CS 458 A2
Patrick Wong
pn2wong 20317267

[Q1 – Identification/Authentication Protocols]

[a](i) Mallory can still intercept all messages and read all messages between Alice and Bob, routing all messages between each other.
[a][ii] Mallory can still intercept all messages and read all messages between Alice and Bob, routing all messages between each other.
[b] The authentication factors the bank uses is Alice's credit card pin when she is trying to use her credit card on the ATM. They are also using her phone number and credit card number to verify her identity – since her account was locked, she called the bank to unlock her account. The bank is able to see who is calling them by matching the credit card with the phone number. Alice identifies the bank by their phone number, which she has in her records or is shown on the ATM machine. The bank identifies Alice by her credit card number, which is uniquely mapped to her.

[Q2 – Lattices]

[a] Alice can read D101, D102, D104, D105. She can write to D102, D103, D104.
[b][i] I(D101) = glb(I(Alice), I(D101)) = classified. The integrity level of Alice and D101 stay the same.
[b][ii] I(Alice) = glb(I(Alice), I(D102)) = secret. The integrity level of Alice and D102 stay the same.
[b][iii] I(Alice) = glb(I(Alice), I(D103)) = secret. The integrity level of Alice and D103 stay the same.
[b][iv] I(D104) = glb(I(Alice), I(D104)) = secret. The integrity level of Alice and D104 stay the same.
[b][v] I(Alice) = glb(I(Alice), I(D105)) = classified. The integrity level of Alice is reduced to classified. The integrity level of D105 stays the same.

Read: I(subject) changes
Write: I(object) changes