unclassified{B}, Unclassified{A,B}, Unclassified{}