Name (UTEID): Mingu Chang (mc35926)
CS Login: mchang
Email: mc-kpmg@hotmail.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?

 because the signature is part of the check, so cannot be easily removed and re-used; the signature cannot be detached and reused for another message

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

 the public key encryption is expensive to apply and message maybe arbitrarily long, but the hash is going to be finite short value.

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

 gain the same assurance that we wanted on the previous slide.

Lecture 54

1. What is the importance of certificate authorities?

 A public key and a user's identity are bound together within a certificate, signed by a certification authority, vouching for the accuracy of the bingind.

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

 so that the last can becomes Y's certificate

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

 The message certifies the binding of Y and Ky. X is the cerifying authority. Data items Y and Ky were not altered or corrupted.

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

 Z has a trustworthy public key for X, to verify X's signature. Data items might get altered or corrupted.

Lecture 55

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

 Certificates can be combined to produce a chain of trust.

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

 Validity interval: start and end times for validity.

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

 We would not be able to validate the certificate.

Lecture 56

1. What are some protocols previously discussed?

 put the item into the box, attach your lock to the hasp, and mail the box to Ivan; Ivan adds his own lock and mails the box back to you.; You remove your

Name (UTEID): Mingu Chang (mc35926)
CS Login: mchang
Email: mc-kpmg@hotmail.com

lock and mail the box back to him. He now removes his lock and opens the box.

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

 Then One cannot send some content confidentially in the context of a hostile or untrustworthy environment, when the two parties do not already share a secret/key

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

 You would have to be able to "reach inside" his encryption to undo yours(your lock).

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

 An evesdropper who stores the three messages can XOR combinations of them to extract M

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

An evesdropper who stores the three messages can XOR combinations of them to extract M

Name (UTEID): Mingu Chang (mc35926)
CS Login: mchang
Email: mc-kpmg@hotmail.com

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

 An evesdropper who stores the three messages can XOR combinations of them to extract M. Anytime you see a value being extraordinary if you see it twice than it cancels out.

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

 because one can possibly extract code from protocol.

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. A protocol is a structured dialogue among two or more parties in a distributed context 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 use cryptography to accomplish security-related functions. Unicity, Integrity, Authenticity, Confidentiality, non-repudiation of origin, Non-repudiation of receipt.

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

 there is a public key infrastructure in place and each of them has a reliable version and the others public key.

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

 Does each party at the end of the day know that the other party has the key and can use it.

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

 yes.

6. How is the protocol in slide 6 flawed?

 Could not get it. Bill Young has mentioned that he will unveil later few lectures hands.

Lecture 58

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

 could the protocol have been designed in a more parsimonious way that is did it do things that it did not need to do.

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

 could have left out some of the message exchanges and still accomplish the same goals

Lecture 59

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

Name (UTEID): Mingu Chang (mc35926)
CS Login: mchang
Email: mc-kpmg@hotmail.com

 some protocols have been in use for years before someone noted a significant vulnerability.

2. Describe potential dangers of a replay attack.

 attacker records messages and replays them at a later time.

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

no because for example if the attackers were able to generate an arbitrary message then there would not really be any defense.

4. What restrictions are imposed on the attacker?

 hard to specify exactly what those constraints are.

5. Why is it important that protocols are asynchronous?

 A party to a protocol won't know anything about the current run of the protocol except the messages it has received and sent. Except for the initiator, other parties will not even know that they are participating until they receive their first message.

Lecture 60

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

 It still may work. Note that a nonce is not a timestamp. Nonce doesn't show that the messages is current that is recent.

Name (UTEID): Mingu Chang (mc35926)
CS Login: mchang
Email: mc-kpmg@hotmail.com

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

 A sends a message containing three components A,B, and Na. Trying to send message from A to B.

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 the way that S knows that message is actually coming from A is by the fact that they share a secret key.
2. Is it fair to ask the question of a key being broken?
   answer maybe yes or no, depending upon the strength of the encryption
3. How might you address these flaws if you were the protocol de signer?
   come up with something better design that key cannot be broken.

Lecture 62

1. What guarantees does Otway-Rees seem to provide to A and B?
   A has K'ab while B has Kab.
2. Are there guarantees that Needham-Schroeder provides that Otway-Rees does not or vice versa?
   Yes.
3. How could you fix the flawed protocol from slide 4?
   make a key so that C cannot see the messages.

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 be able to reason formally about protocol correctness.

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?

 One trick is taking a sequence of message exchanges and generating a collection of belief statements. You have to postulate some reasonable initial assumptions about the state of knowledge/belief of the principals.

Lecture 64

1. What is a modal logic?
   The BAN (Burrows, Abadi, and Needham) logic is a modal logic of belief.

Name (UTEID): Mingu Chang (mc35926)
CS Login: mchang
Email: mc-kpmg@hotmail.com

2. Explain the intuition behind the message meaning inference rule.
   - If A believes (A share(K) B) and A sees {X}k then A believes (B said X).
3. 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.
4. 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.
5. What is idealization and why is it needed?
   - To get from protocol steps to logical inferences, we have a process called idealization. This attempts to turn the message sent into its intended semantics.
   - One purpose of idealization is to omit parts of the message that do not contribute to the beliefs of the recipients

Lecture 65

1. Why do you think plaintext is omitted in a BAN idealization?
   - omitted since all components are plaintext. Idealization says taking a look at each step in the protocol and figuring out what that step is trying to say in terms of beliefs (believes). Plaintext is simple that no terms of belief required.
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.
   - The proof exhibits some assumptions that were not apparent. Use of logic like BAN shows what is provable and also what must be assumed.