Name: Tolu Kalejaiye
UTEID: tok76
CSUserID: tok76

HOMEWORK 4

Lecture 53

1. So that the signature cannot be put on any other transaction not authorized by holder of the signature.
2. To provide a higher level of security.
3. The assurance that the message came from S

Lecture 54

1. They act as a third party that can vouch for the authenticity of the certificate.
2. So that it's known that it was actually signed by X and not someone else pretending to be X.
3. For security purposes. To encrypt the message.
4. It wouldn't be able to verify X's signature, and thereby wouldn't be granted access.

Lecture 55

1. There is some unimpeachable authority ensuring the validity of the entire transaction.
2. To make sure that the certificate in question is still valid and hasn't been deemed outdated or compromised.
3. It wouldn't be possible to validate the certificate

Lecture 56

1. Certificates, public key encryption, cryptographic hash functions.
2. The whole protocol may become ineffective.
3. So that you can get the message inside. If they don't, you're stuck with your lockbox being locked inside another lockbox that you can't get into.
4. By comparing the 1st and 3rd steps, you can determine what Ka does to the message, and then apply that to the 1st step to figure out M.
5. Using the 1st and 3rd steps, you can determine what Ka does to the message, thereby discovering Ka.
6. If you've already figured out M and Ka, you just apply them to step 2 to figure out Kb.
7. They require several levels of misdirection, and you could easily get misdirected while trying to encode the message.

Lecture 57

1. They control the syntax, semantics, and synchronization of communication, and are designed to accomplish a communication-related function.
2. They are necessary to ensure users security while online.
3. That B is expecting a message from A, and that B receives the message.
4. To securely send a key K from A to B.
5. No. The message will be sent, but we cannot ensure it will be sent and received securely.
6. It is flawed because anyone with knowledge of Ka or Kb's public keys can access the encoded key.

Lecture 58

1. These could affect the efficiency of the protocol and/or be used as security loopholes for an attacker.
2. Once again, it could be an issue of efficiency.

Lecture 59

1. Because it may be very hard to analyze what an attacker might do. For example, it's possible to attempt to attack a protocol, but gain no secret information. If no secret information was gained, then does that count as an attack?
2. Possible re-issuing of commands given at an earlier time, giving instructions that were meant for one thing to another thing, accessing information that might have been previously saved, like new passwords, account numbers etc.
3. Yes. Since some protocols may encrypt items that could be sent in the clear, that may be the only information an attacker gains from the system.
4. There are no restrictions imposed on the attacker.
5. If they were synchronous, attackers could time their attacks to correspond with the sending/receiving of certain information, making their job much easier.

Lecture 60

1. Yes, but it would be vulnerable to replay attacks.
2. ?

Lecture 61

1. The attacker can send a message to A using Kas and gain more information about A that way, then begin impersonating A.
2. As long as no ones feelings are hurt.
3. Randomly regenerate keys over a certain interval.

Lecture 62

1. That their messages will be delivered.
2. No.
3. By making sure nonces are sent with every message.

Lecture 63

1. To reduce the possibility of flaws going unnoticed.
2. It is a formal system for reasoning about beliefs that generates a collection of belief statements using a sequence of message exchanges.
3. Beliefs may be rules as to how the program can be used.

Lecture 64

1. A type of belief logic that uses modal operators.
2. A believes it shared $\{X\}_K$ with B, so when it sees it unwrapped, it believes B must have done it.
3. If A hasn't seen X before, but knows B said X at some point, then it must have come from B.
4. If I believe you and you tell me you believe something, I must believe that thing as well (transitive property)
5. Idealization attempts to turn a message into its intended semantics. It is needed to make logical inferences when only given protocol steps.

Lecture 65

1. Because it doesn't need to be idealized since we can already make a logical inference from it.
2. It may be a sort of abstract belief. It may need something that hasn't happened yet, but it can infer that it will happen. (It's called faith)
3. It may be important to know what assumptions are being made so that in case anything goes wrong, you know if it's as a result of an assumption or something else(an attack).