Brian Chow
EID/CS login: bc23784
Email: brianj.chow@yahoo.com
CS 361 (90155)
For 07/03/14

Week 4 Questions

Lecture 53

1) Why is it important for a digital signature to be non-reusable?
    1. So that a message cannot be modified by removing the signature, editing the message, and then reattaching the signature to the message. This helps ensure authenticity.
2) Why is it the hash of the message typically signed, rather than the message itself?
    1. The hash is usually of a fixed size, while the message itself can be of any length.
3) What assurance does R gain from the interchange on slide 4?
    1. Only S can use K_S^{-1}, "a third party can verify the signature with KS", "only R can remove the outer layer of encryption", and the signature is tightly bound to the message M."

Lecture 54

1) What is the importance of certificate authorities?
    1. They verify that a public key is bound to only one party.
2) In the example on slide 5, why does X sign the hash of the first message with its private key?
    1. To verify to Y that it was X who signed the certificate.
3) Why is it necessary to have a hash of Y and K_Y?
    1. It is necessary in order to bind the party together. The hash is used to verify the party.
4) What would happen if Z had a public key for X, but it was not trustworthy?
    1. Z cannot trust certificates that are signed by the untrustworthy public key for X.

Lecture 55

1) What happens at the root of a chain of trust?
    1. There is an "unimpeachable authority in trust."
2) Why does an X.509 certificate include a "validity interval"?
    1. The validity interval specifies the start and end times for the certificate's validity. This means that the certificate will expire after some period of time.
3) What would it mean if the hash and the received value did not match?
    1. Either the certificate has been altered, or an external party is masquerading as the other party.

Lecture 56

1) What are some protocols previously discussed?
    1. One-way functions, asymmetric/symmetric encryption protocols, AES, etc.
2) What may happen if one step of a protocol is ignored?

   1. It could end up breaking the protocol and/or it is not possible to verify that the message was successfully transmitted or who it was sent by.
3) Why must the ciphers commute in order to accomplish the task in slide 4?
   1. This would allow Person A to “'reach inside' Person B's encryption to undo” his. They allow the locks of cryptographic algorithms with appropriate cryptographic keys to be removed.
4) Describe how an attacker can extract M from the protocol in slide 6.
   1. The attacker could XOR message 3 with message 2 to remove B's lock on message 2. The result of this could then be XOR'd with message 1 to remove A's lock on message 1.
5) Describe how an attacker can extract K_a from the protocol in slide 6.
   1. The attacker could XOR the result of the previous question with message 1.
6) Describe how an attacker can extract K_b from the protocol in slide 6.
   1. The attacker could XOR message 1 with message 2, then XOR the result of that with the result of question 4.
7) Why are cryptographic protocols difficult to design and easy to get wrong?
   1. There are many ways to reverse-engineer a step of the protocol, which could lead to further reverse-engineering of the other steps and lead to a completely insecure message.

Lecture 57

1) Explain the importance of protocols in the context of the Internet.
   1. They prevent someone/something from altering the “syntax, semantics, and synchronization of communication” of the structured dialogue between two or more parties, much like the use of prepared statements in SQL helps (but does not completely prevent) SQL injection attacks.
2) Explain the importance of cryptographic protocols in the context of the Internet.
   1. They help ensure, among other things, integrity (a message arrived unmodified), authenticity (the message's claim of origin is true), confidentiality (the message contents are inaccessible to an eavesdropper), and non-repudiation of origin/receipt (sender/receiver can't deny sending/receiving, respectively).
3) What are the assumptions of the protocol in slide 6?
   1. That there is a public key system already in place, the secret key is shared over a secured channel, and that each party has an accurate/reliable copy of the public key.
4) What are the goals of the protocol in slide 6?
   1. That A recognises B and that messages between the two are sent securely.
5) Are the goals of the protocol in slide 6 satisfied? Explain.
   1. Yes – with the assumptions satisfied, only A and B can read messages and verify that the other party sent the message.
6) How is the protocol in slide 6 flawed?
   1. An attacker/either of the parties can intercept a message and change its value, since there is nothing such as a hash to verify the contents of the message.

Lecture 58

1) Why is it important to know if a protocol includes unnecessary steps or messages?
   1. Every additional step that is unnecessary creates another possibility for an attacker reverse-engineering the protocol. Steps may also be used to introduce a covert channel

(e.g., a step that takes a long time to execute could be doing something with the message in the background). In addition, they may result in the protocol taking a longer time to execute to completion.

2) Why is it important to know if a protocol encrypts items that could be sent in the clear?
   1. This would constitute a large waste of time and resources – any and all steps that are unnecessary should be removed from the protocol.

