Name: Vincent Nguy

EID: vn2863

CS Login: vn2863

Email:nguyvincent@yahoo.com

# 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?

If someone somehow is able to get my signature they could use it to send messages as me.

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

If a hash was change the original message would be incorrect so signing the hash is safer

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

That only S has the private key to the message

# Lecture 54

1. What is the importance of certificate authorities?

It’s a third party trusted by both the sender and receiver who manages their “trust” relationship.

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

In case the message might get intercepted and changed a hash of it would retain the original message.

1. Why is it necessary to have a hash of Y and *Ky*?

It certifies the binding of Y and Ky

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

If X assumes he’s trustworthy he could still send and receive messages from X

# Lecture 55

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

It stores information on users who are certified

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

To check for attackers trying to access your id at a time.

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

The certificate signed is different from the original.

# Lecture 56

1. What are some protocols previously discussed?

Exclusive or (XOR) your message with a randomly generated string (key) of the same length

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

It no longer works.

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

The locks prevents eavesdroppers from getting ahold of the content but must commute so the locks could open in any order.

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

Since Ka will be XOR twice it cancels out and a attacker can get ahold of Kb that’s all they need to get M.

1. Describe how an attacker can extract *Ka* from the protocol in slide 6.

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

**CS361 Questions: Week 4** 2

1. Describle how an attacker can extract *Kb* from the protocol in slide 6.

If attacker has Ka he could use extract Kb.

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

Many thing to defend against and if you mess up any step of the protocol it could become useless.

# 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.

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

It helps protect the user from eavesdroppers from being able to access the contents of your message.

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

Two parties want to establish a way of communication safely and are operating under a hostile environment.

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

Key agreement or establishment, Entity authentication, Symmetric encryption and message authentication.

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

Yes. With both steps it verifies the message was received.

1. How is the protocol in slide 6 flawed?

A attack can use this whole protocol as his message and extract the original message.

# Lecture 58

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

Because in a distributed setting. It is necessary to follow the protocol in step order so its important to know all steps.

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

If you want to apply your items you need to know if it’s been encrypted or not or you might be operating on a wrong value.

# Lecture 59

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

Because it could be your protocol is not assuring authentication and secrecy.

1. Describe potential dangers of a replay.

Is it possible to interject messages from an earlier exchange. A attacker can use ealier messages to verify them as a Receiver to me or use my identity to send new messages posing as me.

1. attack.
2. Are there attacks where an attacker gains no secret information? Explain.

**Known-key attack:**

attacker gains some keys used previously and then uses this info to attack the protocol and possibly determine new keys.

**Replay:**

attacker records a communication session and replays some or all of it at a later time.

**Impersonation:**

attacker assumes the identity of one of the legitimate parties in a network.

**Man-in-the-Middle:**

attacker interposes himself between two parties and pretends to each to be the other.

**Interleaving attack:**

attacker injects spurious messages into a protocol run to disrupt or subvert it.

1. What restrictions are imposed on the attacker?

Possibly a one-time use protocol. Some way of authenticating a sender and receiver.

1. Why is it important that protocols are asynchronous?

Because of the distributed nature of a system.

# Lecture 60

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

No it keeps track of how “fresh” the message is.

1. For each step of the NS protocol, answer the two questions on slide 5.
2. *A*→S:*A*,*B*,*Na*

*A says to S here is a new Nonce and I want to communicate with B*

*S knows A wants to communicate with B.*

1. *S*→A:{*Na*,*B*,*Kab*,{*Kab*,*A*}*Kbs*}*Kas*

*S responds to A and generates a new key and sends it back to A with a key for Kbs and Kas.*

*A now has something he could send to B.*

1. *A*→B:{*Kab*,*A*}*Kbs*

A now sends to B: A’s identity and the new key between A&B encrpyed with Kbs

B now knows someone wants to communicate with him. And the sender used S.

1. *B*→A{*Nb*}*Kab*

*B sends the Nouce back to A telling A he recived it*

*A receives the Nouce back and verifies he sent it.*

1. *A*→B{*Nb*−1}*Kab*

*A sends (Nouce-1) back to B telling him it’s the same on his end.*

*B verifies it and its complete.*

# Lecture 61

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

I don’t think so if Kas is later changed the attacker can’t impersonate A with Kas.

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

Depending if the protocol implements a strong or weak tranquility property.

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

Maybe have some process where A can revalidate his identity.

# Lecture 62

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

A person can verify another person using S.

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

Yes. Otway-Rees doesn’t verify if a person has received the correct message.

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

Maybe combine aspects with Needham-Schroeder with Otway.

# Lecture 63

1. Why is the verification of protocols important?

Protocols can be notoriously difficult to get correct. Flaws have been discovered in protocols published many years before. It would be nice to able to reason formally about protocol correctness.

1. 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.

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

As variables read into the program.

# Lecture 64

1. What is a modal logic?

It is formal logic to include modal operators.

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

A shares a key with B so they can communicate. If A can see {X}k then B would have sent it for A to see.

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

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

1. Explain the intuition behind the jurisdiction inference rule.

If A believes B has jurisdiction over X and A believes B believes X. then A believes X.

1. What is idealization and why is it needed?

Turning the message sent into its intended semantics. So we can have a more formal equation. And omit unnecessary parts

# Lecture 65

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

It does not contribute to the “beliefs” of the recipients.

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

If this step is true the belief that is being refered is also true in the future step.

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

You can easily disprove assumptions that are incorrect.