CS361 Questions: Week 4

Name: Tyler Kemme
UTEID: tpk266
CS ID: tpkemme

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 the digital signature is reusable then it can possibly be reused by someone in an action that was not authorized on another document.

2. Why is it the hash of the message typically signed, rather than the message itself?
The hash of the message is signed because the hash is a fixed value that's easy to compute.

3. What assurance does R gain from the interchange on slide 4?
The message is unforgeable, authentic, has non repudation, tamperproof, and is non reausable.

Lecture 54

1. What is the importance of certificate authorities?
Certificate authorities are responsible for binding a public key with an entity. Therefore it is important that they are secure so that public keys are always correctly assigned to one, unique entity.

2. In the example on slide 5, why does X sign the hash of the first message with its private key?
Because then only X, the authority, can decrypt the hash with it's private key.

3. Why is it necessary to have a hash of Y and Ky ?
The hash of Y and Ky are produced when Y sends them to X. When X hashes the identity and public key, it creates a hash value that can only be produced with that original Y and Ky. Thus ensuring that the original Y and Ky are not tampered with.

4. What would happen if Z had a public key for X, but it was not trustworthy?
If another entity claiming to be X(i.e. W) gave Z a public key (Kw) then it could sign the hash with it's private key and send certificates as X.

Lecture 55

1. What happens at the root of a chain of trust?
At the root is some central authority that is generally trusted to create reliable certificates.

2. Why does an X.509 certificate include a "validity interval"?
Certificates are only valid for a certain amount of time to ensure that the certificate cannot be used of faked past the validity interval.

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

If the hash and the received value did not match, then the received value must have been modified in some way from the original source.

Lecture 56

1. What are some protocols previously discussed?

Symmetric encryption, asymmetric encryption, access control methods, etc.

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

If one step of the protocol is ignored, then the protocol itself is useless.

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

The ciphers need to commute so that you can decrypt the sender's encryption to get to your encrypted value.

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

If you XOR message 1 and message 2, the attack now has Kb. If the attack XORs Kb with message 3 then the attack obtains M.

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

If the attacker XORs message 3, which is essentially (M XOR Kb) with message 2, then M and Kb 'cancel out' and produce Ka.

CS361 Questions: Week 4.2

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

If the attack XORs message 1 and 2 it obtains Kb.

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

Cryptographic protocols are hard to design because the designer has to create a system that is secure from every attack, and attackers only need to find one way to compromise a system.

Lecture 57

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

Protocols are important in the context of the internet because it is the only way of ensuring that you are actually communicating with the person you think you're communicating with and that the data they send you is unmodified.

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

Unicity: passwords used on websites should only be known by the user and the owner (to a degree obviously)

Integrity: emails sent through the web are not modified on their way to the receiver

Authenticity: The emails you receive actually came from the person in the “sender” field.

Confidentiality: No one has the ability to access the contents of your message as they travel to

the receiver.

Non-repudiation of origin: the sender of the email cannot say he did not send it.

Non-repudiation of receipt: the receiver cannot say that he did not receive the message.

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

The assumptions are that the public key infrastructure in place is completely secure so that A and B have valid private and public keys.

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

The goals of the protocol are to ensure that B knows that the message it received is from A and that A knows the message it sent was received by B.

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

No the attacker can extract the original message.

6. How is the protocol in slide 6 flawed?

The attacker can send an earlier message sent in the protocol to B and B will essentially send the attacker the original message in plaintext.

Lecture 58

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

If the protocol includes unnecessary steps, then these steps cause extra computational steps which takes more time for no added security.

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

If the protocol encrypts items that could have been sent unencrypted, it is using extra computational energy to encrypt something that doesn't need it.

Lecture 59

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

An attack can be a deliberate misuse of the system but it doesn't have to be deliberate. An attack can be caused by faulty implementation of security protocols. Attackers can also use any tool and attack any part of a system to misuse or steal from the system.

2. Describe potential dangers of a replay attack.

If a protocol only used XORs, an attacker could replay an early message and cause the protocol to give out confidential information.

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

Yes. In an interleaving attack, the attacker might not gain any information, but it could disrupt the flow of information between the sender and receiver.

4. What restrictions are imposed on the attacker?

We assumed that the attacker cannot create arbitrary messages because we assume that they do not have access to certain private values such as private keys.

5. Why is it important that protocols are asynchronous?

It is important that the protocol is asynchronous because then the sender and receiver both only know information they create and they are not aware that the protocol is being implemented until after they receive verification.

Lecture 60

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

Without nonces, A would not be able to tell if the message is a replay of an earlier message in the protocol.

CS361 Questions: Week 4 3

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

1. The sender is saying to S that it is A trying tocommunicate with B with a nonce for security. S is entitled to believe that A is in fact A.
2. The sender is conveying that only A and B can decrypt this information. The receiver A is entitled to believe that this message is from S because it contains the nonce from part 1.
3. The sender, A, is conveying to B that it is A and that it has been verified by S. B is entited to believe that A has been verified by S and that Kab is a valid key.
4. B is saying to A that it is in fact B because it could decrypt A's previous message with B's private key from S. B also says to A that it would like to prove it is talking to A by sending a nonce encrypted with the shared key Kab. A assumes that only B sent this message because only B would have the key Kbs
5.A is saying to B that it has the key and can use it by subtracting one from the nonce, which is only possible by decrypting the nonce. B is entitled to believe that this is from A because only somone with the shared key could alter the nonce in such a way.

Lecture 61

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

A could still be impersonated by decrypting old messages and learning B's identity and a possible fresh shared key Kab.

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

It is fair to ask the question of a key being broken because if a key ever was compromised, there would need to be some sort of implementation for reacting to the compromised key and creating a new key.

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

One way to fix these flaws would be to periodically create new keys Ka, Kb, Kab, Kbs, and Kas all at the same time.

Lecture 62

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

We guarantee for B that it is receiving a message from A and we guarantee for A that B got the message.

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

You could add a unique nonce for the “session” of communication and then C wouldn't be able to use the same message.

Lecture 63

1. Why is the verification of protocols important?

It is very difficult to discover flaws in protocols which makes it difficult to decide if the protocol is actually secure.

2. What is a belief logic?

Belief logic is reasoning about what the parties in a communication flow are entitled to believe after sending or receiving data.

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

Beliefs in programs come in the form of observing values and then deciding whether they are valid or not.

Lecture 64

1. What is a modal logic?

A modal logic is a type of logic that has predicates that perform actions on each other or objects in accordance to some inference rules.

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

Basically, if A believes that it shares a secret key with B and then receives a message with said shared key, A assumes the message came from B. This is because only B could have sent a message with the key that is only known by A and B.

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

If A believes it's receiving a message from B and that the nonce is fresh, then A believes that B believes in the correctness of the nonce. If the nonce is fresh and A knows it's talking to B, then B must have created this nonce.

4. Explain the intuition behind the jurisdiction inference rule.

If A believes that B has jurisdiction over the creation of X and A believes that B believes that it created X, then A trusts or believes in X. Basically, If A trusts B with the creation of X and B believes it created X, then A believes X is valid.

5. What is idealization and why is it needed?

Idealization helps the designer realize exactly what the protocol step is trying to accomplish. Idealization helps translate from the protocol implementation to belief logic.

Lecture 65

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

Plaintext does not specify any belief logic because it is not secure in any way.

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

Steps such as authorization require multiple steps to ensure validity.

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

Belief logic shows every assumption throughout the protocol and sometimes you can find assumptions that should not be assumptions at all.