Eric Tang
et5748

Assignment 5

Lecture 66

1. Pretty good privacy

2. Distrust of government

3. Yes - government agencies couldn't decrypt

4. Many bigger companies don't want freeware; they want to purchase
   reliable software with support.

Lecutre 67

1. Encrypt the has of the message using private key of the sender.
   Package with message - should verify the encryption

2. Encrypt session key with receiver's public key.

   Encrypt the message with session key.
   Package together.

3. Apply authentication step on original message.
   Apply confidentiality step on resulting message.

Lecture 68

1. Compression, email compatibility, and segmentation

2. Save bandwidth

3. Don't want signiture to depend on compression algorthm.

4. Maps groups of three octects into four ASCII characters - all computers can handle ASCII characters.
    (Expands message by 33%);

5. Allows all emailers to receive messages of sizes they may not have been able to handle.

Lecture 69

1. Session (symmetric) keys, Private/Public (asymmetric) keys, and Passphrase-based keys

2. High entropy strings

3. Two n/2-bit blocks generated by keystroke.
    Two blocks encrypted using E algorthm and previous key.
    Combined to form new key.

4. Generated using large random primes.

5. User generated passphrases. To keep private keys private

Lecture 70

1. Last 64 bits (least significant) of public key as ID.

2. Timestamp, key ID, public key, private key, user ID

3. Timestamp, key ID, public key, user ID

4. Enter passphrase, it's hashed, the hash is used to encrypt/decypt private key.

5. Authenticate users - mainly with certificates

6. Owner sends out key revocation certificate (cannot force receivers to acknowledge)

Lecture 71

1. Consumer: Attack stops the consumer from communicating with server
Producer: Attack overwhelm's server resources.
Producer attacks more prevalent

2. Attacker overwhelms server resources by sending illegitmate SYN packets to server -
server allocates and send out ACK packet that will not complete.

3. Table size: attacker just send more SYN packets

Shoten time: server might DoS slower clients
Filter: too aggressive will DoS legitimate requests

Lecture 72

1. Filtering prevents attacks from beginning in the first place - detects malicious packets.

2. Detection: after the attacks begin, detect patterns and react
Prevention: prevent attack before packet accepted

3. Over-provision: add more servers
Filter: detect and prevent malicious packets
Slow down process: slows down receiving of attacks
"Speak up": request more packets - attackers shouldn't be able to send more

Lecture 73

1. Both are bad - which one is worse depends on goal

2. Accurate: ability to detect all attacks
   Precise: ability to never report legitimate requests

3. It's easy to either report everything as an attack or nothing as an attack

4. It occurs in an event where the probability of focused event is very small among other events.
   In security, attacks are a rare occurance among many legitimate requests.

Lecture 74

1. Infect computers, attack whiethouse.gov

2. Static seed; pseudo random number generator

3. Resided in volatile memory (RAM); could remove by reboot

4. Actual random number generator. Random IP's could be non-PC devices and those would crash.

Lecture 75

1. Both exploit the buffer-overflow vulnerability in Microsoftâ€™s IIS webservers.

2. To infect as many devices as possible

3. Set up backdoor to devices

4. Unpatched machines let's bug/worms live - they can still infect that unpatched population

5. People are not reacting to threats by patching. It means we're lazy about security.

Lecture 76

1. Determine which measures of security is trustworthy and effective

2. Requirement for surity functions
Assurance requirment for establishing functional requirments
Methods for meeting functional requirements

3. To approve "quality" crypto products\

4. Basic
Improved physical security
Strong tamper-resistent and countermeasures
Complete envelope of protection - zeroes keys when breached

Lecture 77

1. Criteria for certificates that work internationally

2. The criteria that will allow it to be used internationally

3. For higher security reasons within regions or countries

4. PP: document that covers a security policy
ST: an evaluation for a product - what it should entail

Lecture 78

1. A PP is a documentation on how a security policy should be implimented -

what it should cover, what assumptions should be made, etc.

2. To cover threats and assumtion and to try to validate them.

3. Makes sure all threats are kept in check with a security policy, and to make sure all assumptions are validated by the system.

Lecture 79

1. To submit a system for evalution of security goals

2. A system is submited for evaluation on it's own terms of security and how it will counter them (including any assumptions). A PP is a guideline for products - one to be tested against.

Lecture 80

1. Evaluation assurance levels: evidence that the evaluation will succeed for the indicated level

2. Agencies for lower level EALs, and the government for the higher EALs.

3. Their security specification and requirements may differ than those from other countries.

4. No; they would just pass them and market them for higher profits regardless of how secure it is.

5. It means that someone else can do so similarly.