Name: Luis C Lopez
EID: LL9338
CS Login: LL9338
Email: lclg21@utexas.edu

CS361 Questions: Week 4

Lecture 53

1. Why is it important for a digital signature to be non reusable?
It means that the signature cannot be detached and reused for another message.

2. Why is it the hash of the message typically signed, rather than the message itself?
Because the hash would be a fixed finite small short value.

3. What assurance does R gain from the interchange on slide 4?
That only S can use the private key, a third party can verify the signature with the public key, only R can remove the outer layer of encryption and the signature is tightly bound to the message M.

Lecture 54

1. What is the importance of certificate authorities?
The certificate authorities would vouch for the accuracy of the binding.

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

3. Why is it necessary to have a hash of Y and Ky?
That way X can produce a message with Y's identity and public key, and the signed hash value, so all that becomes the certificate.

4. What would happen if Z had a public key for X, but it was not trustworthy?
Z would check the hash value message of Y and Ky and compares it to the hash value message produced by X.

Lecture 55

1. What happens at the root of a chain of trust?
What happens is that they check very carefully to make sure that the binding between the public key and the identity was in fact valid.

2. Why does an X.509 certificate include a "validity interval"?
Because if a certificate is expired then there is no reason why to trusted so the validity interval means that only for a certain time the certificate has validity.

3. What would it mean if the hash and the received value did not match?
That the certificate is not valid. Someone could have tamper with it. That is why they compare the hash with the received value.

Lecture 56

1. What are some protocols previously discussed?
Cryptography, Key management, Access Control.

2. What may happen if one step of a protocol is ignored?
Then the sender or receiver would not be able to see the message.

3. Why must the ciphers commute in order to accomplish the task in slide 4?
Because if the ciphers commute, you would be able to reach inside the encryption to undo ours.

4. Describe how an attacker can extract M from the protocol in slide 6.
By Xoring Ka to (M Xor Ka) and then Kb to (M Xor Kb).

5. Describe how an attacker can extract Ka from the protocol in slide 6.
By Xoring M to (M Xor Ka)

6. Describe how an attacker can extract Kb from the protocol in slide 6.
By Xoring M to (M Xor Kb).

7. Why are cryptographic protocols difficult to design and easy to get wrong?
Because it is hard to come up with a best cryptographic protocol unless you are an expert in cryptology and plan to spend years reviewing the algorithm.

Lecture 57

1. Explain the importance of protocols in the context of the internet.
Because it is a structured dialogue between two or more parties in a distributed context controlling the syntax, semantics, and synchronization of communication and are designed to accomplish a communication-related function.

2. Explain the importance of cryptographic protocols in the context of the internet.
Because it uses cryptographic mechanism to accomplish some security-related function.

3. What are the assumptions of the protocol in slide 6?
There is a public key infrastructure in place and that each of them has a reliable version of the others public key.

Name: Luis C Lopez
EID: LL9338
CS Login: LL9338
Email: lclg21@utexas.edu

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

For A to send a message to B and know if B received it.

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

Yes because A gets to know that B received the message by B sending back a message signed by B.

6. How is the protocol in slide 6 flawed?

It is flawed because B doesn't know what step he is on when receiving the message.

Lecture 58

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

Because if we know that there are unnecessary steps in the protocol, We can try to make the protocol more efficient by having lesser steps.

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

To make the protocol more efficient and with less steps between A and B.

Lecture 59

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

Because there can be many possibilities of answers to the questions about what constitutes an attack.

2. Describe potential dangers of a replay attack.

An attacker would record messages and then use them at a later time.

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

Yes, an attacker can create an algorithm to destroy the message and still the attacker would not be able to gain any secret information by destroying it.

4. What restrictions are imposed on the attacker?

It is hard to know how to detect restrictions and impose them to the attacker. That is why the protocol should be robust in the face of such a determined and resourceful attacker.

5. Why is it important that protocols are asynchronous?

Because a party to a protocol won't know anything about the current run of the protocol except the messages it has received and sent. Also, except for the initiator, other parties will not know that they are participating until the receive the first message.

Name: Luis C Lopez
EID: LL9338
CS Login: LL9338
Email: lclg21@utexas.edu

Lecture 60

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

No because the Needham-Schroeder protocol uses nonces in their messages to verify that A and B have received their messages.

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

Step 1: A sends S a message saying that A wants to communicate with B with a new nonce for S to generate some keys for A and B.

Step 2: It generates a new key, Kab and packages that key and sends it back to A and its encrypted with Kas, which means that only A and S can see that message. So A has the key.

Step 3: A sends to B that message that was in step 2 encrypted with Kab. A has the key and B has the key.

Step 4: B sends A a new nonce so that A can know that B has the key.

Step 5: A sends back to B a the nonce with some function applied so that B can know that A can use the key.

Lecture 61

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

Because whoever receives the message, they don't know that Kas has been compromised and can think that A is still sending the message.

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

It depends on the strength of the encryption.

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

I would rewrite my own protocols and test it until I know for a fact that there are less flaws in the message.

Lecture 62

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

That A will know that B received the message and B will not that A can see that B saw the message. The same as Needham-Schroeder.

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

Both Needham-Schroeder and Otway-Rees provide the same results using a third party.

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

I would use Otway-Rees protocol to send the message to B so that there can be better encryption.

Name: Luis C Lopez
EID: LL9338
CS Login: LL9338
Email: lclg21@utexas.edu

Lecture 63

1. Why is the verification of protocols important?

Because protocols can be very difficult to get correct with flaws discovered in protocols many years before. So it would be nice to be able to reason about the verification of a protocol.

2. What is a belief logic?

It allows reasoning about what principals within the protocol should be able to infer from the messages they see. It allows abstract proofs, but may miss some important flaws and it is a formal system for reasoning about beliefs.

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

On every step, each receiver infers that the message was sent securely by the previous sender.

Lecture 64

1. What is a modal logic?

Is a type of formal logic that extends classical propositional and predicate logic to include operators expressing modality.

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

Means that if A believes that A and B share a key and A receives a message which is encrypted with that key then A is entitled to believe that message must have come from B.

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

If A believes that X is fresh and A believes that B once said x, then A believes that B believes x.

4. Explain the intuition behind the jurisdiction inference rule.

If A believes B has jurisdiction over X and A believes that B believes X, then A believes x.

5. What is idealization and why is it needed?

Idealization is a process to get from protocol steps to logical inferences. It is needed to turn the message sent into its intended semantics.

Lecture 65

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

Because it is not encrypted and there is not logic for that.

Name: Luis C Lopez
EID: LL9338
CS Login: LL9338
Email: lclg21@utexas.edu

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

Because S is a third party which means S knows what A and B will be communicating between ach other.

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

That B can assume that A sent the key without proving anything and by just using BAN logic.