Name: Jordan Graves
EID: jlg3585
CS Login: jgraves
Email: j.l.graves03@gmail.com

Lecture 53
1. Why is it important for a digital signature to be non reusable?

The signature is a form and authentication. If it were reusable, any documents signed with it would lose authentication integrity. A re-useable signature undermines the purpose of the signature.

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

Public key encryption is expensive. The message may be arbitrarily long but the hash is a fixed value.

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

Unforgeable, authenticity, non-repudiation, tamper proof, non reuseable

Lecture 54
1. What is the importance of certificate authorities?

To be the medium between two people that are mutually suspicious. Serves as a way to validate authenticity of parties or keys.

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

So that the receiver will know that X sent the message.

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

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

Lecture 55
1. What happens at the root of a chain of trust?

Checks credentials to certify authenticity, (binding between public key and identity is valid).

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

It is used to check that the certificate is not expired.

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

The certificate is invalid possibly because the wrong public key was used.

Lecture 56

1. What are some protocols previously discussed?

AES encryption, use of public/private keys, Bell-Lapadula

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

The entire protocol can be a failure. Data can be intercepted, identities can be mimicked. Security is basically compromised.

Or, data can also be inaccessible as intended.

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

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

By XORing all 3 messages.

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

By XORing the last 2 messages.

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

By XORind the first two messages.

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

They can initially make sense intuitively yet have serious fundamental flaws.

Lecture 57

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

The internet is essentially a network of connected nodes which must exchange and understand one another's messages.

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

Sometimes, messages must be sent through the network that is the internet is a secure way such that it is confidential between certain individuals.

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

There is a public key infrastructure in place. Each party has a reliable version of the other's public key.

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

A shares a secret key with B, each party is authenticated to the other.

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

6. How is the protocol in slide 6 flawed?

Lecture 58

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

It is like a program such that one step may depend on the other.

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

Knowing this could shed light on what steps of a protocol are unnecessary and could allow for simplifying the protocol without undermining the goal of the protocol.

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.

An attacker can intercept a password or hash during communication between two parties, then later, while posing as one of the parties can send the intercepted messages, password, or hash as a way to falsely identify themselves as the other party.

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

Through and interleaving attack an attacker can essentially interrupt the communication by bringing it down completely. The attacker gains no information but keeps information from flowing.

4. What restrictions are imposed on the attacker?

MEssages that the attacker interjects can not be arbitrary. Cannot inject a message with a key that the attacker does not have.

5. Why is it important that protocols are asynchronous?

This is the nature of distributed networks. The parties need not, must now and should not have to know what is going on outside of their bubble.

Lecture 60
1. Would the Needham-Schroeder protocol work without nonces?

No, this is used to prevent replay attacks.

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

1.
What is the sender trying to say in her message?
Hey, S! I'm A and I want to talk to B, so generate a new key for us. And by the way, here's a nonce that you can use in subsequent messages so we'll be sure that you're responding to this request.

What is the receiver entitled to believe after receiving the message?
A wants to talk to B, so I need to generate a new session key and get it to them. I should use N_a *in the response so that they'll know it's fresh.*

2.
What is the sender trying to say in her message?

A, here is the session key as well a message with your identity as well as the session key that only B can decrypt that you should send to B. Also, here’s the nonce so you can see that this message is fresh

What is the receiver entitled to believe after receiving the message?

S has generated the session key and an encrypted a message that only B and S can encrypt, once A sends the encrypted message to B, B will have the session key.

3.

What is the sender trying to say in her message?

Hey B, here is the session key, decrypt it with your KB key.

What is the receiver entitled to believe after receiving the message?

That A has the session key, but A does not know B has it.

4.

What is the sender trying to say in her message?

Hey A, I received the session key, are we in the same boat?

What is the receiver entitled to believe after receiving the message?

That B has the session key.

5.

What is the sender trying to say in her message?

Hey B, I acknowledge that you recieved the key and we can use it now to communicate.

What is the receiver entitled to believe after receiving the message?

That A and B now have a secure session key that can be used to communicate.

Lecture 61

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

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

Yes and no. It depends upon the strength of the encryption.

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?

Protocols can be notoriously difficult to get correct so it would be nice to have a way to ensure they meet specifications.

2. What is a belief logic?

A modal logic that allows you to reason about what the parties of the protocols are entitles to believe after receiving a message/

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

The program only runs on belief of some outside entity. A client program is separate from a server program, it runs on the belief that the server program follows some set of rules. the same goes for a protocol which runs based off some assumptions.

Lecture 64
1. What is a modal logic?

The study of the deductive behavior of the expressions 'it is necessary that' and 'it is possible that'.

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

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

4. Explain the intuition behind the jurisdiction inference rule.

5. What is idealization and why is it needed?

An attempt to turn a sent message into its intended semantics.

Lecture 65

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