a2 documentation
Boris Kravchenko
bkravche
20332359

Written Questions

1.

a. Alice can read D102, D104, D105.
Alice can write to D101, D104

b.

i. Alice: Secret, {SecondCup, TimHortons}
D105: Unclassified, {SecondCup}

ii. Alice: Secret, {SecondCup, TimHortons}
D104: Secret, {SecondCup, TimHortons}

iii. Alice: Secret, {SecondCup, TimHortons}
D103: Classified, {Starbucks, SecondCup, TimHortons}

iv. Alice: Secret, {SecondCup, TimHortons}
D102: Secret, {TimHortons}

v. Alice: Secret, {SecondCup, TimHortons}
D101: Secret, {SecondCup, TimHortons}

2. P(accept | Alice) = 97/100
P(reject | Alice) = 3/100 *false negative*
P(accept | imposter) = 5/100 *false positive*
P(reject | imposter) = 95/100
P(imposter) = 2/100

a. P(accept) = [P(accept | Alice) * P(Alice)] + [P(accept | imposter) * P(imposter)]
= 0.9516
P(reject) = 0.0484

P(imposter | reject) = [P(reject | imposter) * P(imposter)] / P(reject)
= .0.3926
= **39.26%**

b. P(Alice | accept) = [P(accept | Alice) * P(alice)] / P(accept)
= 0.9989
= **99.89%**

3.

a. An adversary can split the spoofed packet into tiny fragmented IP packets. The header will also be split up, meaning that a packet filtering gateways will not detect the source address. Stateful inspection firewall will defend against such an attack because it re-assembles fragmented packets.

b. Blocking internal spoofed traffic prevents impersonation attacks, as well as users doing denial-of service attacks of other networks. Blocking external traffic prevents denial of service attacks on UW network, or network mapping. ARP spoofing is still possible.

BONUS

1. Word of mouth is one method. Anyone can run a bridge relay. So for example, a person running a bridge relay in Canada can call their relative in China and simply give them the IP address of the bridge over the phone.
2. Disallow all HTTPS traffic with all unknown hosts. Only allow HTTPS traffic with trusted e-commerce websites and such (use a white list). Essentially outlaw web encryption unless used for an allowed purpose. If user uses HTTP to connect to a bridge, the payload can be filtered normally.