CS361 Questions: Week 4

These questions relate to Modules 12, 13 and 14. Type your answers and submit them on Canvas.

Lecture 53

1. Why is it important for a digital signature to be non reusable?
2. Why is it the hash of the message typically signed, rather than the message itself?
3. What assurance does R gain from the interchange on slide 4?

Lecture 54

1. What is the importance of certificate authorities?
2. In the example on slide 5, why does X sign the hash of the first message with its private key?
3. Why is it necessary to have a hash of Y and $K_y$?
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?
2. Why does an X.509 certificate include a “validity interval”?
3. What would it mean if the hash and the received value did not match?

Lecture 56

1. What are some protocols previously discussed?
2. What may happen if one step of a protocol is ignored?
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.
5. Describe how an attacker can extract $K_a$ from the protocol in slide 6.
6. Describe how an attacker can extract $K_b$ from the protocol in slide 6.
7. Why are cryptographic protocols difficult to design and easy to get wrong?

Lecture 57

1. Explain the importance of protocols in the context of the internet.
2. Explain the importance of cryptographic protocols in the context of the internet.
3. What are the assumptions of the protocol in slide 6?
4. What are the goals of the protocol in slide 6?
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?
2. Why is it important to know if a protocol encrypts items that could be sent in the clear?

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.
3. Are there attacks where an attacker gains no secret information? Explain.
4. What restrictions are imposed on the attacker?
5. Why is it important that protocols are asynchronous?

Lecture 60

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

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

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?

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.