Name: Olamide Fayemiwo
UTEID: oaf226
CSLogin: ofaye
Email: olamide.fayemiwo@live.com

Week 4

Lecture 53

1. It is important for a digital signature to be non reusable because we do not want the signature attached with the message to be reused for another message.
2. The hash of the message is typically signed rather than the message itself because the hash interprets it as something else so that any other party cannot decipher or get the signature and use it for another message.
3. The assurance that R gains from the interchange is that S is the one truly sending the message, so there is authenticity that the message is coming from S.

Lecture 54

1. The importance of certificate authorities is that they can vouch for authenticity for transactions being made between parties.
2. X signs the hash of the first message with its private key to provide authenticity that Y is to be trusted and the message being sent is truly from Y.
3. It is necessary to have the hash of Y and Ky because both are Y's public key and its identity which needs to be verified by the receiver. It is hashed because the receiver needs to know that the public key which is tied to Y is actually for Y and it has not been altered.
4. If Z had a public key for X, but it was not trustworthy then Z will not be able to read the message been sent by Y due to the hashing of the key and identity by X.

Lecture 55

1. At the root of a chain trust, there is some unimpeachable authority.
2. An X.509 certificate includes a validity interval to show how long the party being verified as trustworthy can use that certificate so in the event that it is ever reused, the start and end times for validity will be checked and if it is passed the time, then we know the certificate is not real.
3. If the hash and the received value did not match then that means that the sender could not be vouched for by the third party.

Lecture 56

1. Some protocols previously discussed are BLP, Biba, Chinese Wall Policy, Ring Policy, Clark Wilson Policy.
2. If one step of a protocol is ignored then the message being communicated is not being secure or efficient anymore. Susceptible to malicious interceptors or you would not be able to even receive or send the message.
3. Ciphers must commute in order to be able to reach inside and receive the message being sent /received.
4. An attacker can extract M from the protocol if they figure out (XOR) one of the keys such as Ka's key in step one.
5. An attacker can extract Ka from the protocol in step 2 by xor'ing the message to figure out what Ka is.

6. An attacker can extract Kb from the protocol in step 3 because the two applications of Ka cancel out which leaves B easily to decrypt with his key.
7. Cryptographic protocols are difficult to design because of the complex way to secure messages in order to not let anyone intercept the transaction but it is easy to get it wrong if a simple step is missed which can open a door for malicious interceptors that can read the message.

Lecture 57

1. The importance of protocols in the context of the internet involves multiple things, such as sending an email, moving a file, etc. Internet protocol is used for communicating data across a packet switched network and gives us the ability to connect to the internet.
2. The importance of cryptographic protocols in the context of the internet is that it ensures secure data transport in which authentication, non-repudiation and key agreement is needed.
3. The assumptions of the protocol is that there is a public key infrastructure in place and that each of them has a reliable version of the public key
4. The goals of the protocol are unicity, integrity, and authenticity, and confidentiality, non-repudiation of both origin and receipt.
5. These goals are being satisfied because for unity, both A and B are sharing the messages to each other. Integrity: The message that A sends to B is what B sends back to A unchanged. Authenticity: Both parties have attached keys with the message to show that it is actually them sending it. Confidentiality: The keys that are attached to the messages are only held by A and B. Non-repudiation of origin and receipt: A cannot deny sending the message to B because it has A's keys on it and vice versa.
6. The fatal flaw of the protocol is that there is a way for an eavesdropper C to obtain messages and initiate a new run of the protocol on the sender in which it can cancel out the senders key and replace it with his.

Lecture 58

1. It is important to know if a protocol includes unnecessary steps or messages because it can help to speed up the process or it could eliminate areas that could be susceptible to an attack.
2. It is important to know if a protocol encrypts items that could be sent in the clear because it is possible for an eavesdropper to be able to see it and act like it is the original sender of the message.

