COMP 3632 – Principles of Cybersecurity

Ali Symeri

20591029

Written assignment

1.

(a)

Bob appears to be using a public key length of 128-bit which is quite small for public key encryption such as RSA. It is not secure to have such a small key length and not normal either, so it would be better for him to use a key length of at least 1024 bit, preferably 2048 bit.

(b)

Bob should not be asking a CA to sign his private key, in fact his private key should not be shared or shown to anyone. What should be the case is that the CA should sign his public key.

(c)

Bob should never require the user to give a salt or hash of any kind, specifically password hash. The user should simply send the username and password, probably encrypted, and it should be Bobs job in the server to hash the users password with a salt and store them.

(d)

The answer to this is in the question for (c). Bob should not encrypt the users password, much less store it. It is computationally intensive to do so and takes more time. What he should do is to hash the password with a salt and store the salt and hash instead. It is harder to brute-force this.

2.

IP spoofing

For IP spoofing the attacker can use a fake address for the source IP and redirect the return traffic to another target IP address or maybe even perform some attacks like DoS. The most fitting defense would then be to use Ingress/egress filtering which would block IP addresses that does not make sense to the network structure or addresses that are not part of the networks IP pool, so that the spoofed IP address will be rejected.

Eavesdropping

For Eavesdropping there is an attacker that is listening to the traffic between two or more users. The attacker is not supposed to be allowed to listen to that communication or be able to intercept it. The best defense for this would be to use proxies. Proxies are used to communicate between the two users. So, user A would send messages to the proxy and the proxy would send it to user B. This channel can be encrypted if that is required. The attacker wouldn’t know who the real receiver is, just the proxy, since he now cannot check for the destination IP address to get user B, he just gets the proxy.

Teardrop attack
For Teardrop attack there is a type of DoS attack in which two packets contradict each other. Two contradicting packets for the receiver can be exploited to make him crash. The defense for this would be to do Deep Packet Inspection on the packets. This would enable the firewall to first read the incoming packets contents to then decide if it should be blocked or allowed in, so that the receiver will not get harmed.

3.

(a)

The total amount of advertised bandwidth of relays with the "Guard" flag was 166 Gbit/s and for the "Exit" flag it was 50 Gbit/s. The "Guard" flag is much larger than the "Exit" flag in terms of Gbit/s, this might be due to the "Exit" node being the one that is publicly facing the targeted server which the traffic is going to. This means that if you are, for example, visiting some torrent website and start to download movies, which might be illegal in the exit nodes country, the exit node is the one to take the blame and he would not want that.

(b)

The median download time of a file for a 50 KiB file from the op-hk onion server was 5.42 seconds and for a 5 MiB file it was 30.92 seconds.
50 KiB = 409 600 bits, 409 600 / 5.42 = 75 572 bits/s.
5 MiB = 41 943 040 bits, 41 943 040 / 30.92 = 1 356 501 bits/s.
The difference may be due to the latency that is applied to the downloads. The latency was around 750 ms for downloads that day and adds up when a larger file is to be downloaded, so it takes longer.

(c)

For the disadvantage of using three nodes in a Tor circuit, my guess would be that, since the three nodes encrypt messages from you to the target, it takes much longer to setup the circuit of three nodes with computing the keys, exchanging them and performing three encryptions, so this adds on delays. However, the advantage then for a circuit of three nodes would be that the channel is much more secure and hides you more efficiently. It would be harder for attackers to know what messages you are sending since the information is spread out on the first and last nodes. The first one knows you and the last one knows the destination.

(d)

The highest ratio is the US, 6409:413426. This is most likely due to the high population there compared to the other countries that use Tor. Also it may be due to regulations in the US that may block certain sites and the case of illegal torrenting there.

Programming assignment

(b)

What I notice when using Tor, in for example Youtube is that it is extremely slow to load the page. When playing a video in full-screen in Youtube, Tor warns you that the website can track you and determine your monitor size and recommends using default screen size. I also noticed that, when I go to www.google.se, which is the Swedish version that I normally use, it shows me the Austrian version with their language, not the Swedish version. I also see that when I connect to any website and I click on the lock icon on the top left (certificate button), it shows me that my browser is connected to USA as guard, then France, Romania and finally the website. Also, if I go to https://whatismyipaddress.com/ it will display the exiting nodes IP address and not my own IP address.