Questions Week 4

Name: Matt Hendrickson
EID: mjh2793
CS Login: mjh2793
Email: matthewjames@utexas.edu

Lecture 53

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

Otherwise it could be stolen and reused maliciously

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

you sign the hash because the hash is a fixed finite value but the message could be very long.

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

That it was S who sent the message because only S has the inner key used to encrypt the message

Lecture 54

1. What is the importance of certificate authorities?

It acts as the mediator between two parties to verify that a certificate is valid

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

It shows that X has certified the message and that is it valid.

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

because the message might be very long but the hash is a fixed number.

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

Z would not be able to open the message because it did not have Y's private key.

Lecture 55

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

The root gives out cerifications and authorizations to create other certificates.

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

Some certificates might only be good for a certain period of time

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

The message had been tampered with.

Lecture 56

1. What are some protocols previously discussed?

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

it depends on the step. if step one is ignored, someone could change the message that ivan would read.

if step 2 ignored, then someone could change/read the message that the sender would see.
if step three igored, then ivan could not read the message.

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

If there's a cipher blocking you from taking your "lock" off then the process breaks down.

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

By storing the three messages, an attacker can XOR them in different combinations to get the message and the two keys used to encrypt them.

5. Describle how an attacker can extract Ka from the protocol in slide 6.

XOR message one and two to get Kb.

6. Describle how an attacker can extract Kb from the protocol in slide 6.

XOR message two and three to get Ka.

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

An attacker needs only to find one way to break through and then everything is compromised. In the previous question the attacker was able to get not only the message that was supposed to be confidential but also the keys. Any further encryptions using those keys would be useless.

Lecture 57

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

Since the internet is a way to connect many different people, there must be a shared "language" so that everyone can communicate. Things like IP addresses as a way for everyone to link together.

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

Since the internet is an insecure network, different groups must agree to a set of rules to accomplish some security purpose(confidentiality, integrity, etc.)

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

only A and B have their own secret keys.

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

To ensure confidentiality and that in case 1, it was sent by A and case 2 it was sent by B

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

maybe

6. How is the protocol in slide 6 flawed?

not sure

Lecture 58

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

Those could be ways for an attacker to break in.

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

That could a way for an attacker to get an encrypted message and save it to try and solve the encryption later.

Lecture 59

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

2. Describe potential dangers of a replay attack.
You just have to be able to listen in and record what you hear. You're not attempting to break anything or even crack any passwords/encryptions. It seems like it would be ahrder to detect something like this.
3. Are there attacks where an attacker gains no secret information? Explain.
Maybe the attacker just want to disrupt the flow in information.
4. What restrictions are imposed on the attacker?
A designer should assume his attacker has all the advantages, he can listen in on everything and put his own messages into the flow of information.
5. Why is it important that protocols are asynchronous?

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.
1. A and B are sharing using this nonce for this message
   that A and B are going to be using this nonce .
2. S tells A "Here is a key just for us. you can decrypt it and then send the message I encrypted to B who can then decrypt it, and you can tell its from me because I used our nonce."
   A can decrypt the message and then send the inner message to B
3. A sends a message to B that B can decrypt with the key Kbs^-1
   B knows this message came from A because the message has the AtoB key, Kab.
4. B send a nonce to A
   This message is form B because of the key used and the nonce sent.
5. ??

Lecture 61
1. As in slide 5, if A's key were later changed, after having Kas compromised, how could A still be impersonated?
They could have access to A's nonces.
2. Is it fair to ask the question of a key being broken?
Of course, you have to be able to consider all possibilities of attack.
3. How might you address these flaws if you were the protocol designer?
???

Lecture 62
1. What guarantees does Otway-Rees seem to provide to A and B?

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

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

Lecture 63

1. Why is the verification of protocols important?

It checks if flaws exist within a protocol and if they do, where they appear under what circumstances.

2. What is a belief logic?

a formal system for reasoning about beliefs.

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

Lecture 64

1. What is a modal logic?

formal logic that also includes expressions of modality. Modality is a linguistic term that involves the expressions of belief.

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

If A believes that A and B share a key, K. and A sees a message encrypted with K, then A believes that B has said X sometime in the past.

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

If A believes message X is fresh and A believes B once said X, then A believes B believes X

4. Explain the intuition behind the jurisdiction inference rule.

5. What is idealization and why is it needed?

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?

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

In any proof you have certain assumptions you have in place to make the proof possible.