Adan Cortez

AC42886

Lecture 53

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

The signature should be bound to the document and not be able to be used in another context that the signer didn't authenticate.

2. Why is the hash of the message typically signed?

The hash is fixed and finite while the message can be arbitrarily long and public key cryptography is expensive to apply the longer the message is.

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

R can be assured that the message is unforgettable, authentic, tamperproof and the message has a signature that is non-reusable and cannot be repudiated.

Lecture 54

1. What is the importance of certificate authorities?

They assure a user that a certain party can be trusted if the user and the party have never communicated before. The certificate authorities are able to sign a party's public key and vouch that the key does in fact belong to the party.

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

With its private key?

X signing the hash shows that X is the certifying authority and vouches for Y with the hash showing that her public key is valid.

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

The hash is to ensure that the values Y and Ky weren't changed or corrupted.

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

If the public key were not trustworthy then the scheme would have an invalid certificate, as the hash could not be decrypted.

Lecture 55

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

The trust should be unimpeachable at the root of the chain.

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

The validity interval gives a start and end time for the validity of the digital signature. If the signature is not within the time frame, then it is not to be trusted.

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

If the hash and received value do not match, then that means the public key that was sent was not the one that was certified by a trusted authority. Therefore the key should not be used.

Lecture 56

1. What are some protocols previously discussed?

Public key cryptography (asymmetric), RSA and Diffie Hellman symmetric key exchange.

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

The message can be mangled or unsecure to eavesdroppers if any steps are left out.

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

If the ciphers cannot commute, then in order to remove an internal encryption, the any external encryptions must be removed first. It must be able to commute and be able to decrypt any layer at any given time regardless of the order the encryptions were placed.

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

If the attacker has eavesdropped on all 3 messages, then he can obtain Kb by XORing the first and second messages together and then XOR Kb to the third message to receive M.

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

The attacker can obtain Ka by XORing the second and third messages.

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

The attacker can obtain Kb by XORing the first and second messages.

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

Like most forms of defense systems, it is very hard to design a protocol that is able to defend against all attackers. A defense is only as strong as the weakest link and to account for all links is hard and for an attacker to find the weakest link is easy.

Lecture 57

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

A protocol is a structured dialogue among two or more parties designed to accomplish a communication-related function. In the context of Internet, the rapid spread of information would not be possible without a number of set protocols in order to allow computers within a network to communicate with other computers through the Internet.

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

A cryptographic protocol is using cryptographic mechanisms to accomplish some security-related function. In the context of the Internet, cryptographic protocols are a necessity to hide and defend information from prying eyes. Secure and confidential information would not be possible without cryptographic protocols.

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

The protocol assumes there is a public key crypto system in place and each of them has a reliable version of the other's public key.

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

To be able to share a secret object while authenticating both sides of the protocol and to ensure that both sides of the party know that the other side has the secret object and are able to use it.

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

In a simpler sense, it is satisfied, as both parties know the other is authenticated, has the secret key shared and knows the other party received the message. When introducing attackers into the protocol, it may not necessarily fulfill the goal that both parties know that the other party received the message.

6. How is the protocol in slide 6 flawed?

In order to verify that the message was received, the receiver sends a message back to the sender. But how does the receiver know that the sender received the message. The sender, now receiver, could send a message back. But how does the receiver know the sender got that message, and so on and so forth. So in order to fully verify without doubt, both parties send verification endlessly.

Lecture 58

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

Between multiple parties within a protocol for communication, not all parties start at step one. It becomes important to know for parties joining the protocol to know what steps are unnecessary and what step to start responding at.

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

Encrypting unnecessarily creates undue work within the protocol. Excessive encrypting may also give an attacker more chances to leverage information against the protocol.

Lecture 59

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

If the attacks on the protocol were known, then the design of the protocol would be designed to prevent those attacks.

2. Describe potential dangers of a replay attack.

A replay attack can cause confusion between two people communicating if the attacker is able to record previous messages and insert them into a conversation between the two.

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

Potentially, replay and interleaving attacks can cause confusion but not necessarily disclose information.

4. What restrictions are imposed on the attacker?

We assume the attacker can't generate a message encrypted with a key that it doesn't have unless the message was a record from before.

5. Why is it important that protocols are asynchronous?

The other members of the party other than the initiator won't know they are participating in the protocol until they receive their first message.

Lecture 60

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

No, without the last step of the nonce being decrypted, it is not possible to know that both parties of the key is ready to communicate with each other.

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

For step one, A is telling S that it wants to communicate with B and asking for a key to talk with B and sends a nonce to S. The receiver sees that A wants to communicate with B. For step two, S returns to A a package locked with A's key so that only he can unlock it. The nonce is returned to tell the package is fresh and also includes a key that he can communicate to B with. For step 3, A sends B the key that he got from S telling B that he wants to communicate. B sees this and realizes that he is in step 3 of the protocol to communicate and knows the key came from S. For step 4, B sends a nonce using the key he just got to let A know that he got the key and can use it. A now knows that B has the key ready to use. For step 5, A returns the nonce he got and decrements it before sending it back to B to let B know he got his nonce. B knows from this that both sides are ready to use the key and A was able to decrypt his nonce.

Lecture 61

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

The impersonator could still use the old key like normal to talk to anyone paired with the old decrypted key pairs. He just can’t decrypt new pair communication keys.

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

No, each protocol uses a key of some sort and generally speaking, the protocols are developed in mind with the attacker not having easy access to them or are able to break them other than brute force.

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

Unlike N-S, I would at least make a method to verify that a key is valid if it was broken. Perhaps hide the nonce that S returns and store it in the B locked key to send as well and have B ask S for the nonce used to construct that key.

Lecture 62

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

Both A and B know that the keys are fresh and not reused and that both sides of the party can be assured that they are talking to whom they think they are.

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

B doesn't know that A has the key or not while in N-S both parties know each has the key and is ready to use it. O-R knows that S authenticates both parties and the keys are fresh.

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

Take out the private key lock on the return message from B -> C. If the keys match, then that should be proof enough that both parties are who they claim to be.

Lecture 63

1. Why is the verification of protocols important?

The verification of protocols allow experts to reason formally about the correctness of the protocol as well as find issues with it.

2. What is belief logic?

Belief logic allows reasoning about what principals within the protocol should be able to infer from the message they see. This allows for abstract proofs.

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

Based on each step of the program, it's possible to make some reasonable assumptions about what each principal in the program should know.

Lecture 64

1. What is a modal logic?

Modal logic uses types of operators to express beliefs, attitude and obligations in relation to the statement at hand.

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

If the only two people in the world share the key between them and one person of that pair receives a message encrypted with that key, then intuitively, only the other person in the pair could have encrypted it.

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

If A thinks some message X is fresh, and B sent X, then A believes that B believes that X is fresh.

4. Explain the intuition behind the jurisdiction inference rule.

If A thinks that B is an expert on X and B believes in X, then A should believe in X. Meaning if you hear news from an expert on X who vouches for X, then you should believe in X.

5. What is idealization and why is it needed?

The purpose of idealization is to stare at a protocol and figure out what it is that the protocol is trying to achieve in terms of trying to make the receiver believe. It is needed to get from the state of sending the message to the state of the belief logic.

Lecture 65

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

Plaintext is omitted since all plaintext can be forged.

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

The idealized steps expose assumptions in each step which point to future steps in the protocol.

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

While it does prove the end goal of the protocol, it brings up certain assumptions that much be made for progress through each step of the protocol in order to verify it properly