Lecture 59

1. It is difficult to answer what constitutes an attack on a cryptographic protocol because there are many factors to consider, it's all about understanding what an attacker might do. Such as are both authentication and secrecy assured, do the parties know that they are the people that they are truly talking to, are the messages being sent securely, resources available to the attacker etc.
2. The potential dangers of a replay attack would be the eavesdropper impersonating someone's identity and receiving a message he is not authorized to receive.
3. An interleaving attack is an attack where the attacker gains no secret information because all it does is send spurious messages into a protocol run to disrupt it does not gain anything about the senders or receivers.
4. The attacker can only send the messages, and the attacker does not know who its sending to neither does he have any information about the message.

5. It is important that protocols are asynchronous because it is more secure to run information intermittently rather than in a steady stream. If information is being passed on a steady stream, then attackers will know when to intercept and act like the receiver for a message.

Lecture 60

1. The Needham-Schroeder Protocol might work without nonces, that is if a timestamp is used but that makes the values for the messages not new each time and there is a large window for attackers to know the value being generated by the secure key server.
2. **Step 1**:
    a. The sender A is telling the key server S that it wants to communicate with a receiver B and is requesting that the key sever S create keys with the new nonce it has given.
    b. The receiver S is entitled to believe that S is secure and is willing to communicate securely with B with the generated keys.

    Step 2:
    a. The sender is trying to say that it has created a new key for both A and B to use where it is encrypted and only A and S can decrypt the key, it includes the nonce indicating that the message is fresh, B's identity and the key for both A and B. The new information is encrypted with B's keys in which A cannot decrypt.
    b. The receiver A is entitled to believe that the message is encrypted and that it can actually send this message with both of their keys to B for b to decrypt it.

    Step 3:
    a. The sender A is trying to send the encrypted message to B with A's identity to show that they have a shared key.
    b. The receiver B is supposed to believe that A wants to communicate with B and that there is a shared key that has been generated by the secure key server.

    Step 4:
    a. The sender B is trying to communicate with A that it already has the key it received.
    b. The receiver A is supposed to believe that the information has not been lost when sending it and that B has the key and can use it.

    Step 5:
    a. The sender A is trying to respond to B to tell that it also possesses the key.
    b. The receiver is entitled to believe that A got its message in its previous step and has actually added another function to the message to show authentication.

Lecture 61

1. A could still be impersonated by another subject retrieving information from previous runs and getting a hold of Kab.
2. Asking whether a key is being broken depends on the strength of the encryption.
3. Make an effort to fix step 3 to make sure that Nonces are implemented in to ensure security, or figure out a way to use two separate keys that can be shared.

Lecture 62

1. Otway-Rees seems to provide A and B a session identifier (a number unique for each run of the protocol) and it prevents replay attacks.
2. Needham-Schroeder provides a way for the sender and receiver to make sure that it is both of them that are actually communicating together but in Otway-Rees, the sender B does not know for sure that A has the key.
3. It's a subtle attack so it's hard to find the flaw even fixing it.

Lecture 63

1. The verification of protocol is important because it is a preventative measure due to protocols being widely used and there have been flaws that have gone unnoticed for years. It is difficult to get protocols correctly.
2. A belief logic is a formal system for reasoning about beliefs. Any logic consists of a set of logical operators and rules of inference. Belief logic allows reasoning about what principals within the protocol should be able to infer from the messages they see which allows abstract proofs but may miss some important flaws.
3. Beliefs will be statements in the programs.

Lecture 64

1. A modal logic is a type of formal logic that extends predicate logic to include operators expressing modality (qualifies as a statement).
2. That if A believes that A and B share a key, and A has read (received) X which was encrypted with K, then that means that B sent the message.
3. That if A believes that a message (statement of belief) being read (received) is fresh and that it came from B, then A believes that B also believes.
4. In the jurisdiction inference rule, if A believes that B is an authority of things type X, then A believes that B believes the message (X) then A is entitled to believe X
5. Idealization is made to figure out what a message X is trying to accomplish in making the receiver believe a certain thing. Idealization is needed to omit parts of the message that do not contribute to the beliefs of the recipients.

Lecture 65

1. The plaintext is omitted in a BAN idealization because there are no beliefs in that step. A is sending S a nonce to create, which it is going to do so.
2. Forces you to write assumptions, the proof exhibits some assumptions that are not apparent.
3. It tells you the how the assumptions were used in the run