FIRSTNAME : Michael;
LASTNAME : Truong;
UTEID : mkt532;
CSACCOUNT : mtruong;
EMAIL : mtruong92@utexas.edu;

CS361 Questions: Week 4

The questionsmarked 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?
someone else can authorize operations under your identity

2. Why is it the hash of the message typically signed, rather than the message itself?
public key encryption is expensive to apply, and the message may be arbitrarily long, but the hash is going to be a fixed, finite, short value

3. What assurance does R gain from the interchange on slide 4?
that the message is unforgeable, authentic, no repudiation, tamperproof, and no reusable; confidentiality and authenticity

Lecture 54

1. What is the importance of certificate authorities?
to vouch for the accuracy of the binding between a public key and a user's identity

2. In the example on slide 5, why does X sign the hash of the first message with its private key?
to verify x's signature

3. Why is it necessary to have a hash of Y and K_y?
to encrypt it with x's private key

4. What would happen if Z had a public key for X, but it was not trustworthy?
the hash of y and k_y would not be equivalent to the hash in the signed value

Lecture 55

1. What happens at the root of a chain of trust?
rooted at some unimpeachable authority

2. Why does an X.509 certificate include a "validity interval"?
to indicate when trust can be established; trustworthiness changes over time

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

trust is not established

Lecture 56

1. What are some protocols previously discussed?
bell and lapadula, biba's strict integrity, covert channels, encryption/decryption

2. What may happen if one step of a protocol is ignored?
confidentiality might be compromised

3. Why must the ciphers commute in order to accomplish the task in slide 4?
the two applications of k_a "cancel out," leaving (m xor k_b), which b can easily decrypt with his own key k_b

4. Describe how an attacker can extract M from the protocol in slide 6.
xor (m xor k_a) with xor (m xor k_a xor k_b) with (m xor k_a xor k_b xor k_a)

5. Describle how an attacker can extract K_a from the protocol in slide 6.
xor (m xor k_a xor k_b) with (m xor k_a xor k_b xor k_a)

6. Describle how an attacker can extract K_b from the protocol in slide 6.
xor (m xor k_a) with (m xor k_a xor k_b)

7. Why are cryptographic protocols difficult to design and easy to get wrong?
the environment is hostile or untrustworthy, ciphers have to commute

Lecture 57

1. Explain the importance of protocols in the context of the internet.
a protocol is a structured dialogue among two or more aprties in a distributed context controlling the syntax, semantics, and synchronizatino of communication, and designed to accomplish a communication-related function

2. Explain the importance of cryptographic protocols in the context of the internet.
a cryptographic protocol is a protocol using cryptographic mechanisms to accoplish some security-related function

3. What are the assumptions of the protocol in slide 6?
there's a public key infrastructure in place and that each of them has a reliable version of the other's public key

4. What are the goals of the protocol in slide 6?
does each party know that the other party have the key and can use it

5. Are the goals of the protocol in slide 6 satisfied? Explain.
suppose an attack c obtains the message $\{\{k\}_{ka^{-1}}\}_{kb} = k'$;
c -> b: $\{\{k'\}_{kc^{-1}}\}_{kb}$;
b -> c: $\{\{k'\}_{kb^{-1}}\}_{kc} = \{\{\{\{k\}_{ka^{-1}}\}_{kb}\}_{kb^{-1}}\}_{kc} = \{\{k\}_{ka^{-1}}\}_{kc}$, allowing c to extract the original

k;

6. How is the protocol in slide 6 flawed?
suppose an attack c obtains the message $\{\{k\}_{ka^{-1}}\}_{kb} = k'$;
c -> b: $\{\{k'\}_{kc^{-1}}\}_{kb}$;
b -> c: $\{\{k'\}_{kb^{-1}}\}_{kc} = \{\{\{\{k\}_{ka^{-1}}\}_{kb}\}_{kb^{-1}}\}_{kc} = \{\{k\}_{ka^{-1}}\}_{kc}$, allowing c to extract the original k;

Lecture 58

1. Why is it important to know if a protocol includes unnecessary steps or messages?
to modify the protocol to not include unnecessary steps or messages, to save processing time, bandwidth, and resources

2. Why is it important to know if a protocol encrypts items that could be sent in the clear?
to modify the protocol to not encrypt items that could be sent in the clear; to save processing time, bandwidth, and resources

Lecture 59

1. Why might it be difficult to answer what constitutes an attack on a cryptographic protocol?
"a good attack is one the engineers never thought of"

2. Describe potential dangers of a replay attack.
the parties might get confused or protocol might be disrupted

3. Are there attacks where an attacker gains no secret information? Explain.
replay attacks and interleaving attacks might just disrupt protocol or confuse the parties; unsucessful attacks

4. What restrictions are imposed on the attacker?
the attacker's messages cannot be artibrary, we assume the attack can't generate a message encrypted with a key it doesn't have

5. Why is it important that protocols are asynchronous?
no-one but the initiator knows the protocol is running until they receive the first message; the protocol has to be designed in such a way that when a party receives a message, it knows what the message means and how to respond to it

Lecture 60

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

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

1: i want to talk to b; a wants to talk to b
2: here is the key; here is the key
3: i want to talk you, here is the key; a wants to talk to me, here is the key
4: i got the key and can use it; b has the key and can use it
5: i got the key and can use it; a has the key and can use it

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?
an attacker can pass a message to b: {k_ab, a}_k_bs

2. Is it fair to ask the question of a key being broken?
any cryptographic protocol is going to assume that we have certain secure keys

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

Lecture 62

1. What guarantees does Otway-Rees seem to provide to A and B?
authentication of both parties to each other and to s

2. Are there guarantees that Needham-Schroeder provides that Otway-Rees does not or vice versa?
each message is fresh; b doesn't know for sure that a has the key

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

Lecture 63

1. Why is the verification of protocols important?
protocols are curcial to the internet; it would be great to get them right

2. What is a belief logic?
belief logic: a formal system for reasoning about beliefs. any logic consists of a set of logical operators and rules of inference

3. A protocol is a program; where do you think beliefs come in?
you have to postulate some reasonable initial assumptions about the state of knowledge/belief of the principals

Lecture 64

1. What is a modal logic?
formal logic that extends propositional and predicate logic to include operators expressing modality

2. Explain the intuition behind the message meaning inference rule.
if a believes (a share(k) b) and a sees $\{x\}_k$ then a believes (b said x)

3. Explain the intuition behind the nonce verification inference rule.
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.
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?
idealization: a process to get from protocol steps to logical inferences. this attempts to turn the mesage sent into its intended semantics; one purpose of idealization is 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?
all plaintext is omitted since it can be forged

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

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

it forces you to write down your assumptions and it shows exactly how those assumptions are used in carrying out the proof