Name: Neil Jones
EID: nj2977
CSID: nfjones
Email: neil.franklin.jones@gmail.com

Week 4 Questions

Lecture 53

1. You don't want somebody else to obtain it and impersonate you.

2. The hash is shorter than the message usually.

3. Only S could have sent the message and S cannot deny having sent it.

Lecture 54

1. They provide a way of knowing that a message really came from who it says it came from.

2. So that anybody can decrypt the certificate with X's public key and see that it belongs to Y.

3. It provides a means of checking for validity by decrypting the cert with X's public key and comparing the result to a hash of the Y and K_Y which are provided.

4. Either the cert would decrypt properly and would be untrustworthy or the key would fail to decrypt the cert properly.

Lecture 55

1. There is some sort of unimpeachable authority.

2. Certs should have an expiration date past which they shouldn't be trusted. This could stop potential attacks by timing out malicious certs.

3. They transmission could not be trusted.

Lecture 56

1. RSA, AES-256

2. This could cause the protocol to break or become insecure.

3. The keys have to be able to be applied in any order or the protocol would not work.

4. $(M \text{ xor } K_a) \text{ xor } ((M \text{ xor } K_a) \text{ xor } K_b) = K_b$
   Once you have K_b, you can xor it with $(((M \text{ xor } K_a) \text{ xor } K_b) \text{ xor } K_a)$ to obtain M

5. $((M \text{ xor } K_a) \text{ xor } K_b) \text{ xor } (M \text{ xor } K_b) = K_a$, where K_b was obtained above.

6. $((M \text{ xor } K_a) \text{ xor } K_b) \text{ xor } M \text{ xor } K_b$

7. They may contain mathematical loopholes which are difficult to see.

Lecture 57

1. The internet relies on well defined behavior for commerce and communication.

2. The internet relies on authenticity for commerce and communication.

3. That the public keys are accessible.

4. Transmission of private information.

5. Yes, only the sender could have encrypted the information because they used their private key.

6. If a third party intercepts both messages then they can obtain both private keys by using the public keys.

Lecture 58

1. Extra steps may cause a breach in security or a slowdown in transmission.

2. You could use the information sent in the clear to crack the encryption.

Lecture 59

1. It may be difficult to tell if the person cracking the message is legitimately decrypting it.

2. It could cause the sender or receiver to become confused and disclose information that it shouldn't.

3. a man-in-the-middle attack lets the attacker intercept all communication but does not necessarily let them see the decrypted information.

4. The attacker has to pass along every message it receives or it may be detected.

5. Transmissions can arrive at any time because such systems are distributed.

Lecture 60

1. No, there would be no way to check the freshness of messages.

2. 1. A wants to comm with B. S knows this.
   2. S generates a new key and sends it to A. A knows it can send its key to B.
   3. A can send its key to B. B knows A's key.
   4. B sends its nonce to A. A knows that B is handshaking.
   5. A sends the nonce - 1 back to B to acknowledge the comm. B knows that the comm is valid and complete.

Lecture 61

1.

2. Yes, if you suspect that what you are receiving cannot be trusted.

3.

Lecture 62

1. Freshness of information.

2.

3.

Lecture 63

1. It guarantees that the behavior of the protocol is well defined and it reduces the risk of unforseen attacks.

2. It is the act of reasoning about what principals within the protocol are able to infer from the information passed to them.

3. In the behavior of the program.

Lecture 64

1. A system of logic which uses conditional predicates.

2. A shared its key with B, so any message encrypted with the key must come from B.

3. The nonce implies that the message is fresh so if the nonce is still valid and B said X then B must still believe X.

4. A trusts B and B has power over X, so A must believe X too.

5. It attempts to turn the message sent into its intended semantics. It is important for keeping track of who knows what at each step of the protocol.

Lecture 65

1. If no confidential information has moved around, then any inferences drawn by the receiver don't matter.

2. It represents what the receiver may reasonably believe.

3. This can expose obvious faults in the protocol which would have gone unnoticed otherwise.