Lecture 59

1) Why might it be difficult to answer what constitutes an attack on a cryptographic protocol?
   1. An attack can take many different forms – e.g., impersonating another party, interjecting messages from an earlier exchange (replay attack), etc.
2) Describe potential dangers of a replay attack.
   1. An attacker could masquerade as one of the authorised parties and/or create confusion in one or more parties as to the state of the transaction/protocol.
3) Are there attacks where an attacker gains no secret information? Explain.
   1. Yes – perhaps probably most well-known, a denial-of-service attack, which is usually aimed at disrupting the traffic flow of a website.
4) What restrictions are imposed on the attacker?
   1. S/he cannot send messages (as another party A would be notified of A's participation.
5) Why is it important that protocols are asynchronous?
   1. To prevent more than the necessary number of parties from participating in the protocol (“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?
   1. No. Nonces prevent replay attacks (“A knows that B's message is *fresh* and not a replay from an earlier exchange”).
2) For each step of the NS Protocol, answer the two questions on slide 5 (“What is the sender trying to say with the message? What is the receiver entitled to believe after receiving the message?”).
   1. A wants to send a message to B with a new nonce. The receiver knows that A needs a new key in order to communicate with B.
   2. A receives the needed key, the target of the message, and the message itself (everything needed to communicate with B). The receiver knows that S is the sender.
   3. A informs B of the private key needed for communication. The receiver believes that A intends to use the private key for communication and that the key was created by S.
   4. B informs A that it received the key. The receiver (B) is entitled to believe that A successfully received the key.
   5. A informs B that it too can use the key and received B's last message. The receiver (B) is entitled to believe that the protocol has executed to completion and that the communication channel is now secure.

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?
    1. An attacker who deciphers K_{ab} can still initiate a transaction with B. B will believe it is talking to A.
2) Is it fair to ask the question of a key being broken?
    1. Yes – a key being broken is not a very useful key.
3) How might you address these flaws if you were the protocol designer?
    1. A nonce could be added to message 3, allowing B to determine whether or not the K_{ab} it receives is current and denying an attacker an "unlimited amount of time to crack an old session key and reuse it as if it were fresh."

Lecture 62

1) What guarantees does Otway-Rees seem to provide to A and B?
    1. A or B can prove his/her identity to the other one another through use of the session identifier; nonces help prevent replay attacks; modification of a message can be detected.
2) Are there guarantees that Needham-Schroeder provides that Otway-Rees does not or vice versa?
    1. B is not authenticated to A in Otway-Rees - although the server informs B that A used a nonce, B doesn't know if the nonce was a replay of an older message, which is acquired by an intruder locating an older nonce (which could be used to authenticate the intruder against B).
3) How could you fix the flawed protocol from slide 4?
    1. A certificate could be used to authenticate B to A.

Lecture 63

1) Why is the verification of protocols important?
    1. To ensure that they are not subject to any fatal flaws that may make the protocol essentially useless.
2) What is a belief logic?
    1. A belief logic "allows reasoning about what principles within the protocol should be able to infer from the messages they see." They "allow abstract proofs, but may miss some important flaws."
3) A protocol is a program; where do you think beliefs come in?
    1. During verification of the previous stages of the protocol – if a protocol has reached a certain step, then any assumptions about the previous stages can be believed to have been successfully met.

Lecture 64

1) What is a modal logic?
    1. It is a type of formal logic that allows someone to attach expressions of belief to statements; "rules of inference [are used] for manipulating the protocol to generate a set of beliefs."

2) Explain the intuition behind the message meaning inference rule.
    1. If A believes that it shares a key with B and A sees a message encrypted with that key, then A can reasonably believe that B sent the message.
3) Explain the intuition behind the nonce verification inference rule.
    1. If A believes that a message x is fresh (i.e., not replayed) and A believes that B once sent x, then A believes that B believes that x is fresh.
4) Explain the intuition behind the jurisdiction inference rule.
    1. If A believes B has control over x and A believes that B trusts x, then A can also trust x.
5) What is idealization and why is it needed?
    1. It is a process that is used “to get from protocol steps to logical inferences” by attempting to “turn the message sent into its intended semantics.” It helps “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?
    1. It is unnecessary to include (since it is plaintext) and may interfere with/influence the idealization of subsequent steps in the protocol.
2) Some idealized steps seem to refer to beliefs that will happen later in the protocol. Why would that be?
    1. It is assumed that those beliefs will be satisfied in some future step in the protocol that will unquestionably occur.
3) One benefit of a BAN proof is that is exposes assumptions. Explain that.
    1. Use of a BAN proof can show what is provable and what must be assumed in a given protocol, which allows for the protocol to be analysed and possibly redesigned before its specification is published.