WEEK 4 QUESTIONS

Name: Charu Sharma
EID: cs36739
CS Login: charu
E-mail: charu.sharma@utexas.edu

LECTURE 53

1. A digital signature has to be non reusable, because if it is, it can be detached and then reused for another message, which defeats the purpose of a digital signature.
2. A hash of a message gets signed, because public key encryption is expensive to apply, and the message may be long, while the hash will be a fixed, finite, shorter value.
3. It is unforgeable, because only S has its private key. It's authentic, because a third party can verify the signature with the public key. There is no repudiation since only S can use its decryption key. It is tamper proof because only R can remove the outer layer of encryption. It is not reusable, because the signature is tightly bound to message M.

LECTURE 54

1. A certificate authority is important, because it allows a known third party to vouch for anoter party if appropriate, allowing the first party to have a certain level of trust in the second, based on the third's vouching. It vouches for the accuracy of the public key and a user's identity binding.
2. Only X would know its private key, so it assures that X is really the one vouching as a certificate authority, so that no one has interfered or forged the signature.
3. It has to compare the hash of Y and Ky to the beginning value it received in the signed value, showing that the values weren't changed or corrupted.
4. If X was not trustworthy, then the signature wouldn't be validated. There would be no reason for this entity to be believed based on a non-trustworthy third party vouching for it.

LECTURE 55

1. At the root of a chain of trust is some unimpeachable authority.
2. An X.509 certificate includes a "validity interval", because to record the start and end times for validity so we know how long a certificate is valid for.
3. If the hash and the received value did not match, the signature would not be valid, and ther is no reason to trust the entity.

LECTURE 56

1. Public key encryption, the one-time pad, and private key encryption are both protocols.
2. If a step is missed, the entire protocol could be ruined and security could be violated entirely.
3. If Ivan puts your lockbox inside another locked box, the protocol wouldn't work unless you can reach inside his box to take off your lock. This is what commuting ciphers allow us to do.
4. An eavesdropper could store the three messages and can XOR combinations of them to extract M, Ka, or Kb.

5. If you XOR Step 2 with Step 3, you get Ka, and XORing this with Step 1 will get you Ka. Getting Ka will get you back to M, which is your original message. An eavesdropper has discovered the secret.
6. If you XOR Step 2 with Step 3, you will get Ka.
7. If you XOR Step1 with Step 2, you will get Kb.
8. They are difficult to design, because the designer has to consider each and every different possible state and potential attack. Additionally, they are easy to get wrong, because one aspect of decryption will probably get by the designer.

LECTURE 57

1. Because the Internet works internationally amongst many users, a certain consistency is imperative for the Internet's usage. Protocols are important in establishing this consistency.
2. In the context of the Internet, the cryptographic protocol is important, because the internet is essentially a medium for many subjects to exchange messages. The safe and secure exchange of these potentially private messages requires detailed cryptographic protocols.
3. It assumes that both A's public key is known to B, but its private key is known only to A. It assumes that B's public key is known to A, but its private key is known only to B.
4. The goal is to allow A to share a secret key K with B, but have each party be authenticated to the other.
5. This goal is not accomplished, because A and B won't be able to undo the other's private key.
6. It is flawed because our assumptions were problematic.

LECTURE 58

1. It is important to know I a protocol includes unnecessary steps or messages, because the assumption when using a protocol is that each step has to be followed and ignoring a step will violate the protocol and therefore keep security goals from being met. However, unnecessary steps then will be carried out by the nature of protocols, wasting unnecessary time.
2. Encryption is very expensive, and therefore encrypting items that could be sent in plaintext causes not only confusion but inefficiency.

LECTURE 59

1. There are many ways for an attack to occur, including violation of authentication or secrecy, impersonation of parties, and corruption of messages, as well as many tools attackers can use to carry out these attacks. For this reason, analyzing what constitutes an attack requires us to realize what is really fair to account for in preventing attacks. For instance, if any key is compromised, there may or may not be security consequences, and based on those consequences we might decide we have or have not encountered an attack.
2. A replay attack is dangerous because an old message is being considered fresh, violating the temporal aspect of a message. An outdated message might cause a past action to occur at the wrong time, which could violate and destroy a protocol or process.
3. The restrictions imposed on the attacker include that he or she must be able to glean not only an encryption/decryption key, but where in the process the system is at, as

well as whether he or she has found success in decryption. Also, the attacker must pass messages that look like what the system is expecting.

