NAME: Ali Pasha
UTEID: aap2493
CSACCOUNT: alipasha
EMAIL: alipasha@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 non reusable?
   A check is a *tangible object* authorizing the transaction.
   The signature on the check *confirms authenticity*.

2. Why is it the hash of the message typically signed, rather than the message itself?
   If P signs message M with signature $S(P,M)$, it must be impossible for anyone else to produce $S(P,M)$. Also ensures *no repudiation.*

3. What assurance does R gain from the interchange on slide 4?
   Public key systems are well-suited for digital signatures. Recall that some algorithms, RS

Lecture 54

1. What is the importance of certificate authorities?
   Certification addresses the need for *trust* in computer system

2. In the example on slide 5, why does X sign the hash of the first messagewith its private key?
   do two entities that are mutually suspici

3. Why is it necessary to have a hash of Y and K_y?
   relationship of trust. One way is to rely on a third party who

4. What would happen if Z had a public key for X, but it was not trustworthy?
   "vouches for" the trustworthiness of one

Lecture 55

1. What happens at the root of a chain of trust?
   We may believe a party's affiliation or ask for independent validation

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

In general, we have a “trust threshold,” a degree of

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

Trust we’re willing to confer without going further in the certification process.

Lecture 56

1. What are some protocols previously discussed?

This threshold may depend on the size or nature of

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

authorities for such transactions.

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

Business Bureau, and credit reporting agencies all function in part as certification = authorities for such transactions.

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

The most common circumstance in which trust is needed in a distributed context is in *binding a key to an identity*.

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

That is, how do I know that the public key you present is really your public key and not someone else’s?

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

Establishing trust may involve “chains” of certification.

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

In a large company, your supervisor may vouch for or certify your employment.

Lecture 57

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

His supervisor may vouch for him, and so on. A truly paranoid customer may require a chain of certifications leading back to some unimpeachable authority at the base

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

However, it would be unmanageable to require all of these parties to be present for communication to occur. There is a need to securely store and pass around records of such certification.

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

Sometimes certification occurs through a *common respected individual*. For example, suppose Ann and Andrew work for different divisions within the same company.

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

Presumably, they have a common supervisor (ancestor in the hierarchy tree of the company).

5. Are the goals of the protocol in slide 6 satisfied? Explain.
   If both trust their management, they can certify each other's authenticity via their common supervisor.

6. How is the protocol in slide 6 flawed?
   The chain can begin at the top or from the bottom of the hierarchy.

Lecture 58

1. Why is it important to know if a protocol includes unnecessary steps or messages?
   Electronically, certification is accomplished with digital signatures and hash functions.

2. Why is it important to know if a protocol encrypts items that could be sent in the clear?
   A public key and user's identity are bound together in a *certificate*. This is then signed by a *certification authority*, vouching for the accuracy of the binding.

Lecture 59

1. Why might it be difficult to answer what constitutes an attack on a cryptographic protocol?
   The following are possible steps. Suppose X is the president of the company and her immediate subordinate is Y. Each have a public key pair.

2. Describe potential dangers of a replay attack.
   Y's certificate is X's affirmation of her identity. Anyone can decrypt it with X's public key and look at the contents.

3. Are there attacks where an attacker gains no secret information? Explain.
   Now Y can certify the identify of her subordinates in a similar manner. She appends her certificate to each of theirs.

4. What restrictions are imposed on the attacker?
   Thus, an individual's certificate contains a chain of evidence rooted at some unimpeachable authority.

5. Why is it important that protocols are asynchronous?
   There is also a need for trust in situations where there is not a single hierarchy, such as on the Internet. Two individuals may not have a common "superior."

Lecture 60

1. Would the Needham-Schroeder protocol work without nonces?
   Some entity may be designated as a certification authority (notary public, personnel office, security officer in a company, etc.).

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

On the Internet, several groups serve as “root certification authorities”.

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?

Mastering Chess doesn't just happen. You need to learn to be more protective of your pieces, and more aggressive over the opponent. But you can never be sure you will definitely win a match.

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

Never give any pieces away for free, or give a bad trade.

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

Here are the relative value of pieces: Pawn = 1 Knight = 3 Bishop = 3 Rook = 5 Queen = 9.

Lecture 62

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

The King, obviously, cannot be taken, and is worth the game, basically. Inspect every move you take. Make the move in your mind.

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

Even if you're one pawn up, that could win you the game. That being said, even if you are down by, say, a knight, you could still win the game.

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

Just look for isolated pawns that could be nicked by you. However, don't let your guard down

Lecture 63

1. Why is the verification of protocols important?

Don't go complete aggression. Go about as a rule of thumb, 60% aggression and 40% defending.

2. What is a belief logic?

Chess is like a medieval war. You need to push the opponent back and invade their territory, in hopes of getting closer and closer to their King. If you're in a war, and you're being pushed back while your opponent is moving in on you, is that good for you? No, it will help your opponent win.

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

A rook is worth 5 points, and is easily abandoned in the lonely corner of your side, all by itself, doing nothing.

Lecture 64

1. What is a modal logic?

A waste of 5 points! However, if you move it down to the center of the back of your side, it would be dominating and attacking one of the two most powerful files of the game board - the Center.

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

Not only does it conflict with the touch-move rule, but it also makes you look like a bit of a dandy, and that you're not sure about where you're going to move the piece, if at all.

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

You don't have to practice against other people. You can also buy a chess engine to install for your computer and/or laptop, to play against the CPU!

4. Explain the intuition behind the jurisdiction inference rule.

In more recent Windows and Mac computers, a chess game is built in. Use this to practice!

5. What is idealization and why is it needed?

Play with confidence that you are going to win.

Lecture 65

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

Just keep practicing and don't give any pieces away! Keep moving forward! Protect your pieces and invade the board!

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

Don't ever risk your king, it's the most valuable piece on the board. Don't ever move backwards unless absolutely necessary.

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

If you completed all of these steps and you still lose, let the computer go first and just ask for a hint every time. However, if you want the satisfaction of beating the computer by yourself, just keep practicing.