Freda Anderson fa3365
CS 361, Summer 2014
7/3/14

CS361 Questions: Week 4

Lecture 53

1. Why is it important for a digital signature to be non reusable?
    a. So the signature cannot be detached and reused for a different message.
2. Why is it the hash of the message typically signed, rather than the message itself?
    a. Public key encryption is expensive – hashes are cheaper. The hash is signed for authentication reasons.
3. What assurance does R gain from the interchange on slide 4?
    a. R knows that the message was sent from S.

Lecture 54

1. What is the importance of certificate authorities?
    a. A certificate is a letter of introduction – vouching for the accuracy of the binding.
2. In the example on slide 5, why does X sign the hash of the first message with its private key?
    a. So that Y knows it is really X.
3. Why is it necessary to have a hash of Y and Ky?
    a. The certifying authority needs both to certify the binding.
4. What would happen if Z had a public key for X, but it was not trustworthy?
    a. It wouldn't have a hash of X.

Lecture 55

1. What happens at the root of a chain of trust?
    a. It should be an unimpeachable authority that holds all chains.
2. Why does an X.509 certificate include a "validity interval"?
    a. So the user can check the times.
3. What would it mean if the hash and the received value did not match?
    a. Something or someone has appended or removed something.

Lecture 56

1. What are some protocols previously discussed?
    a. HTTP
2. What may happen if one step of a protocol is ignored?
    a. It doesn't work
3. Why must the ciphers commute in order to accomplish the task in slide 4?
    a. They both need the same key.
4. Describe how an attacker can extract M from the protocol in slide 6.
    a. An eavesdropper who stores the three messages can XOR combinations of them to extract any of M, Ka, and Kb.

5. Describe how an attacker can extract K_a from the protocol in slide 6.
    a. An eavesdropper who stores the three messages can XOR combinations of them to extract any of M, Ka, and Kb.
6. Describe how an attacker can extract K_b from the protocol in slide 6.
    a. An eavesdropper who stores the three messages can XOR combinations of them to extract any of M, Ka, and Kb.
7. Why are cryptographic protocols difficult to design and easy to get wrong?
    a. Because you just need one easy point of entry or a few pieces of data to get a key or value.

Lecture 57

1. Explain the importance of protocols in the context of the internet.
    a. An internet protocol is a structured dialogue among two or more parties (host to router, host to host, router to router…) from anywhere in the world that can connect to a connected subnetwork.
2. Explain the importance of cryptographic protocols in the context of the internet.
    a. Cryptographic protocols in the context of the internet allows the secure transfer of data – so that no one can change or eavesdrop a message.
3. What are the assumptions of the protocol in slide 6?
    a. A can open the message from B by using their secret key and B can open the message by using B's secret key. The assumption is that A can verify it is B and B can verify it is A.
4. What are the goals of the protocol in slide 6?
    a. Verification
5. Are the goals of the protocol in slide 6 satisfied? Explain.
    a. No, they are not because Kb and Ka are public and any one can use them.
6. How is the protocol in slide 6 flawed?
    a. Kb and Ka are public and any one can use them.

Lecture 58

1. Why is it important to know if a protocol includes unnecessary steps or messages?
    a. To know if data is repeated.
2. Why is it important to know if a protocol encrypts items that could be sent in the clear?
    a. To know the sensitivity of the information.

Lecture 59

1. Why might it be difficult to answer what constitutes an attack on a cryptographic protocol?
    a. Attack subtle, there are many different types of attacks, and there can be holes in protocols people aren't aware of.
2. Describe potential dangers of a replay attack.
    a. There is double data - this can reset or increment values.
3. Are there attacks where an attacker gains no secret information? Explain.
    a. Yes, attackers can add information without reading.
4. What restrictions are imposed on the attacker?

    a. They have to follow some part of the protocol.
5. Why is it important that protocols are asynchronous?
    a. So that the attacker can't synchronize an attack.

Lecture 60

1. Would the Needham-Schroeder protocol work without nonces?
    a. It would work but it wouldn't be secure.
2. For each step of the NS protocol, answer the two questions on slide 5.
    a. What is the sender trying to say with this message?
        i. Sends Na
        ii. Kab
        iii. Kab
        iv. Nb
        v. Nb -1
    b. What is the receiver entitled to believe after receiving the message?
        i. A's and B's messages are fresh/Nb is a new nonce.

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?
    a. A impersonator requests a new nonce with B.
2. Is it fair to ask the question of a key being broken?
    a. Yes
3. How might you address these flaws if you were the protocol designer
    a. Question the key everytime.

Lecture 62

1. What guarantees does Otway-Rees seem to provide to A and B?
    a.
2. Are there guarantees that Needham-Schroeder provides that Otway-Rees does not or vice versa?
3. How could you fix the flawed protocol from slide 4?

Lecture 63

1. Why is the verification of protocols important?
    a. Protocols are crucial to the Internet – we should strive to get them right.
2. What is a belief logic?
    a. Belief logic allows reasoning about what principals within the protocol should be able to infer from the messages they see.
3. A protocol is a program; where do you think beliefs come in?
    a. Initial assumptions.

Lecture 64

1. What is a modal logic?
    a. A logic that express belief of the state/qualify a statement.
2. Explain the intuition behind the message meaning inference rule.
    a. A is an authority on X and can be trusted on X. If A trusts X, X can be trusted.
3. Explain the intuition behind the nonce verification inference rule.
    a. 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.
    a. 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?
    a. Idealization attempts to turn the message sent into its intended semantics. It is needed 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?
    a. It does not contribute to the beliefs of the recipients.
2. Some idealized steps seem to refer to beliefs that will happen later in the protocol. Why would that be?
    a. It means that if we do this the later state should be true.
3. One benefit of a BAN proof is that it exposes assumptions. Explain that.
    a. In order to get to state x, one must start from state y.