4. Protocols must be asynchronous, because a party to a protocol can't know anything about the current run of the protocol except the messages it has received and sent. This means that besides the intitiator, other parties participating won't even know that they are participating until they receive their first message.

LECTURE 60

1. The Needham-Schroeder protocol wouldn't work without nonces, because the nonces allow the recipients to know that the messages they are receiving are not only authentic but fresh rather than replays of old messages by an attacker.
2. In step 1, the sender is trying to tell the server that A and B are going to communicate with the help of Na. The receiver is led to believe that A and B will communicate, and Na shows that the message is fresh. In step 2, the server tells A gives A the private key A and B will be sharing. A is led to believe that this key is private and fresh. In step 3, A is trying to tell B its message with its private key, encrypted through the server's key received in the last step, so that B is led to believe that A's message is secure, from A, and that its server key is only available to it and the server. In step 4, B is trying to tell A its nonce as fresh encrypted with their private key, so that A is led to believe B will give it fresh information. In step 5, A is trying to tell B that its message is old, encrypted by their private key, which is what B is led to believe.

LECTURE 61

1. A could still be impersonated with the old key, so that B still believes that it is talking to A, because it has old messages decrypted.
2. It is fair, because a broken key could allow every message to be decrypted, which has grave consequences for the security of the system.
3. I would encrypt them using a combination of top approaches rather than just one, because they are the most important section of secure systems.

LECTURE 62

1. Otway-Rees seems to ensure that A and B are really communicating fresh, encrypted messages with one another through a server, S.
2. Otway-Rees provides the additional guarantee that the message is actually fresh, since Needham-Schroeder had potential for replay if an old key were broken. Each key is encrypted in Otway-Rees algorithm.
3. I would switch Ka-1 and Kb, so that the canceling doesn't occur.

LECTURE 63

1. Since protocols are easy to make mistakes on, it is necessary to be able to reason formally about protocol correctness and have a rational, organized, and consistent process for protocol verification.
2. Belief logics is a method that allows reasoning about what principles within the protocol should be able to infer from the messages they see. Because it allows abstract proofs instead of system-specific rules, it may miss some important flaws in a protocol.
3. When examining a program, it is important to examine the big picture. Every program is built on abstract algorithms which rely on certain principles and goals.

The assurance that these goals are not being violated verifies the program to an extent.

LECTURE 64

1. Modal logic is a formal logic that extends propositional and predicate logic to include operators expressing modality to qualify a statement.
2. The meaning inference rule says that if A believes in the validity and security of a secret key K between it and B, and A sees a message X encrypted with that key K, then A believes that B said X, since that is the only way the message could be encrypted with the secret, trusted key K.
3. Nonce verification says that if A believes X is a fresh message, and A believes that B once said X, then A believes B believes X, because in order for B to currently believe X, X must be current and said by B at some point, namely this point if X is fresh.
4. Jurisdiction says that if A believes B has jurisdiction over X and A believes B believes X, then A believes X, too. This makes sense, since B is an authority on X, A trusts B, and A knows B believes X, so A will also believe X, since B has vouched for X.
5. Idealization is a process which attempts to turn a message sent into its intended semantics. It is necessary, because it omits parts of the message that don’t contribute to the beliefs of the recipient, making it easier to use the new semantic form to form beliefs logic.

LECTURE 65

1. Plaintext is omitted in a BAN idealization, because plaintext could have been forged.
2. Idealized steps have to consider future consequences of current beliefs, because a belief could violate protocol in the future.
3. It exposes assumptions, because leaps of faith can be found in the beliefs as you step through them. This can expose an outrageous assumption which causes a violation of protocol and breach of security.