Name: Cohen Ellis
EID: cce335
CS Login: coel09
Email: coel09@yahoo.com

CS361 Questions: Week 4

The questions marked with a dagger (†) require external research and may be more extensive and time consuming. You don't have to do them for the assignment but, but do them to increase your competency in the class.

Lecture 53

1. Why is it important for a digital signature to be non-reusable?

   We do not want the signature to be able to be used for other messages that may not be from S.

2. Why is it the hash of the message typically signed, rather than the message itself?

   The hash is fixed in size and generally is short in value.

3. What assurance does R gain from the interchange on slide 4?

   Only R can decrypt the message sent to it by S with his private key. With S's private key used to encrypt the message, R knows that the message was sent from S.

Lecture 54

1. What is the importance of certificate authorities?

   So that an individual can vouch the authentication of another party.

2. In the example on slide 5, why does X sign the hash of the first message with its private key?

   So that Z can see if X is trustworthy, by using X's public key.

3. Why is it necessary to have a hash of Y and K_y?

   In order to make sure that the original message was not changed.

4. What would happen if Z had a public key for X, but it was not trustworthy?

Name: Cohen Ellis
EID: cce335
CS Login: coel09
Email: coel09@yahoo.com

Z would not be able to open the message from Y, or unhash the message.

Lecture 55

1. What happens at the root of a chain of trust?

   The root is the one giving authorization to the certificates.

2. Why does an X.509 certificate include a "validity interval"?

   If the information is old/outdated, you should not trust it.

3. What would it mean if the hash and the received value did not match?

   This would mean that the message was intercepted and changed, or that the certificate is not trustworthy.

Lecture 56

1. What are some protocols previously discussed?

   A one-time pad, Diffie – Hellman, AES, and public and private keys.

2. What may happen if one step of a protocol is ignored?

   The receiver would not be able to open/read the message.

3. Why must the ciphers commute in order to accomplish the task in slide 4?

   This is so that S can reach inside of R's encryption to undo his.

4. Describe how an attacker can extract M from the protocol in slide 6.

   The attacker can xor all of the messages sent and cancel out all of the keys to get to the message.

5. Describe how an attacker can extract K_a from the protocol in slide 6.

   The attacker can xor the similar Kb keys and see that the Ka key is also xor with M.

Name: Cohen Ellis
EID: cce335
CS Login: coel09
Email: coel09@yahoo.com

6. Describe how an attacker can extract K_b from the protocol in slide 6.

   The attacker can xor messages 1 and 2 together, and find the similarities with message 3.

7. Why are cryptographic protocols difficult to design and easy to get wrong?

   Many times, if used incorrectly, the receiver would not be able to read the message, or an eavesdropper can collect all of the key and message information.

Lecture 57

1. Explain the importance of protocols in the context of the internet.

   So that information can be communicated securely.

2. Explain the importance of cryptographic protocols in the context of the internet.

   So that information can be sent securely.

3. What are the assumptions of the protocol in slide 6?

   Both assume that each has reliable access to their perspective keys

4. What are the goals of the protocol in slide 6?

   That A and B are communicating securely.

5. Are the goals of the protocol in slide 6 satisfied?

   Yes they are satisfied, but it is unknown if the message was sent.

6. How is the protocol in slide 6 flawed?

   If the messages we intercepted and xor, the message could be opened by an eavesdropper.

Name: Cohen Ellis
EID: cce335
CS Login: coel09
Email: coel09@yahoo.com

Lecture 58

1. Why is it important to know if a protocol includes unnecessary steps or messages?

   Protocols take up space and include sending messages back and forth. We do not want to send messages that could be intercepted and decrypted using these messages.

2. Why is it important to know if a protocol encrypts items that could be sent in the clear?

   It is important to not send messages that could be intercepted and used to get the keys or messages. We do not want to continuously sent messages.

Lecture 59

1. Why might it be difficult to answer what constitutes an attack on a cryptographic protocol?

   The attacker can use different types of attacks.

2. Describe potential dangers of a replay attack.

   The attacker can use past keys to try to open messages.

3. Are there attacks where an attacker gains no secret information? Explain.

   No, when dealing with protocol it is safe to assume that all attacks can gain secret information.

4. What restrictions are imposed on the attacker?

   The attacker has to know something about the protocol, he can’t just drop in and attack arbitrarily.

5. Why is it important that protocols are asynchronous?

   We do not want the attack to be able to know when data is being sent, and do not want to have anything recorded.

Name: Cohen Ellis
EID: cce335
CS Login: coel09
Email: coel09@yahoo.com

Lecture 60

1. Would the Needham-Schroeder protocol work without nonces.

   No.

2. For each step of the NS protocol, answer the two questions on slide 5.

   Step 1: S needs to generate a key for A & B using Na. Step 2: A believes that it is confidential and that S has responded to the first message. Step 3: B knows that the message came from S. Step 4 and Step 5: knows that each received the messages and were able to decrypt the message.

Lecture 61

1. As in slide 5, if A's key were later changed, after having K_{as} compromised, how could A still be impersonated?

   The attacker can still send messages to S and then receive keys when sending to B.

2. Is it fair to ask the question of a key being broken?

   It is fair because it is still a type of attack.

3. How might you address these flaws if you were the protocol designer?

   After step 2 I would make it mandatory for a key change after every interaction with S and A and, S and B.

Lecture 62

1. What guarantees does Otway-Rees seem to provide to A and B?

   That they both share a secure key with S.

2. Are there guarantees that Needham-Schroeder provides that Otway-Rees does not or vice versa?

   Yes.

Name: Cohen Ellis
EID: cce335
CS Login: coel09
Email: coel09@yahoo.com

3. How could you fix the flawed protocol from slide 4?

   Have K encrypted with its public key until it receives the shared key with B.

Lecture 63

1. Why is the verification of protocols important?

   Flaws have been discovered in protocols published many years before the flaw was found.

2. What is a belief logic?

   They allow reasoning about what principals within the protocol should be able to infer from the messages they see.

3. A protocol is a program; where do you think beliefs come in?

   Beliefs come in when you need to implement protocol.

Lecture 64

1. What is a modal logic?

   Has primitives for formulas and rules to implement them.

2. Explain the intuition behind the message meaning inference rule.

   That A can trust B if he uses the key that they both share.

3. Explain the intuition behind the nonce verification inference rule.

   That x is a belief, and not a message.

4. Explain the intuition behind the jurisdiction inference rule.

   If I hear something from an expert, I can believe them.

5. What is idealization and why is it needed?

   Turns the message into the intended semantics.

Name: Cohen Ellis
EID: cce335
CS Login: coel09
Email: coel09@yahoo.com

Lecture 65

1. Why do you think plaintext is omitted in a BAN idealization?

   Plaintext can be forged.

2. Some idealized steps seem to refer to beliefs that will happen later in the protocol. Why would that be?

   We assume that these beliefs will happen by the end of the step or protocol since the idealized versions do not happen one after the other.

3. One benefit of a BAN proof is that it exposes assumptions. Explain that.

   Many times the if the assumptions are surprising, you can know how to fix your protocol.