Name: Scott Stephens
EID: sts768
CS Login: scott483
Email: stevo4932@gmail.com

Lecture 53

it is important for a digital signature to be non reusable so someone can't reuse it for another unauthorized purpose.

2. The hash is a fixed finite value while the message itself could be very long and complex to compute. That is why the hash is signed instead of the message.
3. R is assured that it is unforgettable authentic, no repudiation, tamper proof and not reusable.

Lecture 54

1. Certificate authorities help vouch or unknown third parties.
2. X signs the hash so that everyone knows that x has seen and trusts the message.
3. It is necessary to have a hash of y and ky to compare with the single
values to make sure nothing was corrupted.

Lecture 55
2. validity interval tells you how long it's trustworthy and vouched for.
3. Then it's not connect and is not valid.

Lecture 56
1. public and private key encryption as well as a one-time pad were previous protocols. Also the Confidentially and integrity models were protocols.
2. if a step is missing the whole system may fall apart and one or both parties may not be able to access the information.
3. Ciphers must commute so that part A is able to both put on and take off their lock.
4. M can extract the protocols by storing all three messages you have access to all the xor combos.
5. if you take m xor kb and m xor kax or kb then xor those two, the M's and kbs cancel out leaving ka.
6. KxKa xor Mx Ka x or Kb = Kb.
7. Cryptographic protocols have lots of way to accidentally give clues.

Lecture 57
1. Protocols for the internet ensure correct information is given and received by proper parties is vital to the use of the internet as trusted communication channel.
2. To ensure that information that flows is trustworthy and confidential for other pparties involved so that it can be a communication channel.
3. Public key infrastructure and they both have a copy of the others public key.
4. the goals are that each party has key k and that a is talking to b and b to a.

Lecture 58
1. Unnecessary steps or messages could be less efficient and more prone to attacks by allowing more clues to be explored.
2. It is important because it would be less efficient and more opportunity for hackers to learn something about the encryption.

Lecture 59
1. There are many different ways that a protocol may be changed or intercepted.
2. The dangers of a replay attack are the ability for someone to use messages from the past to confuse and learn about messages they are not authorized to view.
3. The attacker can't be an arbitrary message or hard to express what those are.
4. Protocols need to asynchronous so that a receiver knows how to respond to a received message.

Lecture 60
1. Without nonce, Needham-schroeder would work but you may be susceptible to replay attacks.
2. a) Says hey s, I'm A and I want to talk with B, here is a nonces, the receiver believes that A wants to communicate with B.
b) Says here is anew packaged key Kab that only wee can open, A believes S sent a new key Kab that can be used to talk with be (because it had A's nonce).
C) A tells B what the key is to talk to each other through a package only him and s can open. B wakes up and belies A want to communicate with him.
d) b says hey I have the key to A e) A says I have received that p knows you have the key.

Lecture 61
1. In step three a previously saved message could be sent to be and it would not be detectable since neither kas or kab are required for B to receive the message.
2. Yes it's computers, so it's always possible. But the actual danger depends on the strength of the system.
3. Might be helpful to replace the key's every so often and to have B verify with S that the Kab sent from S is actually valid.

Lecture 62
1. Seems to provide the guarantee that A and B are who they say they are as they have S broken.
2. Otway-Rees does not allow A to know if B has the key as message 4 may have been lost.
3. To fix the flaw you would need to remove the B public key step so that it does not cancel anything out.

Lecture 63.
1. So that holes in your security protocols are caught and potential malicious activities are stopped.
2. Allows reasoning about what principals within the protocol should be able to infer from the messages they see.
3. Beliefs for programs come in on the expectation of how they will run and what they do with the information they receive and produce.

Lecture 64
1. It is a set of operators and inference rules to infer new facts from old ones.
2. Basically where if only a and b share a key and a message is encrypted with that key. It can be assumed that only the of the two parties could be the sender.
3. if A believes X is a new message and that x came from B, then A must think that B believes X.
4. It means A is an authority on X and can be trusted on X. aka if B is superior to X and I believe B, then I must believe X.
5. Idealization is used to get from protocol steps to logical inferences. It is needed to omit parts of the message that do not contribute to the beliefs of the recipients.

Lecture 65

1. Plain text in BAN can be forged and so is omitted.
2. So that you can infer where you are going with this step and make sure that it will be possible.
3. It helps you to understand what is happening and what the state of information between each party is so that you know how to proceed with your next step. It can also save you from having to question each possibility.