NAME: Aaron Dishman
UTID: adishman
CSTURNIN: adishman
EMAIL: aaron.dishman@utexas.edu

CS361 Questions: Week 4

The questions marked with a dagger (†) require external research and may be more 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 a signature can not be stripped off and attached to another "document"

2. Why is it the hash of the message typically signed, rather than the message itself?
   For efficiency of computation. Public key encryption is expensive to apply, and message may be long, but hash is a fixed, finite, short value.

3. What assurance does R gain from the interchange on slide 4?
   That the message is from S and only R can read it

Lecture 54

1. What is the importance of certificate authorities?
   Trusted source that vouches for the binding between an identity and public key.

2. In the example on slide 5, why does X sign the hash of the first message with its private key?
   So that Y knows that this hash function came from X

3. Why is it necessary to have a hash of Y and $\mathbf{K}_y$?
   because if you check it against an actual hashing of the original values and the result is the same, you can reasonably assume that those values weren't messed with.

4. What would happen if Z had a public key for X, but it was not trustworthy?
   couldn't trust that y and y's public key have an association

Lecture 55

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

2. Why does an X.509 certificate include a "validity interval"?
   because certificates can become invalid over time, so an expired certificate should not be trusted

3. What would it mean if the hash and the received value did not match?
   it would mean that somewhere along the line, the values were changed, possibly maliciously

Lecture 56

1. What are some protocols previously discussed?
   Diffie-Hellman exchange, AES

2. What may happen if one step of a protocol is ignored?
   an eavesdropper could break the encryption

3. Why must the ciphers commute in order to accomplish the task in slide 4?
   so that the “locks” can be “unlocked” at the end of the exchange by the receiver

4. Describe how an attacker can extract M from the protocol in slide 6.
   could keep a copy of all the messages passed, use the commutative property of xor to remove all “locks” and extract M

5. Describe how an attacker can extract K_a from the protocol in slide 6.
   xor the first message with the last message, eliminating the Ka from first message

6. Describe how an attacker can extract K_b from the protocol in slide 6.
   xor first message with the last message to strip Ka from last message.
   xor second message with new third message

7. Why are cryptographic protocols difficult to design and easy to get wrong?
   because they have many subtleties that can expose weaknesses

Lecture 57

1. Explain the importance of protocols in the context of the internet.
   because a protocol is a structured dialogue among two or more parties in a distributed context (like the internet) controlling the syntax,semantics, and synchronization of communication, and designed to accomplish a communication-related function

2. Explain the importance of cryptographic protocols in the context of the internet.
   cryptographic protocols add security related functions to communications

3. What are the assumptions of the protocol in slide 6?
   only a and b know their respective private keys

4. What are the goals of the protocol in slide 6?
   confidentiality, authenticity, unicity

5. Are the goals of the protocol in slide 6 satisfied? Explain.
not all of them, the reason why explained in question 6

6. How is the protocol in slide 6 flawed?
because an interceptor (Eve) could send a message to B signed with Eve's private key internally, and B's public key externally ({{M}ke-1}kb), prompting B to respond with a message signed with B's private key internally, and Eve's public key externally ({{M}kb-1}ke). Then Eve could strip of it's own encryption, and now contains copies of both B's public and private keys, allowing Eve access any of B's encrypted messages.

Lecture 58

1. Why is it important to know if a protocol includes unnecessary steps or messages?
because unnecessary steps or messages should be eliminated from the protocol

2. Why is it important to know if a protocol encrypts items that could be sent in the clear?
because if they could be sent in the clear, they are unnecessary, therefore, should not be included

Lecture 59

1. Why might it be difficult to answer what constitutes an attack on a cryptographic protocol?
because you might not see the consequences of an attack, you might not know if authenticity and secrecy is assured, possibly because of a man in the middle attack.

2. Describe potential dangers of a replay attack.
if a previously sent message was recorded, and sent again at a later time, it might be used to crack the encryption key of a message.

3. Are there attacks where an attacker gains no secret information? Explain.
a replay attack might not lead to a cracked encryption, but still confuse or disrupt the communication flow between the communicating parties

4. What restrictions are imposed on the attacker?
we assume the attacker can't generate a message encrypted with a key it doesn't have. hard to specify exactly what those constraints are.

5. Why is it important that protocols are asynchronous?
because it shouldn't matter at what time events that break protocols happen the protocol should hold at any given time

Lecture 60

1. Would the Needham-Schroeder protocol work without nonces?
    maybe if you added a timestamp

2. For each step of the NS protocol, answer the two questions on slide 5.\
question 1:
    1) hey trusted source S, sender A wants to establish a secure connection with B
    2) hey A, here is a new key for you and B to use to communicate securely
    3) hey B, here is a new key we can use to communicate securely,
    4) hey A, here is a nonce encrypted with our new key
    5) hey B, I received your nonce

question 2:
    1) A wants to establish a secure connection with B, and this is a “fresh” message because of the Nonce of A
    2) A can believe that this message came from sender, and it’s fresh because it contains A’s nonce
    3) B can believe that this is a secure key sent from S to A, because it is encrypted with the key that S and B share, and it contains a key. It doesn’t know how fresh it is, though, because it doesn’t contain a nonce
    4) this nonce came from B
    5) A has received my nonce, because I got a message back with my nonce changed

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?
    if someone didn’t pay attention to the expiration of the old key

2. Is it fair to ask the question of a key being broken?
    not really, because it might be possible for someone to impersonate A from the beginning

3. How might you address these flaws if you were the protocol designer?
    add a nonce to step 3

Lecture 62

1. What guarantees does Otway-Rees seem to provide to A and B?
    that they each share a key to securely communicate

2. Are there guarantees that Needham-Schroeder provides that Otway-Rees

does not or vice versa?

At the end, NS seems to guarantee to each party that they each received the message/key

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

adding a time stamp or nonce

Lecture 63

1. Why is the verification of protocols important?

because an incorrect protocol can have subtle incorrectness that go unnoticed for a long time and be exploited by many people

2. What is a belief logic?

A belief logic is a formal system for reasoning about beliefs. Any logic consists of a set of logical operators and rules of inference.

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

in this context, “beliefs” just refers to what a node can reasonably infer from some transaction

Lecture 64

1. What is a modal logic?

a set of primitives for describing logic, and a set of inference rules for inferring new facts from previous exchanges

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

If A believes A and B share a key K, and A sees a message encrypted with K then A can reasonably believe B said X.

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

If A believes that a message(or statement of belief), X, is fresh, and A believes B once said X, then A can reasonably believe that B believes X.

4. Explain the intuition behind the jurisdiction inference rule.

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

5. What is idealization and why is it needed?

This attempts to turn the message sent into its intended semantics. To get from protocol steps to logical inferences.

Lecture 65

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

because it is inconsequential to the logic

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

in order to streamline the protocol and what it is trying to say

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

because some assumptions can lead to exploitable vulnerabilities.