Chad Custodio

Cgc735

Aitan791

chadcus@gmail.com

Week 4 Questions

Lecture 53

1. So nobody else could have potential access to it if it were to be in a different place.
2. The hash will be a small finite value rather than a long message.
3. It is unforgeable, authentic, non-repudiated, tamperproof, and not reusable.

Lecture 54

1. It helps ensure some sort of reliability with the key because of the web of trust.
2. To put it's signiture and force the receiver to use it's public key.
3. To compare hash values to make sure that the data items are unchanged.
4. Then it would check Y's private key to ensure it was valid binding.

Lecutre 55

1. Certifications
2. Puts a time contraint for validity.
3. Then it is not valid.

Lecture 56

1. Almost every every model involved in what we had learned during the course
2. It would not be as strong of a protocol and wouldn't be worth using.
3. So you can get inside of the "box" and take out lock off.
4. Sees how many XOR's there are and then try to cancel them out.
5. Figure out which message leaves it open and make it to that same state with XOR's.
6. Pretty much the same reason at question 5.
7. It is hard to design something that could effectively keep out eavsdroppers while making sure that there are no missed steps.

Lecture 57

1. Almost everything on the internet requires some sort of exchange of messages.
2. They pretty much do every kind of security assurance to make sure that the information is safe.
3. There is a public key structure in place and that these keys are reliable.

4. To make sure that the shared key is authenticated to the other and make sure that one sees that the other received the message.
5. Yes because they both need each others key to unlock and see the message and B sent a message to say that he received A's message.
6. At some point there will be a way for an attacker to strip off the keys and see the secret key.

Lecture 58

1. To shorten the process and still get the same goals.
2. Typically you wouldn't want these items to be taken and decrypted.

Lecture 59

1. Because there are many ways that an attackers could look like an authentic authority. It is also hard to know if something is compromised.
2. Valuable information is reusable because of the recorded messsage.
3. Yes because a bad attacker might just get his own message or other non-useful messages from the flow.
4. Attacker cannot create a message with a key that he should not have at all.
5. Receiver know what the messge means and how to respond to it..

Lecture 60

1. No.
2. I want to communicate with B. There are no keys yet.
Here are the keys and it is fresh. I can finally send the message to B.
You are a part of the message flow. A wants to communicate with me and there is a key that I can use to do this.
I received the message from the previous step. B has the key and can use it.
I can decrypt the message to get the key. A has the key and can use it.

Lecture 61

1. Even if the key were changed, having Kas means that the attacker could access any changes to A.
2. It depends on the strength of the encryption.
3. Find out the most vulnerable steps in the protocol.

Lecture 62

1. There is direct communication from the start.
2. In NS, B eventually knows if A got the key.
3. Require decryption with B's private key.
Lecture 63
1. It is good to know about the protocol's correctness.
2. A formal system for reasoning about beliefs.

3. From belief statements that are assumptions about the program.

Lecture 64

1. Extends classical propositional and predicate logic to include operators expressing modality.
2. A will know a message is from B because it is encrypted with their shared key.
3. Generates a trust with a statement of beliefs.
4. Allows A to trust something because of B.
5. Turns the message sent into its intended semantics. It omits parts of the message that do not contribute to beliefs.

Lecute 65

1. Because these things don't really help contribute to certain beliefs.
2. To predict what is needed to help with the flow
3. Because it helps bring more beliefs that would potentially benefit the protocol