Name: **Zhenyu Zhu**

Date: **6/28/2014**

EID: **cike**

CS login: **zhenyu**

Email: **zhu_zhenyu@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 not reusable?

   Because if a digital signature it is reusable on another document, then it is not unique for R when he received different message with same signature, it creates ambiguous reply to increase the uncertainty instead of reducing it. Also the other properties of the signature (unforgeable, no repudiation, tamperproof) all have been broken.

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

   Because public key encryption system is expensive to apply, and the message can be arbitrary long, but hash of the message is typically a fix finite short value.

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

   R gains unforgeable and no repudiation since only S can use his private key. R gains authentic since a third party can verify the signature with S's public key. R gains tamperproof since only R with his private key can remove the outer layer of encryption. Finally R gains not reusable since the signing is the encryption of the message itself, and it can't be separate the signature and the message.

Lecture 54

1. What is the importance of certificate authorities?

   It is the essential part to gain a web of trust between two suspicious entities. It vouches for the accuracy of the binding between a public key and a user's identity, so a third party can rely on certification to have a trust with the user.

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

   So a third party who has a trustworthy public key for X, can verify X's signature and gain a web of trust to whoever X's vouch for.

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

   To make sure that this signature has not being altered or corrupted, so a third party Z who has X's public key can recalculate hash value of the digital signature and compare with X's encrypted hash value to make sure that this certificate is valid.

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

   Then Z is not sure if this signature is really from X or not, and if X is not been verified, then Y can't be trusted since X is the root and the certifying authority for Y.

Lecture 55

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

   Root should be some unimpeachable authority agreed by everyone.

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

   It contains the information tells the third party that how long is this certificate valid for, so for example we shouldn't trust the certificate who has been expired.

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

   The subject's distinguished name and subject's public key info has been altered or corrupted.

Lecture 56

1. What are some protocols previously discussed?

   Covert Channel, Non-Interference, Key Exchange, Certificate.

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

   The goal of sending the content confidentially to others cannot be reached.

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

   One cipher has to be able to "reach inside" the other's encryption to undo its own encryption base on the protocol steps.

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

   XOR all three messages he eavesdropped.

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

   XOR the 2nd and 3rd messages he eavesdropped.

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

   XOR the 1st and 2nd messages he eavesdropped.

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

   Because a perfect cipher only exist theoretically, and cryptographic protocol involves communication channel, bandwidth, encryption method, receiving the message, have to preserve confidentiality, integrity and authenticity of the message, any one error in the above will make the overall goal to fail. It must be robust and reliable in the hostile and unsecure environment.

Lecture 57

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

   Because Internet is build on exchange of information among different hosts. Internet Protocol is the principle communications protocols to relay datagrams across network boundaries. It's routing function enable internetworking, and essentially establishes the Internet. (Wikipedia)

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

   Because some information is not public information and need to be send securely. Such goal can be achieved by a protocol using cryptographic mechanisms to accomplish some security-related function.

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

   There is a PKI (public key infrastructure) system in place and both A and B has reliable certificate to valid their identity with their public keys.

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

   Unicity, Integrity, Authenticity, Confidentiality, and Non-repudiation of sender and receiver.

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

   Unicity can be verifying if success perform step 1 and step 2. Integrity can be verified by comparing the key received with the key they send. Authenticity and Non-repudiation can be verified since only A or B knows its private key to create the message. Confidentiality is reached by A or B since they can only use its private key to decrypted the outer layer of encryption in step 1 and 2.

6. How is the protocol in slide 6 flawed?

   If C intercept message from step 1 and send this message result as K' to B in the same format as in step 1 in a new protocol, after B's reply to C, C can extra K.

Lecture 58

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

   Because it takes a lot involving making a protocol working, and we don't want to encrypt public information and don't want exchange extra information that can be skipped and still achieve the goal.

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

   Because encryption algorithm is slow and difficult to implement, if we encrypts item that could be sent in the clear, we are wasting resources that could be use to improve performance on other parts, and making the implementation of the protocol more difficult than it needs to be.

Lecture 59

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

   Because a good attack is an engineer never thought of. There are so many different types of attacks on protocol focus on different aspect of the protocol, and just as the principle of easiest penetration, it is difficult to pin down what the attacker will do and cover all the weak points.

2. Describe potential dangers of a replay attack.

   It can misinform the parties involved with the protocol with out of date information. For example, in a stock exchange, it could upload information couple days ago from a phish site, to mislead people who are trying to buy a stock. In a military attack mission, it could inject wrong attack time and cause the troops movement in chaos.

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

   Interleaving attack, where attacker injects spurious messages into a protocol run to disrupt or subvert it. In this attack, attacker gains no secret information, but it still can cause bad things to happen.

