Name: Neil Jones
EID: nj2977
CSID: nfjones
Email: neil.franklin.jones@gmail.com

Week 5 Questions

Lecture 66

1. A general cryptographic scheme which uses several common algorithms.

2. He saw that the public needed a strong encryption scheme to protect information from government eyes.

3. Yes, it is very secure.

4. The company that produces it acts as a trusted third party, so that people using their PGP implementation don't have to worry about their info being compromised.

Lecture 67

1. The sender creates a message and generates a hash for it. They then encrypt the hash with their private key and prepend it to the message. The receiver decrypts the hash and compares it to a hash that they generate from the sent message in order to verify that the message came from the correct sender.

2. The sender encrypts the message using session key K. The sender then encrypts the key with the receiver's public key and sends it along with the encrypted message. The receiver uses their private key to decrypt the key and then use the key to decrypt the message.

3. Apply confidentiality to the result of authentication and send.

Lecture 68

1. Compression, Email compatibility, Segmentation.

2. It makes the message more compact and easier to send.

3. So that the signature doesn't depend on the compression algorithm and so that the encrypted message will have less redundancy.

4. It prevents the email service from misinterpreting some bit strings as control messages.

5. It allows the message to be sent in parts if it is very large.

Lecture 69

1. Session, public, private, pass-phrase based

2. They can only be used once and they have to be used symmetrically.

3. The previous key is encrypted and then combined with 2 half-size keys which are generated from user key-strokes.

4. A private and public keys are generated according to the RSA standard and the private key is encrypted.

5. They are encrypted and can only be retrieved by using a passphrase.

Lecture 70

1. They have ID's.

2. Each key has: timestamp, key ID, public key, private key, user ID

3. Each key has: timestamp, key ID public key, user ID

4. Retrieve the key from the key ring. Decrypt the key using a passphrase provided by the owner.

5. Determining how much a key can be trusted.

6. The owner issues a signed key revocation cert.

Lecture 71

1. The consumer problem involves a man in the middle while the producer problem involves overwhelming the receiver with transmissions.

2. The attacker sends TCP syn's without acking the server's response. This ties up server resources.

3. 1. It only lengthens the amount of time the server can stay in operation without fixing the problem.
    2. The attacker can just increase the rate of submission.
    3. Having to do this for every TCP handshake wastes time.

Lecture 72

1. It doesn't allow server resources to be tied up on prospectively illegitimate packets.

2. IDS reacts after an attack begins while IPS attempts to keep them from affecting the system in the first place.

3. Have too many servers to be overwhelmed. Filter packets. Slow down processing.

Request additional traffic from all senders.

Lecture 73

1. False positives occur when harmless activity is detected as harmful activity while false negatives do the opposite. False negatives are probably worse because they allow attacks to be effective.

2. It is accurate if it detects all genuine attacks and precise if it never misclassifies behavior.

3. It would be easy to build a system that lets nothing through (accurate) or which lets everything through (precise).

4. It says that any raised alarm has a high likelihood of being false if the probability of attack is low enough and the probability of false alarm is high enough. It is relevant to IDS because it affects the precision of the system.

Lecture 74

1. It DDOSed whitehouse.gov and defaced several sites by infecting many computers and running system code on them.

2. It used a static seed to generate random numbers so it always generated IP's from the same set. This caused it to spread slowly.

3. It resides only in RAM, so it can be wiped out by rebooting. The machine may be reinfected though.

4. It used a random seed in its number generator.

Lecture 75

1. They both exploited the same vulnerability.

2. To make preventative action against infection less effective.

3. It installed a backdoor on machines so that they can be used as zombies for future use.

4. It was not memory-resident so rebooting the machine would not get rid of it.

Lecture 76

1. It endows the product with some level of trustworthiness.

2. It has a set of requirements for secure functionality, a set of assurance requirements needed to establish the functional requirements, a methodology for determining that the functional requirements are met, and a measure of trustworthiness as a result.

3. The fact that they are physical devices requires that they be tamper-proof.

4. Level 1: has to have at least one approved algorithm or function.
Level 2: Tamper-evident packaging.
Level 3: Strong tamper-resistance and countermeasures.
Level 4: Complete envelope of protection including immediate zeroing of keys upon tampering.

Lecture 77

1. A system by which to evaluate security software and devices that can be used by anybody.

2. It is an open standard.

3. Some nations may have more stringent requirements than others.

4. A PP is a description of a family of products, while a ST is a document that contains the security requirements of an individual product.

Lecture 78

1. It is a method of assuring that the correct homeowners are charged for their garbage collection service.

2. Authentication mostly. The right people have to be charged for the right garbage.

3. It is a method of ensuring that all security objectives are being handled.

Lecture 79

1. Assuring that no untrusted users can use the system and that OS timestamps are accurate.

2. It is specific to a particular system rather than a set of systems with similar properties.

Lecture 80

1. They are levels of security certification that represent different levels of rigor in system design and implementation.

2. National institutions.

3. The tests are conducted on a national basis, so higher EAL's assigned by other countries may be there to trick other nations into using compromised systems.

4. No, otherwise the certification would have no trustworthiness or meaning.

5. The code may be obscured, so the interpretation of the model used may be misclassified. The process isn't predictable reliable.