Ryan Young

CSE 3400

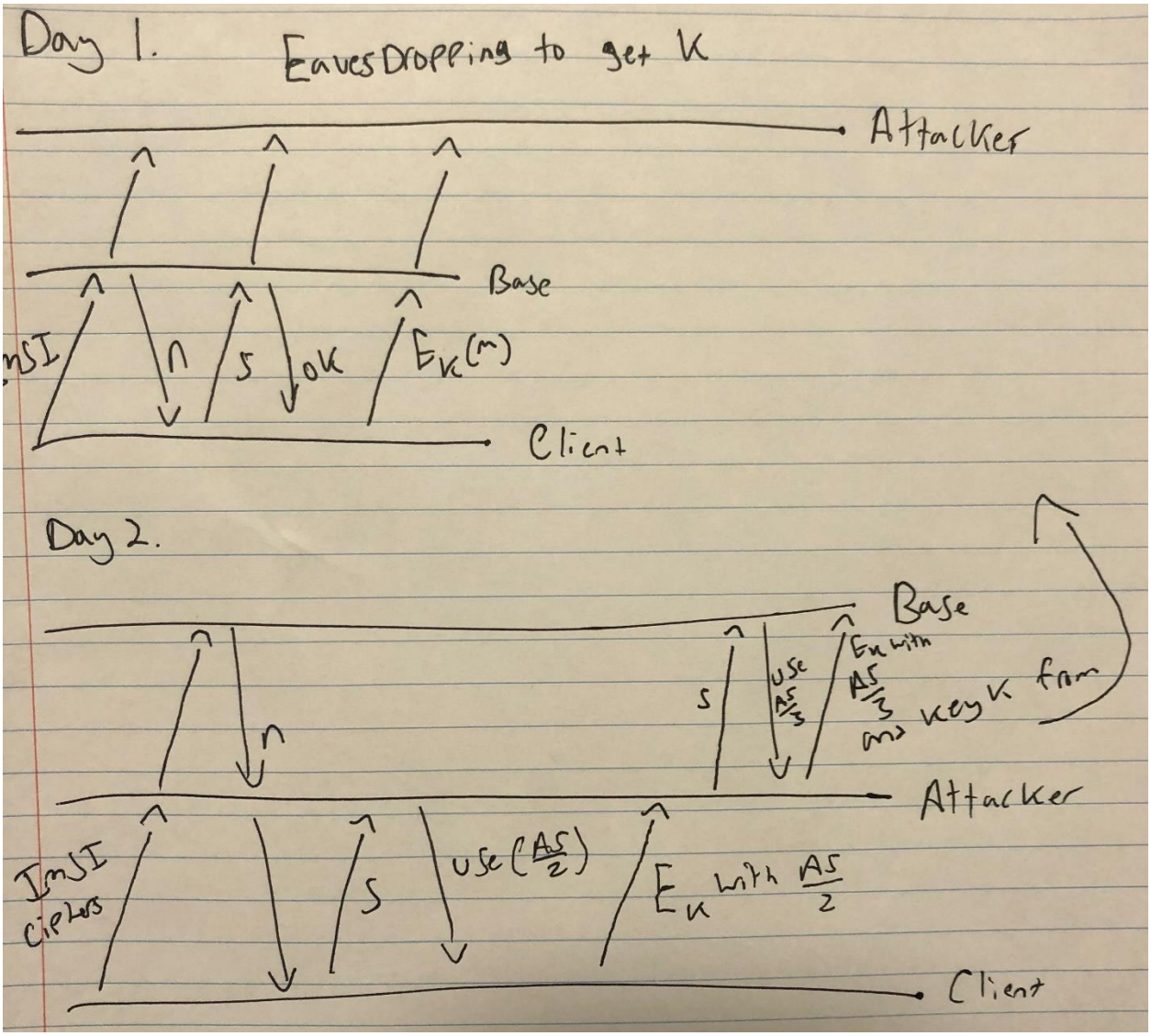
3/13/2020

Homework 5

1.) *Let (Enc, Dec) be an IND-CPA secure encryption scheme and let $Enc'_k(m) = Enc_k(Compress(m))$, where Compress is a compression function. Show that Enc' is not IND-CPA secure.*
The IND-CPA game is where the attacker wins if he or she can distinguish between two cipher texts based off input plaintexts. Since we know that compression of a randomly generated strings do not compress well and non-random strings compress generally fine, the attacker can input m_1 such that it is a randomly generated string and m_2 where it is a normal English language string such as "Hello". This will then allow the attacker to see the differences in length between the two messages because encryption in general does not hide length and thus the attacker wins the IND-CPA game.

