COMP3632 Assignment 2

MENG Zihan

20412027

zmengaa@connect.ust.hk

1.

a) Key length in RSA algorithm is likely to be 1024 or 2048 bit long, so Bob's public key should have length 1024 or 2048.

b) Bob should ask the CA to sign his public verification key instead of private signing key.

c) Alice just need to send her password using 128-bit AES, and at Bob's server side, Bob will hash and salt her password and store it in his database.

d) Bob shall not encrypt passwords. Instead, he shall hash the password with salt and store the hashed passwords in his database. Every time Alice wants to login using her password, Bob only needs to check the integrity of hashed password.

2.

a) IP spoofing – defense: Ingress/egress filtering.
Explanation: IP spoofing is an attack that fakes the sender's identity or impersonate another computer system. By performing ingress filtering, the firewall can block IPs that don't make sense based on the network structure. This can prevent an outside attacker spoofing the address of an internal machine. In the meantime, performing egress filtering can prevent an attacker within the network using IP spoofing to attack external machines.

b) Eavesdropping – defense: Proxies.
Explanation: If there exists a chain of proxies, then only the first proxy knows your identity and only the last proxy knows the destination. Encryption is layered such that only the final proxy can read your packets.

c) Teardrop attack – defense: Deep Packet Inspection.
Explanation: Teardrop attack is performed by having two fragmented packets conflicting each other. By performing Deep Packet Inspection, the data being sent over a computer network will be checked in detail. Hence, the conflictions can be detected by performing Deep Packet Inspection.

3.

a) The amount of advertised bandwidth of relays with "Guard" flag is 165.102858936 and the amount of advertised bandwidth of "Exit" relays is 53.385365688 on 2017-01-01.
Total amount of advertised bandwidth of relays with the "Guard" flag is more.
Since the exit relay is the final relay that Tor traffic passes through before it reaches the destination. Number of users is larger than the number of destinations, so the number of "Guard" relays is more than the number of "Exit" relays.

b) For 50 KiB file: 75571.9557 bits per second
For 5 MiB file: 1357373.86805 bits per second
Difference: downloading larger file is faster. Probably because the connection of a transfer is relatively slower and takes the most portion of time used in downloading.

c) Disadvantage: The traffic is relatively slower by using 3 nodes in a Tor circuit.
Advantage: Only the first proxy knows the identity of the user and only the final proxy knows the destination. Encryption is layered such that only the final proxy can read the packets or users.

d)

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 %)

Country: Turkey
Ratio: 0.80474624
Reason: Turkey blocked use of both virtual private networks (VPN) and the Tor

anonymity network to circumvent internet censorship in the country. Hence, people cannot directly connect to Tor relays.

- Programming assignment
  Part (b)
  1) The connection using Tor browser to a website is much slower than browsing websites normally.
  2) Websites ending with ".onion" can be connected to using Tor browser.
  3) Tor usually uses three relays to construct the circuit, so its more secure than normal browsing and the chance of being un-anonymous is much lower.