Name: Ridwan Hoq
EID: rmh2376
CS Login: ridwan
Email: ridwanhoq@gmail.com

Lecture 66

1. Pretty Good Privacy, a security protocol
2. Because solutions at the time were pretty bad and the government could crack them
3. Yes, from a variety of standpoints
4. To continue development and ensure that the level of quality remains good

Lecture 67

1. PGP authentication is as follows:
    a. Sender creates a message M
    b. Sender generates a hash of M
    c. Sender signs the hash with private key and prepends the result to the message
    d. Receiver decrypts the hash with sender's public key
    e. Receiver generates a hash of M and compares it to the decrypted hash from sender
2. PGP confidentiality is as follows:
    a. Sender generates a random session key K and encrypts message M with it
    b. K is encrypted with Recievers public key and then prepended onto M
    c. R decrypts K with its private key and then uses K to decrypt M.
3. Do both protocols

Lecture 68

1. Compression, email compatibility, segmentation
2. Compression is needed to reduce bandwidth usage for sending messages over the internet
3. So the decryption protocol doesn't depend on the compression algorithm
4. Radix 64 is needed for email encryption
5. Segmentation is needed to break up the message

Lecture 69

1. There are four kinds used by PGP
2. Sessions have special properties
3. Session keys are generated by the unique random number generator similar to UUID
4. RSA keys and session keys are generated in the same way.
5. Private keys are protected so that no one can impersonate somebody

Lecture 70

1. He tries every single combo until he unlocks it
2. All your private keys are there
3. All your public keys are there
4. You just pop the key off
5. To ensure the key is legitimate from the correct source.
6. You generate a new key so that old keys don't work anymore

Lecture 71

1. Consumer problems have to do with consuming things that should be secure where as producer problems have to do with producing things that should be secure.
2. Syn flooding is when you flood everything in your message with synergistic synergy.
3. Because they're not time efficient or space efficient.

Lecture 72

1. Filtering thru all packets could ascertain which packets are harmful
2. Intrusion detection is when intrusions are detected where as intrusion prevention prevents intrusions
3. There's a couple of ways to DDOS which means there is a DDOS here and a DDOS there and there's a DDOS every where.

Lecture 73

1. False positive is when you think something is penetrated but its not, false negatives is when you think something doesn't penetrate but it does. It depends on the situation.
2. Accuracy is when something is close to the correct value but precision is when you repeatedly get the same value
3. You can't have both
4. Base rate fallacy is the argument that the base rate is either accurate or precise but not both

Lecture 74

1. Determine when something has gone wrong
2. It didn't do that well enough
3. A worm is memory resident when it saves itself into memory
4. It prevented memory resident worms

Lecture 75

1. It improved upon previous version by a large degree since it was more robust and powerful
2. To better solve the problem of worm holes in space which wasn't prevented before
3. Code Red II was all about the prevention of security since it was there
4. That would effect the efficacy of the algorithm
5. They learned that Code Red protocol wasn't enough to prevent what they needed to prevent

Lecture 76

1. To ensure that everything is double checked by a third party
2. You have to evaluate many aspects of a program/app like its input, its output, and how it saves data
3. You need a seperate evaluation mechanism for crypto to take into account for the cryptography which throws off the whole evaluation from before
4. There are four levels for the certification process.

Lecture 77

1. The common criteria is the criteria in which all apps must meet
2. Since all programs have input/output then it must meet the criteria for those aspects
3. National schemes determine security based on a nation's laws

4. Protection profile specifies data for each object being protected, whereas a security target marks out which targets might be infilitrated.

Lecture 78

1. There is an overall goal for the protection profile of WBIS
2. There are various parts of the protection profile of WBIS
3. The matrix identifies the various parts and how they contribute the overall goal

Lecture 79

1. Sun identitiy manager manages identities because it has the ability to do so.
2. There's quite a bit of difference in between the two types so it should be pretty clear to be honest.

Lecture 80

1. EALs are not even close to being correct even though they might mean something to someone.
2. Common Criteria is evaluated by an independent third party since most places are aware of the common criteria.
3. They are not recognized by people since it is not prevalant.
4. No since they cannot be trusted to secure their own things.
5. Because it may not be an accurate representation of the model.