Brittany Kvanvig bmk447

Questions Week 4

Lecture 53

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

   The signature can't be able to be attached to something else besides the specified document. You can't take the signature off the intended message and forge it onto something else

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

   For authentication reasons

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

   The message is secure and authentically sent from S.

Lecture 54

1. What is the importance of certificate authorities?

   Letter of introduction

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

   X is the certifying authority. X is vouching for Y and Ky.

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

   Because X is the certifying authority and this certifies the binding of Y and Ky

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

   You wouldn't have a hash of X

Lecture 55

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

It holds all the chains and is an unimpeachable authority.

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

This exists so the user knows if the certificate is still valid.

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

The certificate has been interfered with in some way.

Lecture 56

1. What are some protocols previously discussed?

AES, http

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

The message may be intercepted or modified.

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

They both need the same key

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

An eavesdropper who stores the three messages can XOR combinations of them to extract any of M, Ka, and Kb

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

An eavesdropper who stores the three messages can XOR combinations of them to extract any of M, Ka, and Kb

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

An eavesdropper who stores the three messages can XOR combinations of them to extract any of M, Ka, and Kb

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

Because there are ways to extract information that is subtle and unable to be detected by the sender/receiver

Lecture 57

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

Almost everything that occurs on the internet occurs via a protocol

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

Secure transferring of data so no one can eavesdrop or change information.

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

A can open the message from B by using A's secret key. B can open the message by using B's secret key. They've authenticated themselves.

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

Verification

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

No they are not because Kb and Ka are public and anyone can use them.

6. How is the protocol in slide 6 flawed?

Same as above: can be subtly intercepted and decoded.

Lecture 58

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

If a step is unnecessary there are more possible points of penetration of the protocol, when they aren't necessary.

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

It would give information of the encryption algorithm if the clear message is ever found out.

Lecture 59

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

Because many attacks are subtle and many different types of attacks that make use of many different aspects of the protocol

2. Describe potential dangers of a replay attack.

The attack could be used to crack the protocol and you wouldn't know how long your information has been intercepted.

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

    Yes, because an attack can impersonate someone to add information without the authorization. The attacker doesn't gain any information but they add what should be unauthorized messages to the protocol

4. What restrictions are imposed on the attacker?

    They can't send arbitrary messages. They have to follow the protocol in some ways

5. Why is it important that protocols are asynchronous?

    So the attackers can't see where in the protocol a message is and synchronize the attack.

Lecture 60

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

No, because then there would be no way of knowing if a message is fresh and secure.

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

    1. A is telling S that they want to send a nonce to B

        S knows to create a unique key

    2. S sends A a nonce for a and b secured with keys

        A knows they have a shared secure key

    3. A sends B their shared key secured with B's key

        B knows A wants to send him a message

    4. B sends A his nonce secured with their shared key

        A knows B got his shared key

    5. A sends B nonce-1 with their shared key

        B knows A got his 1st message

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?

   Yes, because B wouldn't know A's key has changed.

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?

   Attempt to minimize the flaws.

Lecture 62

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

   Give them both a secure key and a way to safely send a message without being intercepted

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

   Otway-Rees does not guarantee they both have knowledge of the key.

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

   If A & B had a secret key instead of public and private keys

Lecture 63

1. Why is the verification of protocols important?

   To see if a protocol is "correct" or secure

2. What is a belief logic?

   Allow reasoning about what principals within the protocol should be able to infer from the messages they see.

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

   Beliefs play a role in the security of the protocol by what A believes about B,

the protocol or any combination of the three.

Lecture 64

1. What is a modal logic?

Logic that allows speakers to attach belief to a statement.

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

If A thinks they share a key with only B, and A sees {X}k, then he can assume only B could have sent that message.

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

If A thinks X is fresh and A thinks B said X, then A must think that A also believes X.

4. Explain the intuition behind the jurisdiction inference rule.

A is trusting B's judgment on verifying X.

5. What is idealization and why is it needed?

It simplifies a protocol to just the beliefs of the participants.

Lecture 65

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

Because any plaintext can be forged.

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

Because the other protocols don't deal with beliefs, they need the idealized steps to try to verify the beliefs.

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

It exposes places where logic could get in the way of noticing a potential flaw in the protocol. If we assume only A and B have knowledge of K, we never take into consideration the case where someone has wrongfully gained knowledge of K maliciously.