Name: Terry Liang
EID: twl378
CS Login: tliang
Email: liang810612@hotmail.com

Assignment 5

Lecture 66

1. PGP is an email encryption that is extremely strong and uses the best available cryptographic algorithms as building blocks and yet it is easy to use.
2. Zimmermann had a strong distrust of the government, and believed strongly that everyone had an absolute right to privacy.
3. I suppose from the cases provided in the slide.
4. Because the free version of PGP might has been modified by someone for malicious purpose.

Lecture 67

1. The sender creates a message and give it a hash value and signs the hash with his private key and prepends result to the message. The receiver can use his public key to verify the signature and recover the hash code. Later, the receiver can generate a new hash code for M and compare with the decrypted hash code.
2. The sender creates a message M and a random session key K. the message is encrypted with K. and K is encrypted using recipient's public key and prepend to the message. Recover uses his private key to recover the session key that is used to decrypt the message.
3. Apply the authentication step to the original message and confidentiality to the resulting message.

Lecture 68

1. Compression, email compatibility and segmentation
2. for a well engineer purpose to save space.
3. So the signature does not depend on the compression algorithm
4. It takes a standard 3 octets and turn into 4 ascii character. The radix-64 is needed because email systems would choke on certain bit strings they'd interpret as control commands.
5. Email systems often restrict message length. Longer messages must be broken into segments which are mailed separately.

Lecture 69

1. Session keys, public and private keys, and passphrase generated keys.
2. It is associated with a single message and used only once.
3. the encryption algorithm E is used to generate a new n-bit key from a previous session key and two n/2-bit blocks generated based on user keystrokes.
4. An odd number n of sufficient size is generated and tested for primarily. If it is not prime, then repeat with another randomly generated number, until a prime is found.
5. It is protected by the passphrase system. It is necessary because the security of the system depends on protecting private keys.

Lecture 70

1. It would see a likely unique ID for the user.
2. Timestamp, Key ID, public key, private key, User ID
3. Timestamp, key ID, public key, User ID
4. It uses the Key ID field in the session key component of the message as an index.
5. It indicates the extent to which PGP trusts that this is a valid public key for this user.
6. The owner issues a signed key revocation certificate. Recipients are expected to update their public-key rings.

Lecture 71

1. The consumer problem is the attacker gets logically between the client and service and somehow disrupts the communication. The produce problem is the attacker produces and offers or requests so many services that the server is overwhelmed. The producer problems are more prevalent.
2. The transaction may involve some handshake; the attacker does not respond and the server ties up resources waiting for a response.
3. The first could consume considerable resources, the second might disallow connections by slower clients, the third may be hard to determine.

Lecture 72

1. It can detect patterns of identifiers in the request stream and block messages in that pattern.
2. IDS can analyze traffic patterns and react to anomalous patterns. IPS attempts to prevent intrusions by more aggressively blocking attempted attacks.
3. Over-provisioning the network and will have too many serves to be overwhelmed.
   Filtering attack packets and somehow distinguish the attack packets from regular packets.

Slow down processing will disadvantage all requestors, but perhaps disproportionately disadvantages attackers.

Speak-up solution requests additional traffic from all requestors.

Lecture 73

1. False negatives is a genuine attack is not detected. False positives is harmless behavior is mis-classified as an attack. I think the false negatives would cause bigger problem.
2. Accurate means if it detects all genuine attacks. Precise if it never reports legitimate behavior as an attack.
3. When you build both accuracy and preciseness in the IDS, it is almost impossible because you need to worry about everything.
4. It is an error in thinking. Because the only 1% are actually attacks and the detection accuracy of your IDS is 90%.

Lecture 74

1. It generate a list of IP addresses and attempt to infect those machines. It also launch a DoS flooding attack.
2. It has the static seed, and it could be disinfected by rebooting the computer.
3. It can be erase when rebooting the computer.
4. It uses the random seed in the random number generator.

Lecture 75

1. It exploits the same vulnerability as CodeRed.
2. It uses a much more sophisticated propagation strategy.
3. It tries to install a mechanism for remote access to the infected machine.
4. Those are really likely that the CodeRed can reapeatly attack on those machines.
5. We are lousy about patching our machines.

Lecture 76

1. It provides a standardized process of independent evaluation by expert teams to provide a certified level of confidence for security products.
2. a set of requirements defining security functionality, a set of assurance requirements needed for establishing the functional requirements, a methodology for determining that the functional requirements are met, a measure of the evaluation result indicating the trustworthiness of the evaluated system.
3. Because they are used for different purpose.

4. The first one is basically is for normal family, and level 4 is probably for the military or government.

Lecture 77

1. It contains the policies and evaluation methodology, country-specific evaluation methodologies.
2. It is adopted by some 26 countries.
3. Some countries have specific need to secure systems evaluation.
4. PP is a description of a family of products in terms of threats, environmental issues and assumptions, security objectives, and requirements of the Common Criteria. The security target is a document that contains the security requirements of a product to be evaluated, and specifies the measures offered by the product to meet those requirements.

Lecture 78

1. It illustrates the components of a protection profile. It doesn't relate to any specific product, but describes what security means for a particular class of systems.
2. It provides a systematic way of deciding whether threats and assumptions are being addressed by mechanisms and requirements.
3. IT a mapping from threats to assumptions to security objectives.

Lecture79

1. Mapping of security requirements to sub functions. Assurance measures provided by the vendor.
2. The policy may be specified fresh or as previously evaluated protection profiles. The ideas is to specify what security means for this product and how the product enforces that notion of security.

Lecture 80

1. It defines the care with which the product was developed and the rigor of the evaluation process.
2. It is performed by independent labs in each country.
3. The standard of the evaluation might be different in higher level.
4. No. The vendor could raise the level however they want then.
5. Because it would not be an effective to evaluate the product.