COMP3632 Assignment 2

Wang, Tiantian

1. (a)Mistake: Bob uses the encrypted secret key for AES.
Bob should use his private key to decrypted the message sent by Alice to know the real key.

(b) Mistake: Bod asks a CA to sign his private RSA key. Alice doesn't know who the CA is.
Bob should ask a CA to sign his public RSA key. He should not reveal the private key to anyone. Alice can also know who's the CA by clicking into the lock button in her website.

(c) Mistake: Alice uses hashed password to login.
Alice should use the original password to login. The system will hash what she enters and compare with the one stored in the database.

(d) Mistake: Bob stores Alice's encrypted password.
Bob should not store encrypted password, which is dangerous. He should store the hashed password and salt.

2. IP spoofing -> ingress/egress filtering: IP spoofing uses fake addresses which may be detected by ingress/egress filtering, blocking meaningless addresses

Eavesdropping -> proxies: proxies can provide anonymity for users to avoid eavesdropping

Teardrop attack -> deep packet inspection: teardrop attack uses contradicting fragmented packets which can be detected by inspecting in detail the data sent over the network

3. (a) Guard advertised bandwidth: 166.071429408
Exit advertised bandwidth: 50.569675424
Guard advertised bandwidth is more than exit. One reason could be that the number of guard relays are much larger than that of exit relays.

(b) 50 KiB: 7447.27
5 MiB: 1353001.29
The circuit build up time and latency are almost the same for different size of files. 50 KiB files spend a greater portion of download time on that.

(c) Disadvantage: latency because of the encryption and decryption among many relays
Advantage: protect confidentiality

(d) Top 10 countries of bridge users on 2017-06-01

Country	Mean daily users
United Arab Emirates	15074 (20.68 %)
Ukraine	12060 (16.54 %)
Russia	7691 (10.55 %)
United States	6409 (8.79 %)
Turkey	3425 (4.70 %)
India	2486 (3.41 %)
United Kingdom	2048 (2.81 %)
Germany	1953 (2.68 %)
Iran	1741 (2.39 %)
Belarus	1665 (2.28 %)

Ukraine is the country with the greatest ratio of bridge users compared to relay users on 2017-06-01.