Haoshu Yuwen
Hy2892

Assignment 4

Lecture 53:
1. If a digital signature was reusable, then a third party attacker could lift the signature use it themselves.

2. Signing the hash means that you wouldn't have to also hash the signature and is therefore theoretically more efficient.

3. S sent the message and only R can decrypt it.

Lecture 54:
1. So a user can be sure that a person's listed public key is actually their public key.

2. That way, anyone else can confirm that it was X that signed it.

3. It lets everyone know that the contents of Y and Ky were not modified.

4. Then Z could not be sure of the previous assumptions?

Lecture 55:
1. There is an unimpeachable authority.

2. So we have flexibility. Something won't necessarily be valid forever.

3. Something has been tampered with.

Lecture 56:
1. RSA encryption would be a good example.

2. The entire system would then be vulnerable.

3. If they didn't commute you wouldn't be able to retriever your own encryption to decrypt.

4. He can XOR the third step with Kb.

5. XOR the second step with the result of the first step.

6. Just like every other security issue, protection must be against all threats while threats only have to exploit one weakness.

Lecture 57:

1. The Internet is all about the exchange of information so protocols dealing with information exchange are a fundamental part of the Internet.

2. The same as above but dealing with sensitive topics.

3. We assume that A and B bot have a public and private key and that the messages sent from A to B actually reach B and vice versa.

4. The goal is to pass K to the other party without a third party member from finding out what K is.

5. No cause a clever third party actor can deduce K if I'm right regarding the flaw in this protocol.

6. A third party actor may use the encrypted messages to cancel each other out, deducing K.

Lecture 58:
1. Efficiency purposes?

2. Again, so you don't waste effort encrypting something that doesn't need it.

Lecture 59:
1. Without seeing the results, it's difficult to classify it as an attack.

2. For example, suppose the military sends the order "bomb city x" and then a replay attack sends the message again a year later in peacetime. That would be pretty bad probably.

3. Yeah, failed attacks.

4. No the messages the attacker sends must be compatible with the protocol.

5. Makes it less predictable and therefore less vulnerable to attack.

Lecture 60:
1. Technically yes since B would still receiver the message, it's just that B will not be certain this message is not a repeat of a previous one.

2. uhh

Lecture 61:
1. He's already cracked the key once, I'm sure he can do it again.

2. Yes. I'm sure it happens all the time.

3. I would let people know about them and just be careful cause I don't think there's a perfect protocol

Lecture 62:
1. Assurances that A sent the message.

2. Yes. If the message is current.

3. Don't make the receiver send anything back.

Lecture 63:1
1. So users can have a reasonable expectation of effectiveness.

2. "Belief logics allow reasoning about what principals within the protocol should be able to infer from the messages they see."

3. The users.