CS458

Bo Liu
b69liu
20521697

October 2017

1 Written Part

1. (a) Knows: PIN, password, unlock pattern
Has; Wearable device
Is: fingerprint, finger swipe(finger movement habit)

   (b) PIN: can be guessed(DoS attack if limit times) or shoulder snooping.
Pattern: finger's track can be left on the screen if not always wear gloves.
Wearable: it might be stolen at the same time with the cell-phone, or the thief put steals the cellphone and put it near your to unlock.

   (c) $A : UserisAlice$
$\bar{A} : User\ is\ not\ Alice$
$U : still\ Unlock$
$\bar{U} : lock\ after\ a\ swipe$
$P(U|\bar{A}) = 5\%$
$P(\bar{U}|\bar{A}) = 95\%$
$P(\bar{U}|A) = 8\%$
$P(U|A) = 92\%$
$P(\bar{A}) = 10\%$
$P(A) = 90\%$
$P(\bar{A}|\bar{U}) = \frac{P(\bar{U}|\bar{A})P(\bar{A})}{P(\bar{U}|A)P(A)+P(\bar{U}|\bar{A})P(\bar{A})} = \frac{0.95*0.10}{0.08*0.90+0.95*0.10} = 0.5689$
It can be less strict, it is not big problem to allow thief operate few times with unsecured content before it lock.
It can dynamically adjust the accuracy of locking. For example, if there are frequent accepted swipes, which means the user is most likely Alice. So it can lower its strictness during a certain time period to decrease false rejection rate.
Also, it can learn Alice's pattern along with her using. If it accept immediately after a reject, the rejection probably is false rejection. So the AI can be trained.

2. (a) D001:
D002:write
D003:read, write
D004:
D005:read

   (b) i. D101 = (Secret,Alpha, Delta)

   ii. Alice = (Confidential,Alpha, Delta)

   iii. D103 = (Confidential,Delta)

   iv. Eve writes to D104 (Confidential,Beta, Delta)

   v. Carol: (Confidential,)

3. (a) it can prevent packet from inside but the source IP is not inside, and packet from outside with inside source IP in header.

   (b) i. It needs a state firewall to identify what connect is initial from internal and what from external. So, it can prevent the connection to server that initiate from external network.

   ii. I think, packet filtering gateway is enough. It can check all packets' url, can compare it to blacklist.

   iii. Stateful inspection firewall is needed, since it needs to check the payload of each packet and record.

   (c) I don't think so, as the travel does not go through the firewall at all.

DIRECTION	PROTOCOL	SOURCE	PORT	DESTINATION	PORT
IN	SSH	172.16.101.0/24	ANY	172.16.100.25	ANY