COMP3632 Assignment 2: Written Portion

Sim, Kyu Doun

20306527

1. Alice and Bob

(a) A MAC is used for authentication and is attached to the messages from Alice to Bob to authenticate the person who sent the message is Alice. However, it must be sent under the assumption that the two parties have already established a secret key. Bob should not be using the same 128-bit secret key to send the HMAC and to establish a SKE at the same time. The HMAC here becomes pointless because Alice is sending Enc(Secret Key) and Hash(Enc(Secret key) XOR Secret Key). Let's say an attacker modifies the Enc(Secret Key). When Bob receives the hashed text, he has no way to verify the HMAC, because when Bob decrypts the received "modified Enc(Secret Key)", even if Bob can decrypt it, he will not be able to retrieve the correct secret key, and cannot perform the XOR with the Enc(Secret key) sent by Alice. What Bob should have done is he should have first established a secret key first, and then authenticate whether if the person is Alice. If Bob would want to still authenticate that the person sending is Alice, they should have predetermined a key to use for MAC.

(b) It is strange that Bob is sending his public encryption key created from RSA to a CA to verify as himself. Bob should be sending the web server's public verification key, not a public encryption key. Furthermore, Bob should have been using a longer RSA. 128-bit RSA is vulnerable against brute force factorization. Bob should have at least used a 2048- or 4096-bit length keys RSA.

(c) Alice should not be the one to hash and salt her password and then send it to Bob, and Bob should not store the received encrypted password directly to the password database. If an attacker can break in the password database, it can also discover the secret key as well. With that secret key, the attacker can look at communications between Alice and Bob. With that secret key, the attacker can look at what Alice sent to Bob before, a hash of her password and salt. This directly reveals the password of Alice and the attacker could easily log in as Alice. For this case, it is nothing difference from storing Alice's password as plain text in the password database. Rather after Bob receives Alice's password in plaintext, it should hash and salt and then store it in the password database.

(d) An encrypted password should never be stored rather than to be hashed and then stored. Since both secret key and password should be stored in the most secure place, if the attacker figures out where the password database is, he could also steal the key alongside the password DB. Then, the attacker has access to the entire password in a plain text form. Again, a password should be hashed and then stored

2. Attack and Defense. The answer is presented as an (Attack, Defense) pair and a follow up explanation.

- (IP Spoofing, **Ingress/Egress Filtering**)

The purpose of an ingress or egress filtering is to detect any IPs that go in or out that seems nonsensical or bizarre. IP spoofing is the creation of IP packets with false source IP. With ingress filtering, it will block packets from outside the network with a source address inside the network. With egress filtering, it will block packets from inside the network with a source address that is not inside.

- (Eavesdropping, **Proxies**)

Eavesdroppers can see the source and the destination IP. However, if the user uses proxies, he or she can hide the source and/or the destination of a packet. The packet from the user will either only reveal the source IP or the destination IP. Therefore, even if the eavesdropper peaks into a packet, the attacker will not be able to know where the packet is going or where it comes from. Anonymity and privacy

- (Teardrop Attack, **Deep Packet Inspection**)

A Teardrop Attack will be performed like sending many tiny fragments to eat up CPU or send fragment that would be completely contained in a previous fragment. By performing Deep Packet Inspection, it can look at the contents of the packets. Deep Packet Inspection can figure out if the packet content of fragmented packets cannot be correctly assembled, and therefore defend against Teardrop Attack. The core function of a deep packet inspection is that it can look at the content of the packets, and it could detect and contradiction inside the packets.

3. Tor

(a)

“Guard” AND NOT “Exit”: 249.635765144

NOT “Guard” AND “Exit”: 19.30846652

The bandwidth of relays with the “Guard” flag is a lot more than the “Exit” bandwidth. Majority of the people do not want to volunteer as exits because they could be legally involved or even responsible in a traffic that has done something illegal. Even if they had nothing to do with the traffic, they have served as an exit, so any trouble will be associated with them. This could further keep them banned by their ISPs or get in trouble that is unrelated to them.

(b)

50kiB takes 5.315 seconds, and 5MiB takes 28.58 seconds.

Respective median download rates are

50 kiB

409600 bits / 5.315 seconds = 77064.910630 bits per second = $7.71 * 10^4$ bits per second

5 MiB

4.194e+7 bits/ 28.580 seconds = 1467459.7620 bits per second = $1.47 * 10^6$ bits per second

The huge difference in download time comes from the fact that the total download time is influenced by the latency of the file. While downloading a small file, most of the time it took is dominated by the latency. For larger files the time required to download is dominated by the actual download rate.

(c)

The disadvantage of using 3 nodes is that latency will be higher than using one node. Furthermore, the user needs to deal with situations such as the exit node becomes a bottleneck.

The advantage of using 3 nodes is that it could protect privacy and anonymity more than using one node. If only one node is used, the single node can see the user’s true source and destination, so the user needs to trust the volunteering single node. If the user is using 3 nodes, an attacker would have to hack all 3 nodes to compromise the user, but if the user is only using a single node, it takes less effort to compromise privacy of the user for the attacker.

4. Superfish

(a) Planted malware and Spyware. It is a planted malware because Lenovo computers came pre-installed with Superfish and this means that the firm has purposely installed these malwares on Lenovo computers. Superfish is a spyware because it intercepts the real certificate and is secretly collecting data about the user's browsing patterns to monetize it.

(b) The Superfish behaves kind of like a MITM, but not exactly. Instead of the user establishing a proper secure communication between the user and the website, the user will be sending requests to the Superfish. The Superfish will then send that request to the proper webserver and will deliver back the response from the webserver to the user. This is possible because Superfish has added itself as a root CA, so it is able to be treated as legitimate by browsers. If the user is talking to the website using the website's encryption key, then Superfish certainly cannot change the contents because Superfish doesn't have the website's decryption key. However, since Superfish can intercept the real certificate of the web site, it could modify the packets sent from the website to what it wants, and present to the user. So instead of the user talking to the website with the website's encryption key, the user is talking to Superfish with a fake encryption key presented by Superfish, and Superfish will be able to decrypt the message and read it, encrypt is using the website's public key encryption, and will get a proper response back from the website, able to decrypt it because it has faked the website with its fake certificate, modify the packet from the website, and then send it pack to the user using the fake public encryption key.

(c) If the Superfish malware used the same signing key for every laptop computer, this means that every computer had the same signing key sitting on every machine. The signing key must exist in the installed computers. If an attacker wants to impersonate as a website, he or she could first extract the signing key from the installed computers. Since every Suprfish-installed machine trust any websites signed off by Super-fish, the attacker can create a fake website or link to impersonate as Facebook or Youtube for example, sign off by using the signing key in the machine, then from the victim's point of view, there is nothing suspicious or the browser will not warn the user that it might be a fake website or a link. Superfish also uses the same certificate for every site, so there are various routes from the attackers to exploit and impersonate as a certain website.

(d) Users could check and investigate the browser's certificate settings that allow them to see details about which certificates are provided and signed by whom. If they could recognize that if a certificate from Google is signed by Superfish rather than a trustworthy CA or by Google, they can be suspicious of the provided certificate or at least question whether if Superfish is a trustworthy signer.