CS 458 A2
Yu Gan
20563500

1.

a) Alice uses three authentication factors, which are something she know, something about her context, and something she is. PIN, password, and unlock pattern are things that Alice know. Wearable device is something about Alice's context. Fingerprint is Alice's biometric, so this belongs to something Alice is.

b) If someone shoulder surfs Alice when she is entering her PIN, the person can easily know the PIN.
After Alice enters the unlock pattern, the trail of pattern is left on the screen of her smartphone. Thus, somebody would know the unlock pattern if he sees the screen.
If Alice puts her smartphone and the wearable device in her bag and someone steal her bag, the person can unlock Alice's smartphone because he has the wearable device.

c) $P_{other|reject} = \frac{P_{reject|other} * P_{other}}{P_{reject}} = \frac{(1-5\%)*10\%}{(1-5\%)*10\%+8\%*(1-10\%)} = 56\%$

Thus, the probability that the lock is a result of someone other than Alice using the phone is 56%.
We can reduce the false rejection rate by combining other authentication factors with finger swipe. Instead of locking the smartphone after only one unidentified finger swipe, the smartphone can use PIN or wearable device to give the user a second try after the failed finger swipe.

2.

a) Alice has neither read nor write access to document D001.
Alice has write access to document D002.
Alice has both read and write access to document D003.
Alice has neither read nor write access to document D004.
Alice has read access to document D005.

b) Document D101's integrity classification changes to (Secret, {Alpha, Delta}).
Alice's integrity classification changes to (Confidential, {Alpha}).
Document D103's integrity classification changes to (Confidential, {Delta}).
Document D104's integrity classification changes to (Confidential, {Beta, Delta}).
Carol's integrity classification changes to (Confidential, {empty}).

3.

a) It can defense against IP address spoofing attack. It can drop all packets originating from uWaterloo whose source address is not of the form of uWaterloo IP address and traffic originating from outside of uWaterloo whose source address is of the form of uWaterloo IP address.

b) We need to deploy stateful inspection firewall and application proxy. Stateful inspection firewall can prevent all the devices in the lab from browsing malicious

websites and record all remote login operations from the external networks to the work computers. Application proxy can prevent hosts in the external networks initiating a connection to the experiment computers and the server directly.

c) The firewall cannot control access from the work computer to the experiment computers and the server. It can only control external network user's access to lab and lab user's access to external networks.

DIRECTION	PROTOCOL	SOURCE	PORT	DESTINATION	PORT
OUT	TCP	172.16.1.1	ANY	172.16.100.0/24	254
IN	TCP	172.16.100.0/24	254	172.16.1.1	ANY