CS361 Questions: Week 4

Daniel Ricaud
UTeid: dr25237
Csid: dr25237

Thequestionsmarkedwitha dagger(†) requireexternalresearch and maybemore 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?

So that another sender cant authenticate itself.

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

For an extra layer of encryption.

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

That M actually came from S.

Lecture 54

1. What is the importance of certificate authorities?

They provide certificates and verify users identities.

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

That way Y can sign that hash X created to reply in a way that X knows Y is replying to the same message X sent.

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

Because X's certificate contains the hashed Y certificate

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

It could act like it was X.

Lecture 55

An identity is given a certificate, this certificate is then added to any child certificates that originate from it.

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

So that the key can eventually expire and be refreshed with a new secure one.

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

That the message was insecure.

Lecture 56

1. What are some protocols previously discussed?

Biba’s Strict Integrity, Chinese Wall, Bell and LaPadula

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

Security could be compromised.

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

So that you can reach in the outer encryption to undo your inner encryption.

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

If he takes the first 3 messages then he has all the information necessary to try and XOR the information out of the message.

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

Once the attacker has M and the original encrypted message, he has 2 of the 3 parts so he can easily find Ka, what was used to turn M into the encrypted M

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

The same way he got Ka, once he has M he can take the excrypted M sent from B.

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

They are complicated and it’s difficult to cover every covert channel.

Lecture 57

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

transaction is made online.

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

It’s important to be able to privately send information through the internet due in part to the last question and the amount of transactions that occur.

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

That the system is unsecure so messages need encrypting.

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

To send secure encrypted messages between A and B

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

Yes, each person A and B can send hashed messaged to the other.

5. How is the protocol in slide 6 flawed?

An attacker could intercept both messages and decrypt it.

Lecture 58

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

Each unnecessary step is another chance for a security leak.

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

Because it is redundant and probably includes other unnecessary steps that could lead to a security risk.

Lecture 59

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

There are many different definitions of what constitutes an attack and many facets of security that need to be covered to prevent all attacks.

2. Describe potential dangers of a replay attack.

The attacker could reply and make it look like an authenticated reply.

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

Yes, there could be an attack in which the attacker only manipulates

Designers should assume that an attacker can intercept all traffic.

5. Why is it important that protocols are asynchronous?

It keeps everything that the initiator is doing more hidden from the parties.

Lecture 60

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

No because there is no public key data structure.

CS361 Questions: Week 4

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

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?

Because it is at the beginning of the protocol chain.

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

Yes

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

Do a one time pad so they wouldn't worry about the key being broken.

Lecture 62

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

Encrypted hashed messages.

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

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

Use an asynchronous protocol

Lecture 63

1. Why is the verification of protocols important?

2. What is a belief logic?

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

Lecture 64

1. What is a modal logic?

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?

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.