Name: Terry Liang

EID: twl378

CS Login: tliang

Email: liang810612!

Assignment 4

Lecture 53

1. It cannot be reused for another message.
2. Because the hash is fixed finite short value, the public key encryption is expensive to apply.
3. Unforgeable, authentic, no repudiation, tamperproof, not reusable.

Lecture 54

1. It vouches for the accuracy of the binding.
2. Because the message would become reliable.
3. It is the reference when Z try to know if Y and Ky are not corrupted or altered.
4. Z would not be able to decrypt the message.

Lecture 55

1. The root of trust must be someone really trustworthy.
2. Because the certificate is valid for certain amount of time.
3. The message might have been altered or corrupted.

Lecture 56

1. The Diffie-Hellman key exchange, AES
2. One might not be able to receive the message.
3. So one can reach inside the property.
4. It can store three messages and XOR combinations of them to extract any of M, Ka, and Kb.
5. It can xor with Kb and they are canceled out which has Ka exposed.
6. It can xor with Ka and they are canceled out which has Kb exposed.
7. Because one might think it is unbreakable and it is not.

Lecture 57

1. It can assure that the sender and receiver both receive the valuable messages in a hostile environment.
2. It uses cryptographic mechanisms to accomplish some security-related function.
3. There is a public infrastructure key in place, and each has the key.
4. Both A and B know that each other has received the message or sent the message
5. Yes. Both A and B could possibly have receive or send the message to each other.
6. Someone might have the keys to decrypt their private keys. Or A and B are not the real person.

Lecture 58

1. Because it can save the space and time to decrypt the message.
2. It would save more spaces in the message and lower the cost.

Lecture 59

1. Because there are many ways that the attackers can attack the system without really being discovered.
2. The party can get confused when they used the replay attack to interject message.
3. No, I do not think so. Because they attack on the protocols for the valuable messages.
4. No arbitrary messages. It is still hard to think of many restrictions that can restrict their attacks.
5. Any party to the protocol will not know anything about the current run of the protocol except the messages it has received and sent.

Lecture 60

1. Probably not. The nonces are to notify the parties that their messages are fresh.
2. I. A tells S that he wants to talk with B with the nonce
   S belive its from A because it has A's nonce
   II. S tells A that he's encrypted the message with two keys Kbs,Kas
   A knows because there is his encrypted key outside the message
   III. A sends message to B with Kbs outside the message that wants B to decrypt
   When B decrypted, he knows it's from A because there is Kab
   IV. B sends A a new nonce with the key Kab, saying B got the key from A
   A can tell because he sees the key
   V. A says that he got the message and give B a new Key for proof
   B knows that calculation and can use the message.

Lecture 61

1. The attacker could send the message before the real A sends it.
2. Yes and no question. It depends on how strong the encryption is.
3. Maybe create nonce with step 3 or create sophisticate encryptions.

Lecture 62

1. It seems to guarantee that it is a fresh message.
2. A talk to B and wants B to send message to S. To authenticate both A and B. but B does not know A has the key.
3. Encrypt inside the message.

Lecture 63

1. Because it is crucial to the internet and we should get them right.
2. It is a formal system for reasoning about beliefs. Any logic consists of a set of logical operators and rules of inference.
3. It could be at the beginning, in the middle, or the output of the program.

Lecture 64

1. It's a type of formal logic that extends classical propositional and predicate logic to include operators expressing modality.
2. If A belies A and B has shard K and A sees the message with K then A believe it is from B.
3. If A believe that the message X is fresh and A believes B once said X, then A believes B believes X.
4. If A believes B has jurisdiction over X and A believes B believes X, then A believes X.
5. It attempt to run the message sent into its intended semantics. I is to omit parts of the message that do not contribute to the beliefs of the recipients.

Lecture 65

1. Because there is no special contents besides the plaintext.
2. It just tries to prevent some bad things that could happen.
3. The BAN tries to show people explicitly what vulnerability that protocol might have by exposing every assumption there is.