Emily Ngo

Emn367

Ngo.emily@utexas.edu

Lecture 53

1. You want it to be non-reusable so an attacker can't strip the signature and use it for another message.
2. The message itself is expensive.
3. That the signature is unforgeable, authentic, non-reputable, tamperproof, and not reusable.

Lecture 54

1. They are authorities that are trusted to check credentials and certify parties.
2. When X uses its private key to sign the message, others can see that only X could have signed it.
3. The hash ensures that the message of Y's identity has not been altered.
4. The X's public key is just used to decrypt X's message and check Y's certificate. Z can still try to use it to confirm Y's certificate, but it might not work if it is truly not X's public key.

Lecture 55

1. An unimpeachable authority; authority that everyone believes.
2. The certificate will expire, this way the subject only has a time period of when it should be trusted before it needs to be certified again. This is incase overtime the subject becomes untrustworthy.
3. The certificate is not valid, and subject shouldn't be trusted.

Lecture 56

1. Clark and Wilson Certification and Enforcement rules are protocols to follow.
2. The end goal of communicating secret content could fail.
3. Encryption algorithms are not able to undo inner encryptions because it is not commutative. If the ciphers commute this problem that the encryption algorithms have can be solved.
4. He can just XOR step 2 and 3 and then XOR the result with Step 1.
5. He can XOR step 2 and step 3 to get Ka alone.
6. He can XOR step 1 and 2 to get Kb alone.
7. Not a lot of mechanisms are commutative, and if they are they might have security issues so that is why it is hard to design.

Lecture 57

1. Internet is a hostile and unstable environment activities in general need an IP to connect to and relying data to and from a local network and internet.
2. Cryptographic protocols helps us secure activities like inputting passwords, exchanging emails, or download/uploading materials.
3. Each have reliable public keys, the receiver actually gets the message.
4. Each party can authenticate the message being sent.

5. Assuming if each party has the public key for the sender they can authenticate who sent the message by decrypting with that public key.
6. An eavesdropper can decrypt a message that was intended for B by sending the message again to B and B will decrypt it with its private key (signature).

Lecture 58

1. Protocols might implement successive steps that can be easily cancelled, by having extra unnecessary steps this might be more likely.
2. It is a confidentiality issue, if the message is sent out into the clear it is susceptible to attacks.

Lecture 59

1. It gets hard to define what the attacker can do with the information or wants to do with it. Such as impersonation or eavesdropping or man in the middle.
2. It could be that the replay sends message later on that can disrupt a protocol or confuse sender and receiver, which is similar to interleaving attack but the messages are known.
3. An interleaving attack is an attack where there are no info to be gain, the end goal is to disrupt a protocol without gaining information in return by sending messages.
4. For certain attacks to occur the attack must already have some known knowledge about the protocol, like the known-key the attacker must have the key from a previous time or is able to generate it which is unlikely.
5. The party involve doesn't know anything about the activity of the protocol except the messages received or sent. This way attackers can't extract info from the parties involved.

Lecture 60

1. The nonce is used to determine if a message is a replay or not. (fresh or not)
2. A. A asks S for a key to send to B. Nonce tells B that it is fresh.
   B. Sender makes a key with the nonce, B, the Key, and encryption with Kbs. A knows the message is fresh.
   C. A send the Kbs encryption which lets B knows it is step 3. B knows Kbs is key is from S.
   D. B send to A a new nonce. A knows B received message.
   E. A send to B that nonce – 1. B knows A knows B received message with correct key.

Lecture 61

1. The way that S know that message is from A is thru Kas, a sender sending something to S can impersonate A because of the shared key knowledge.
2. Depends on the strength of the encryption.
3. Regularly change the Keys shared with parties and the key server.

Lecture 62

1. Allows party to prove identities and prevent eavesdropping and replay attacks with M and Kbs and Kas.
2. In NS B knows that A gets the Key for the session or not.

3. Not allow any messages that are replays of sent messages to be sent again.

Lecture 63

1. To make sure the protocol is doing what it is supposed to be without major consequential flaws.
2. Modal logic that allows reasoning that a protocol is correct.
3. Beliefs comes in between the sequence of message exchanges of the program. After receiving a message what do you believe?

Lecture 64

1. Modal logic is logic that uses operators, propositional, and predicate logic.
2. If A and B share a Key and A sees that Key from B then A knows it is from B.
3. If X is fresh and A knows it is from B, then B believes X too.
4. If B is superior to X and B believes X then A believes X too.
5. One purpose of idealization is to omit parts of the message that do not contribute to the beliefs of the recipients. To get from protocol steps to logical inferences, idealization is used.

Lecture 65

1. Plaintext is easily forged so it is omitted.
2. The steps should be trying to accomplish whatever the protocol is trying to accomplish.
3. The beliefs are basically assumptions that can be exposed in the real protocol.