CS361 Questions: Week 4

Lecture 53

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

If a signature could be re-used, it could be forged.

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

Its less expensive. Signing multiple blocks of a message can be difficult. Potential exploits.

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

Only R can remove the outer layer of encryption; therefore, R knows the message has not been tampered with.

Lecture 54

1. What is the importance of certificate authorities?

To verify that a public key is associated with a certain person.

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

To verify that X actually sent the message.

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

To compare against the Y and Ky sent along with it. If a hash of Y and Ky on the side of Z does not produce X's previously hashed Y,Ky, then the message may have been tampered with.

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

Z wouldn't trust X for verifying the message given by Y

Lecture 55

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

Ideally, the root is an unimpeachable authority of trust.

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

Requires re-authentication after a certain point, keeps trust renewed. An old certificate could have been stolen.

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

Data may be corrupted.

Lecture 56

1. What are some protocols previously discussed?

Diffie-Hellman

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

The message fails and data cannot be read.

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

If A can reach in and pull of his own lock while B's is still on, then the message is essentially secure for B to use.

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

1 XOR 3 XOR 2

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

2 XOR 3

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

1 XOR 2

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

All flaws are hard to see for a defender. One flaw of all of them is easy to see for an attacker.

Lecture 57

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

Any agreed upon form of communication over the internet is a protocol. If protocols didn't exist, one may not understand what a bunch of 1's and 0's flowng into their modem means.

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

To ensure secure communications.

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

There is a PKI in place and A and B have each others public key.

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

To share a secret key K and authentication of one another.

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

No, someone can

6. How is the protocol in slide 6 flawed?

K can be extracted by C intercepting old messages and sending them back.

Lecture 58

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

To see if a protocol could be done more efficiently.

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

Same as #1.

Lecture 59

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

Are any assets potentially vulnerable afterwards?

2. Describe potential dangers of a replay attack.

An adversary posing as another user and being successfully authenticated by sending old messages.

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

Yes, they can gain authentication instead.

4. What restrictions are imposed on the attacker?

It is hard to specify what the limitations of an attacker are.

5. Why is it important that protocols are asynchronous?

The protocol has to be designed that when a message is received the receiver knows how to respond to it.

Lecture 60

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

Nonces provide the ability for showing a message is fresh, if nonces weren't used then there is a significant amount of vulnerability exposed.

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

1. A is requesting a secret key from S to be used with B. A is providing a nonce to prove freshness. S believes that A generated the nonce properly.

2. S is providing a secret key to use between A and B for A, the nonce first given to verify the message, and the secret key along wth A's identity encrypted with B and S's secret key. Basically, A here is a key and here is verification, send this to B so he can receive the key and verify its secure. A believes S generated a fresh key for A and B to use; additionally, A believes S encrypted a message for B with a key that S and B share.

3. A tells B that here is a key encrypted with a key he shares with S. B realizes this message only could have been generated by S.

4. B sends a nonce for verification and ack. A sends a change of the nonce to show verification and ack.

Lecture 61

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

The only method of authentication S has of A is through Kas. Therefore, C can use Kas to impersonate A by generating new keys to talk with others.

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

Depends on strength of encryption.

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

Implement key validity periods, increase level of encryption on communications.

Lecture 62

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

Proof of authentication of each other.

2. Are there guarantees that Needham-Schroeder provides that Otway-Rees

does not or vice versa?

Otway provides proof of authentication

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

Use nonces for freshness.

Lecture 63

1. Why is the verification of protocols important?

To verify that certain assumptions can be made when using a certain protocol and that the protocol satisfies certain requirements.

2. What is a belief logic?

A modal logic that allows you to reason about what the principles of a protocol are allowed to believe after a message is received.

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

We believe that the program should work as intended. E.g. a messenger created a proper nonce.

Lecture 64

1. What is a modal logic?

formal logic used to prove beliefs and assumptions.

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

If A can believe something, then A can act upon that belief or assume transitively about that belief.

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

If A thinks a message is fresh and B sent that message, then A thinks B thinks that message is fresh.

4. Explain the intuition behind the jurisdiction inference rule.

If A believes B has jursidiction over X, then A believes what B says about X.

5. What is idealization and why is it needed?

To understand what a piece of message is used to achieve some purpose.

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?

It assumes that these beliefs will happen later in order to make an assertion now.

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

It shows how the assumptions are used to carry out a proof. It exposes weaknesses in proofs.