COMP3632 Assignment 2

SU, Heng
20310671
hsuab@connect.ust.hk

November 10, 2017

Problem 1

(a)

Using RSA with 128 bits is too weak. The current recommended key size is at least 2048 bits. Aftewards, Bob can use the public key to encrypt secret keys for AES (128 bits). Then, Bob and Alice can use *AES* in CTR mode to communicate securely.

(b)

It is not necessary for the website admin to ever know or be able to know the passwords of his users. Therefore, encrypting them is a bad idea because it means someone could potentially decrypt it. Instead, he should use a cryptographically secure hash to hash the passwords (with a random salt), and store the username, salt, and hash output. This way, even if a hacker compromises his servers, the best they can do is brute force each password one at a time, which is computationally infeasible.

(c)

Certificates are the CA's signature (not necessarily RSA) of the website's *public* key, not private key. The CA (or anyone else) should never be able to see the website's private key. Furthermore, after the web user verifies the ECC key, they use this key to exchange a symmetric key to protect further communication. Continuing to use public key cryptography would be too slow.

Problem 2

In an IP spoofing attack, an attacker impersonates someone else by swapping their own IP address with that of the victim's. The best defense for this is to use ingress/egress filtering. Ingress filtering allows us to block packets with a source IP which isn't allocated to the source network. Egress filtering can block packets from leaving our network which has a source IP that doesn't make sense based on our network. These two filters help defend against spoofed IPs.

In an Eavesdropping attack, an unauthorized third party is intercepting the communications between two parties. The best defense against this is to use proxies. Without a proxy, the attacker can see the source and destination IP. With a proxy, the attacker can only know that you're talking to the proxy, but not the real recipient, (or that the recipient is communicating with the proxy, but not you). This improves anonymity. If you add in encryption, then the attacker is unable to know the contents of your message as well, improving confidentiality and integrity.

A teardrop attack is a type of DoS attack which relies on sending fragmented packets which contradict each other. When the recipient server tries to reassemble the packets, it crashes due to a problem during the reassembly. The solution is to use deep packet inspection. Deep packet inspection can be used to inspect the contents and format of every packet, and ensure that the packet would not cause any potential problems on the server.

Problem 3

See `ptext0` and `ptext1`

Problem 4

(a)

On 2017-01-01, total amount of advertised bandwidth of relays with the *Guard* flag but not the *Exit* flag was 16,226,837,333 bytes per second. On the same day, the total amount of advertised bandwidth of relays with the *Exit* flag but not the *Guard* flag was was around 1,789,118,085 bytes per second. The advertised bandwidth for *Guard* relays is roughly a magnitude greater than that of the *Exit* relays. One reason for this phenomenon is that hosting an exit node is a potential liability. Traffic generated by Tor users appear to be coming from an exit node. If any of the users are visiting illegal websites, then that illicit traffic appears to be coming from the exit node. Therefore, there is less of an incentive to be an exit node because the owners do not want to be held liable.

(b)

On 2017-06-01, it took 5420 ms to download a 50 KiB file on the *op-hk* onion server, a download rate of 75,570 bits per second (9.446 kB/s). On the same day, it took 30920 ms to download a 5 MiB file, a download rate of 1.357×10^6 bits per second (169.6 kB/s). This is because whenever a client tries to communicate with a server, there is latency involved. This delay imposes a constant overhead on both download attempts. The first download seems to have a slow download rate beacuse of the large proportion of time wasted on overhead. However, in the second download, the overhead is not as significant relative to the time for actual downloading.

(c)

The disadvantage of using three nodes in a Tor circuit instead of one node is that there is greater overhead and latency when establishing and using the circuit, respectively. The user must establish keys with each node at the start, and must encrypt every message three times with three keys before sending them out. The messages must pass through three hops instead of one, increasing latency.

The advantage is that this allows for greater anonymity. Using Tor with a single node is similar to using an ordinary proxy. If a hacker compromised the proxy, then they would know both the contents of Alice's messages and her intended recipient. However, with three Tor nodes, this is not the case. The attacker must be able to control all three nodes in order to deduce her recipient (and contents, if the website isn't also using encryption). The first node knows only your identity, and the last node only knows the message and recipient. Since Tor disallows establishing a circuit with nodes which are close to each other, it is difficult for an attacker to control all three nodes at once.

(d)

On 2017-06-01, for all countries with more than 1,000 daily Tor users, the country with the greatest ratio of bridge users compared to relay users was Turkey (3425:4256 bridge to relay, 0.805). Due to Turkey's geopolitical instability, Erdogan has consistently pushed for internet censorship, including the banning of Tor. Citizens are able to bypass the block of public Tor relays with bridges, since there does not exist a complete public list of them.

(e)

According to *Digitale Gesellschaft*, a German civil rights and consumer protection group specializing on internet policy, the country with the most number of users by percentage of population (as of June 2017) is Moldova, with 963 Tor users per 100,000 internet users. Although there is no state or ISP level internet censorship, Moldovans often use Tor to bypass internet filters at work or at internet cafes. However, if we include outliers, then the answer is Seychelles, with roughly 137,500 relay users for a country with a population size of 94,677. According to discussions within the metrics team, this seemingly impossible spike

during the August of 2017 may have been due to a bug with the counting technique. Another possibility is that cybercriminals may host their servers in such remote locations to carry out unlawful activities.

Padding Oracle Attack

(a)

$$x' = (\texttt{ABABABABAB})_{16}$$

We need to pad x' from 5 bytes long to 16 bytes long to form x. We want to add 11 bytes in order to do so, so we'll add the byte $(\texttt{0B})_{16} = 11$ eleven times.

$$x = (\texttt{ABABABABAB0B0B0B0B0B0B0B0B0B0B0B})_{16}$$

(b)

Given:

$$y_1 = C(IV \oplus x_1)$$
$$y_i = C(y_{i-1} \oplus x_i) \text{ for } i = 2, 3, ...N$$

Therefore:

$$IV \oplus x_1 = D(y_1)$$
$$y_1 \oplus x_2 = D(y_2)$$

$$x_1 = D(y_1) \oplus IV$$
$$x_2 = D(y_2) \oplus y_1$$
$$\text{plaintext} = (x_1|x_2) = (D(y_1) \oplus IV|D(y_2) \oplus y_1)$$

(c)

See `decrypt.java`

(d)

See `encrypt.java`