Name: Tolu Kalejaiye
UTEID: tok76
CSUserID: tok76

HOMEWORK 5

Lecture 66

1. It's an encryption algorithm that's almost as strong as military grade encryption.
2. He distrusted the government and believed that civilians should be able to keep their information private.
3. It provides very effective security. Secure to the point that the government didn't want it developed.
4. Perhaps it comes packaged in a manner that's easier to use through a company.

Lecture 67

1. The authentication protocol uses a hash to encode the message, and also encodes the private key. The receiver uses the public key to get the private key and then decode the message.
2. The confidentiality protocol encrypts the message and the key, and the receiver has to decrypt the key to then use it on the message.
3. Apply the authentication step to the original message, then the confidentiality step to the resulting message.

Lecture 68

1. Compression, email compatibility, and segmentation.
2. It reduces redundancy in the message, which strengthens encryption.
3. Signing first makes sure the signature doesn't rely on the encryption, and compression before encryption reduces redundancy in the message, strengthening encryption.
4. It masks groups of 3 octets in a message into 4 ASCII characters. It is needed because some email systems would interpret certain octets as control commands and choke.
5. Emails often restrict message length, so a message may need to be broken up into segments and then reassembled at the receiving end.

Lecture 69

1. Session keys, public and private keys, and passphrase generated keys.
2. They have to be generated once per message.
3. Depending on the encryption algorithm chosen, an n-bit key is chosen and used to create two blocks of size n/2. The blocks are encrypted using the algorithm and the previous key, and a new key is generated.

4. The keys would be generated at a high number(around > 200 bits) then tested for primality. If prime, they are eligible.
5. It is encoded using bits of the hash key. It's important because you don't want the private key to be publicly available.

Lecture 70

1. He/she could do as PGP does, and use a section of the key as the user's ID.
2. A timestamp, key ID, public and private key, and User ID.
3. A timestamp, key ID, public key, and User ID.
4. You retrieve the encrypted key using the key ID, then recover the session key and decrypt the message, after being given the correct passphrase by the user.
5. It is the extent to which PGP believes the public key is valid for the user.
6. The owner issues a signed key revocation certificate.

Lecture 71

1. The consumer problem involves the attacker simply getting in the way of communication between the client and server. The producer problem is a direct attack on the server by attempting to overload it.
2. In syn flooding, the server begins a handshake protocol with the client, but when the client doesn't respond, it waits, and ends up backing up the system, as many more of these requests are coming in as well.
3. They would either take too many resources and be too hard to execute, or disadvantage those with slower but legitimate connections.

Lecture 72

1. Because it is able to detect patterns of identifiers in a stream and block them.
2. Intrusion prevention systems aim to stop the intrusion from ever happening by attempting to identify incoming traffic. Intrusion detection systems can only react to anomalies witnessed in the traffic patterns.
3. Overprovisioning the network: Have an unreasonably large amount of servers. Filtering attack packets: Detect which packets are not regular. Slow down processing: slow down processing power of servers and take fewer requests. "Speak Up" Solution: Increase all requests and detect which servers aren't giving any more requests. Those will be the bots.

Lecture 73

1. A false positive is wrongfully calling a non-threat a threat. A false negative is not detecting the threat. A false negative would be worse, as the danger of a threat is worse than misclassifying a non-threat.
2. Accurate means no false negatives. Precise means no false positives.

3. The problem isn't achieving one of the two, the problem is being able to do both, as their goals can interfere with each other.
4. This measures the probability of a system raising a false alarm. It's important to help better the IDS system.

Lecture 74

1. It attempted to execute a DoS attack on ww1.whitehouse.gov.
2. It was ineffective because it was generated using a static seed.
3. Memory resident worms reside in memory and all one has to do to get rid of it(at least temporarily) is reset their machine.
4. The second version used a random seed.

Lecture 75

1. It exploited the same feature.
2. Because the worm remained dormant, they would have a longer time to incorporate more machines into the network before even being realized. By the time an attack happened, it would be too devastating.
3. It attempted to get a backdoor into several machines, so as to use them as zombies for a future attack.
4. They remain vulnerable to further attacks.
5. They found that in many cases, the software to prevent an attack already exists. People just aren't using it.

Lecture 76

1. To prevent attacks
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. Perhaps they require much more rigorous evaluation.
4. Level 1: basic security; at least one approved algorithm or function.
   Level 2: improved physical security, 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 shared criteria on secure systems evaluation.
2. It's used by about 26 countries.
3. Different countries may have different laws and objectives.

4. A protection profile is a family of products in terms of threats, objectives, and requirements of the public profile. A security target pertains to just one target of evaluation, and its requirements.

Lecture 78

1. The goal of the protection profile is to ensure that wrong data is not submitted to the database.
2. To detect invalid tags, detect incorrect weight info, and deal with fault tolerance.
3. It's a visual representation of who is in a position to affect each threat or vulnerability.

Lecture 79

1. The overall goal is to ensure that only authorized users can use the system, and that those authorized users cannot perform unauthorized actions.
2. A security target evaluation isn't as extensive as a protection profile, and analyzes one thing more closely, as opposed to blanketing several categories.

Lecture 80

1. They are evaluation levels used to categorize a security product.
2. These are performed by a recognized, independent evaluating body.
3. Higher EALs would most likely be used for things that are of a high sensitivity. Most countries wouldn't want to use foreign technology to protect their own secrets.
4. No. Because they can lie.
5. Because then you know how it works and can infiltrate it.