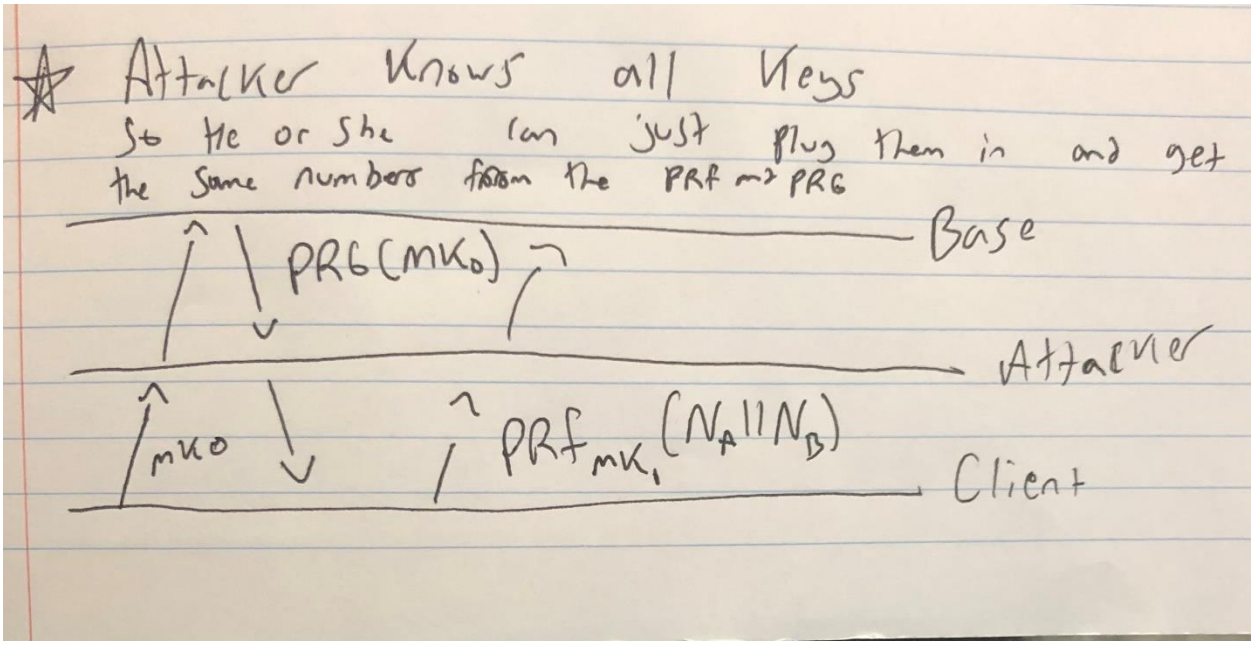
2.) *Present an alternative design for a KDC protocol, which avoids the assumption of synchronized clocks. Your solution should maintain client-server communication, i.e., the KDC (as a server) should only send responses to incoming requests and never initiate communication with a client. Hint: you can take ideas from 2pp, add an additional state for counters and defining the contents of the flows in Fig. 5.9.*
In two way protocols we know that you can either send time or you can have each user have a nonce and since we are not allowed to use time anymore it is only logical we use a nonce. We are also assuming that the KDC knows Alice and Bobs nonces. In taking a queue from the 2pp protocol, Alice can send her name, and her nonce to Bob. This initial nonce transmission cannot be done using the KDC because the KDC is not allowed to initiate communication with the client. Once this nonce exchange between the two parties occurs Alice will send 'Bob', her nonce and $MAC_{k(m/a)}$(nonce || 'Bob') and the KDC will send her back $c_B=E_{k(E/B}(K_{AB})$, T = (c_B, $MAC_{k(m/B)}$(nonce||"Alice'||c_B)) and $c_A= E_{k(E/A)}(K_{AB})$, $MAC_{k(m/a)}$(nonce || 'Bob' || c_A || T) as long as her nonce is correct. She will then send this to Bob same as in the original diagram except replacing time with her nonce. Bob will then do the same but replace time with his nonce. To improve further there could be some sort of encryption when sending the nonces in the initiation of the handshake.

3.) *(GSM combined replay and degrade attack). Present a sequence diagram like Figure 5.11, showing a "combined replay and downgrade attack', allowing an attacker which eavesdrop on the entire communication between mobile and base on day D, encrypted using a 'strong' cipher, say A5/3, to decrypt all of that ciphertext communication, by later impersonating as a base and performing a downgrade attack.*



4.) *(Forward Secrecy vs. Perfect Forward Secrecy(PFS)). Present a sequence diagram, showing that the forward-secrecy key-setup handshake protocol presented in subsection 5.6., does not ensure Perfect Forward Secrecy(PFS).*

This handshake protocol call does not provide Perfect Forward Secrecy because a session I does not remain secure after it ends if all keys are exposed the attacker can simply input the key into the PRF to get the key for the PRG and then use the previous output of the PRG and the whole communication line is now exposed:



5.) *Consider the following mutual-authentication protocol, using shared key k and a (secure) block cipher (E, D):*

1.) *Alice sends N_A to Bob.*
2.) *Bob replies with N_B, $E_k(N_A)$.*
3.) *Alice completes the handshake by sending $E_k(N_B$ xor $E_k(N_A))$*

Show an attack against this protocol and identify design principles violated by the protocol (allowing such attacks).

A main in the middle attack will work on this one because the attacker can open two connections with Bob. The first connection the attacker will pretend to be Alice and send her information. In this first connection the attacker will receive Bob's nonce and in the second connection the attacker will begin by sending the nonce Bob just sent. Bob will then send back the encryption of this nonce and the attacker will then rely in the first connection with this newly acquired encryption of Bob's nonce. This breaking the protocol and this means that the handshake violates, key usage limitation and the security goals and attack model because the handshake does not account for all methods of attacking it.