Eric Tang
et5748

Assignment 4

Lecture 53

1. Signature should be bound to the document

2. Hash is smaller than the message

3. Unforgeable, authentic, no repudiation, tamperp roof, not reusable

Lecture 54

1. Establishes a trust between the end users

2. To create a certificate

3. To certify Y and it's public key - also used to check for corruption

4. Z could still receive Y and Ky

Lecture 55

1. Ideally, the chain is rooted at some unimpeacha ble authority.

2. How long the certificate is valid for (don't tr ust expired)

3. Corrupted data

Lecture 56

1. One-time padding

2. Security may be compromised

3. To share a key in order to send a message

4. Store all three message, XOR all three steps

5. XOR 2 and 3

6. XOR 1 and 2

7. Many loops that can be exploited; leaks can uni ntentionally happen

Lecture 57

1. A protocol is a structured dialogue among two o r more parties in a distributed context.

2. Using cryptographic mechanisms to accomplish se crutiy-related functions.

3. Reliable public keys

4. Does each party know the other party has receiv e keys/can use key.

5. No, could have middle attack.

6. They don't verify each other

Lecture 58

1. Because protocol steps are usually temporal

2. No as expensive

Lecture 59

1. Are both authentication and secrecy assured?
   Is it possible to impersonate one or more of th
e parties?
   Is it possible to interject messages from an ea
rlier exchange
   (replay attack)?
   What tools can an attacker deploy?
   If any key is compromised, what are the consequ
ences?

2. Retain message and later replay message to inte
rrupt flow of system.

3. That is not the usual assumption - we assume at
tacker has all non-secret info.

4. Cannot use arbitrary messages to attack.

5. Receiver won't know when a message is sent to
it, but must be ready to accept and process it.

Lecture 60

1. No

2. 1) A wants to send message to B; A wants to se
nd a message to B
   2) S verifies that A wants to send to B; A is
ready to sent to B
   3) A sends to B a secure message; B receives m
essage w/ it's public key
   4) B acknowledges it received the message; A b
elieves B received
   5) A nods to B that it received message; both
know messages received

Lecture 61

1. Yes

2. Not really

3. Try to include nounce in later steps.

Lecture 62

1. Authenticates both parties

2. A and B know they received messages

3. Hash

Lecture 63

1. So end users can verify one another as trsuted parties

2. A belief logic is a formal system for reasonin g about beliefs. Any logic consists of a set of lo gical operators and rules of inference.

3. Statements (bool)

Lecture 64

1. Logic model of belief.

2. If A believes (A share(K) B) and A sees {X}K th en 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 b elieves B believes X, then A believes X.

5. Attempts to turn the message sent into its int ended semantics. It helps omit parts of message th at don't contribute to the belief of recipients.

Lecture 65

1. There's no belief logic yet

2. There needs to be assumptions to base the system's logic off of.

3. Helps build new info for protocol.