Lena Ko
UTEID: lk5399
CS: lk5399
Ko.lena92@gmail.com

Lecture 53

1.If a signature is detached and reused for another message, a subject could falsely authenticate himself.

2. Public key utilization is expensive and the message may be long but the hash is finite.

3. R gains the assurance that the message was sent from S, unforgeable, authentic, non-repudiation, tamperproof, not reusable.

Lecture 54

1. A certification authority vouches for the accuracy of the binding.

2. X signs the hash of the first message with its private key to assure that it was indeed X who certified the message.

3. The hash assures that the original message was not corrupted or changed somehow by comparing the values.

4. Z would not be able to read the certificate.

Lecture 55

1.At the root of a chain of trust there is an unimpeachable authority.

2. X.509 includes a validity interval because it designates a time that the certificate is valid for. It should not be trusted if it is expired.

3. The integrity has been compromised.

Lecture 56

1.Some protocols previously discussed are key exchange and x.509.

2. If one step of a protocol is ignored, it may not be as secure as it should be.

3. Ciphers commute in order to accomplish the task because

4. An attacker can XOR Mkb with Kb to get M.

5. An attacker can XOR MKaKbKa with MKaKb to get Ka.

6. An attacker can XOR MKaKb with MKa to get Kb.

7. There are conditions where an attacker could extract each message.

Lecture 57

1. Everything that occurs on the Internet occurs via a protocol. It controls the syntax and sync of communication and communication related functions. I.e. sending emails, files

2. Cryptographic protocols use mechanisms to accomplish a security function.

3. The assumption is that there is a public key structure in place and they have reliable public keys.

4. The goals are that the party has the key and a is talking to b and b is talking to a.

5. The flaw is that C can intercept the first message and send it with its own signature . B then sends the message with its own signature. The original message and B's signature cancel each other out, allowing C to extract the original K.

Lecture 58

1. It might have done things it didn't need to do.

2. The protocol might be inefficient because it didn't need to encrypt the items.

Lecture 59

1. What constitutes an attack is hard to understand because protocols have unknown vulnerabilities.

2. A replay attack is dangerous because they can use the recorded messages to inject them into the flow so the parties get confused.

3. Yes, the attacker can just disrupt the flow without receiving messages. They may confuse the parties such as the interleaving attack.

4. Restrictions imposed on the attacker are that the attacker can't create messages with a key that it doesn't have.

5. Protocols need to be asynchronous for security purposes. The messages need to be in the form for the party to be able to know how to respond.

Lecture 60

1.

a. A says to S to create a new key

b. S responds by generating a new key Kab, and packages the key and sends to a with a nonce that tells the message is fresh.

c. A sends key to B, A doesn't know b has the key B realizes Needham Schroeder protocol

d. b encrypts with new session key and says has the key and can use it
a knows b has session key

e. A responds by saying he has the key as well.

2.No, a nonce needs to be used so that they senders know there has not been a replay attack.

Lecture 61

1. S knows that a message actually coming from A is the fact that they share a secret key.

2. Yes and no, it depends on how secure the keys are made.

Lecture 62

1. Otway-Rees seem to provide A and B the guarantee that they are secure.

2. Needham Shroeder guarantees that A also has the key while Otway-Rees does not.

3. Adding a nonce would fix the problem because C would not be able to send the same message.

Lecture 63

1. Protocol verification is important because protocols can be difficult to get correct.

2. Belief logic allow reasoning about what principals within the protocol should be able to infer from the messages they see. Allows abstract proofs, but may miss some important flaws. IT is a formal system for reasoning about beliefs. Any logic consists of a set of logical operators and rules of inference.

3. If a protocol is a program, the beliefs come in when receiving messages, what one is entitled to believe. Need to specify initial beliefs to explain the protocol.

Lecture 64

1. Modal logic uses modal operators, a logic belief.

2. If A believes (A share(k)B) and A sees {x}k then A believes B said X.

3. If A believes X is fresh and A believes B once said X, then A believes B believes X.

4. If A believes B has jurisdiction over X and A believes B believes X, then A believes X.

5. Idealization is a process in which you get from protocol steps to logical inferences. A purpose of idealization is to omit parts of the message that do not contribute to the beliefs of the recipients. In BAN all plaintext is omitted since it can be forged. Idealization gets to the belief logic by understanding the protocol. Looking at each step in a protocol and figure out what it is trying to say.

Lecture 65

1. Plaintext is omitted because it does not have a belief logic, just a open message.

2. Idealized steps are assumptions of protocols so it may skip to steps from later in the protocol.

3. BAN exposes assumptions so it is easy to see what flaws a protocol may have in its assumptions.