4. What restrictions are imposed on the attacker?

   That the message attacker trying to send/inject into the protocol has to be of a form that the send used and the content has to make sense to the subject, so the malicious message can be identify and respond to by the recipient. Otherwise it can be easily spotted as an attack, and won't be a successful attack.

5. Why is it important that protocols are asynchronous?

   If only the initiator knows when to send the message, it will be harder for the attacker to coordinate an attack or intercept the message. And if party only knows the message it sent and received, it is impossible to them to leak other sensitive information.

Lecture 60

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

   No, if there is no nonce, then the principals in the NS protocol cannot determine if the message is fresh or it's been a message from replay attack.

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

   Step 1: Sending saying: To S, this is A, I want to talk to B, Generate a key for us, use N_a in the reply subsequent message so I know it is the correct response. Receiver believes: A wan to talk to B, generate a key, reply with N_a

   Step 2: Sending saying: To A, this message can only be decrypted by AS private key, here is N_a to show message is reply to your request, you want to talk to B, here is the key for K_{ab}, this is the signature you want to send to B, it will certify you as A and you're the key. Receiver believes: This is the fresh reply from S, key is been generate for AB, and I need to send the signature to B.

   Step 3: Sending saying: To B, here is the my signature certify by S, it also contain Key for communication between A and B. Receiver believing: I can decrypt this message using private key of BS, A is certify by S, A want to talk to me with Key AB.

   Step 4: Sending saying: To A, send you a nonce with our new session key, ack. Receiver believing: B wants me to ack with new session key.

   Step 5: Sending saying: To B, ack with session key and function to the nonce N_b. Receiver belief: Session secure. It is the correct A I am talking to.

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 S still kept K_{as} in his key server, since the first step is communication from A to S without encryption, so attacker can sends this message and use K_{as} to decrypt S's reply in step 2. Since A is the initiator of the message and S only knows message is from A by their shared key K_{as}.

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

   Yes and no depend on the context and depends on the strength of the encryption.

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

   In the case of Bauer, et al. encrypt the message in step 1 with K_{as} or whatever new key A is change to and inform S about the change when deleting old record of K_{as}.

   In step 2 of NS, ask S to communicate with B directly with K_{bs} and give the K_{ab} to B. Do not send message without nonce.

Lecture 62

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

   The M (session identifier), it tells A and B they are in the same session. To B, it guarantees B gets K_{ab}, but to A, it does not guarantee K_{ab}.

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

   NS guarantee that at the end of protocol, both A and B has K_{ab}, but OR at the end of protocol only guarantee that B has the K_{ab}, and we are not sure if A received the message that contains key or not.

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

   Use a common nonce known only by A and B, if C intercepts the message, but C sends to B has no nonce, B knows that the message is from the attacker.

Lecture 63

1. Why is the verification of protocols important?

   Because protocols are crucial to the Internet, it would be great to get them right and find their flaws, so Internet can be made safer than it is right now.

2. What is a belief logics?

   It is one of the approaches to the protocol verification problem. Belief logics allow reasoning about what principals within the protocol should be able to infer from the messages they see. Allows abstract proofs, but may miss some important flaws.

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

   First we have to make some reasonable initial assumption about the state of knowledge/belief of the principals. Then we can take a sequence of message exchanges (program steps) and generate a collection of belief statements (abstract proof). And belief is what the principal infer from the message they see each step within the protocol.

Lecture 64

1. What is a modal logic?

   Standard propositional and predicate logic with some additional primitive and rules of influence built in to reason about a particular domain.

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

   If A believes A share a Key K with B and A sees a message {X} encrypted with key K, then A believes that message X is coming from B.

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

   If A believes message X is fresh, and A believes that message X coming from B, then A believes that B believes X (statement of belief)

4. Explain the intuition behind the jurisdiction inference rule.

   If A believes B is an authority on X, and A believes that B believes X, then A believes X.

5. What is idealization and why is it needed?

   Idealization is a process to get from protocol steps to logical inference, and this attempts to turn the message sent into its intended semantics. It is needed since the belief logic is a modal logic of belief, it consists a set of logical operators and rules of inference, not a sequence of message exchange or program statements.

Lecture 65

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

   Because it is the part of message that do not contribute to the beliefs of the recipient and because it can be forged by anyone since it is not encrypted.

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

   It might be the final goal of the protocol, also it could be the initial assumption we are force to given at the beginning of the proof. We write these assumptions of beliefs that will happen later because we believed that it would happen at the end of protocol run. We use these assumptions in carry out the proof, and find any suspicious assumption.

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

   Because we are forcing to write down all assumptions at the initial stage of the proof, and it shows exactly how these assumptions are used in carry out the proofs. If some assumption acts funny or surprised us, it can give us insight if this is indeed a weak/strong point of this protocol.