COMP3632 Assignment 2: Written Portion

Sim, Kyu Doun

20306527

1. Alice and Bob

Other scenarios

(a) [4 points] Alice wants to communicate with Bob, her friend, securely. She generates a public/private key pair using RSA (128 bits), sends Bob the public key in person, and then Bob uses the public key to encrypt secret keys for AES (128 bits) in CTR mode and sends them to Alice.

Solution: 128-bit RSA is not secure because a brute force factorization attack can break 128-bit RSA quickly. RSA should be at the bare minimum 1024-bit, or better 2048- or 4096- bit.

(b) [4 points] To store passwords securely, a website administrator uses AES encryption with a secret key and a 64-bit IV to encrypt all users’ passwords. A CRC32 checksum is used to ensure correctness against random bit ﬂip errors.

Solution: Encryption should not be used to store passwords. The secret key could be stolen alongside the password database. It is better to use a hash.

(c) [4 points] A website has a TLS certiﬁcate, which is a CA’s RSA signature of the website’s private ECC key. After the visiting web user veriﬁes the ECC key, all further communication between the client and the server is encrypted and decrypted with this key.

Solution: The CA should sign the website’s public ECC key, not the private key. Otherwise, the web user cannot verify it unless she also acquires a copy of the private ECC key. (3 marks at most for ECC not being eﬃcient to encrypt and decypt.)

(a) Alice 128 bit secret key: secret key should be long lasting, encryption, it shouldn’t use to authenticate, Alice should be the only one who knows the secret key

The HMAC is redundant. The Hash- MAC cannot be used to authenticate this message to prove that it is Alice.

(b) Bob should ask a CA to sign his public 256-bit RSA key using CA’s private signature key, not the 256bit ECC key. The ECC key is a PKE and is only used for encryption. A public verification key should only sign private signature key.

(c) adfdsfasdf

(d) A password should never be encrypted, but rather be hashed and stored.

Encryption should not be used to store passwords. The secret key could be stolen alongside the password database. It is better to use a hash.

2. Attack and Defense: The following would describe as an (Attack, Defense) pair.

* (IP Spoofing, )
* (Eavesdropping, )
* (Teardrop Attack, )

IP spooﬁng - Ingress/egress ﬁltering, which is meant to defeat IP spooﬁng by detecting nonsensical IPs. Eavesdropping - Proxies. Proxies can hide the source and/or destination of a packet, defeating eavesdroppres. Deep Packet Inspection is a technique used by eavesdroppers, not a technique used to defeat eavesdroppers. Teardrop attack - Deep Packet Inspection. Deep Packet Inspection is able to ﬁnd if the packet content of fragmented packets cannot be correctly assembled together, which is how a teardrop attack operates.

3. Tor

(a) 16,226,837,333, 1,789,118,085 Gbit/s respectively. The former is almost 10 times more. Many people do not want to be exits because this may make them legally liable for the traﬃc that they carry out, and they may be banned by their ISPs.

(b) 5420, 30920 median ms to load respectively for 50 KiB and 5 MiB. Median download rate is 51200/5420 = 9446 B/s for the former and 5242880/30920 = 169560 B/s for the latter. The large diﬀerence is because the total download time includes the latency of the ﬁle. The amount of time required to download a small ﬁle is dominated by the latency, whereas the amount of time required to download a large ﬁle is dominated by the actual download rate.

(c) Disadvantage: Latency is higher with three nodes. Advantage: If we use one node, it can see both our true source and destination, so we must trust it (and we should not trust it because it is a volunteer). This compromises our privacy

4. Superfish

1. Planted malware and Spyware or keylogger
2. Superfish can change the content because

Create its own certificate, which is fake,

Computer -> Public Key -> Browser

Create own CA, this is trust worthy, encrypt everything using the CA

Superfish decrypt, gains info and encrypts it again

1. Asdf
2. Users could check

Steal the signing key authenticate what ever they want

