**Lecture 66**

1. Pretty Good Privacy, used best available encryption algorithm.

2. He wanted to develop an encryption system that the average Joe could use

3. Yes, the FBI, government, and Italian police couldn’t crack it

4. Despite being free, it is offered for sale because some companies don’t want freeware (need a service to call on incase something goes wrong)

**Lecture 67**

1. Authentication: The message sender signs the hash of the message with the private key, which is appended to the entire message.

2. Confidentiality: The sender generates the message and a session key (symmetric encryption) and encrypt the key with the using the receiver’s public key.

3. To get both authentication and confidentiality just put both of those steps together

**Lecture 68**

1. PGP also offers compression, email compatibility, and segmentation
2. To increase the amount of data you can transmit (bandwidth)
3. So that the encryption algorithm doesn’t have to depend on the compression.
4. It makes sure there aren’t any weird characters or symbols. Makes every character in the system an ascii character.
5. Segmentation breaks the message into pieces, so that the mailers can handle all message sizes

**Lecture 69**

1. Session key, public key, private key, and passphrase based key
2. They need to be randomly generated and have high entropy
3. From keyboard input and mouse movement
4. RSA is used for PGP asymmetric encryption. Keys are generated using prime numbers
5. The private keys protected by encrypting them with a passphrase and storing them in a hash function

**Lecture 70**

1. Have the sender send the public key with the message, associate a unique ID with each sender so we know which key to use, or generate an ID for the pair (based on the last 64 bits of the message).
2. Your own private key and fields to help identify them (timestamp, key ID, public key, private key, and user ID)
3. Public key ring includes timestamp, key ID, public key, user ID
4. It uses the keyID field to identify the user and the passphrase to recover the private key
5. To determine the legitimacy of the certificates and chains
6. The key can be revoked by sending out the revocation certificate (for outdate or untrusted keys)

**Lecture 71**

1. Consumer problems: the attacker gets logically between the client and service and somehow disrupts the communication

producer problems: the attacker produces offers or requests so many services that the server is overwhelmed.

1. syn flooding: relying on the properties of a TCP 3 way handshake to overflow the server. By sending syn messages, it forces the server to not send back ack messages to the point where no clients can reach the server
2. The first three solutions to syn flooding not ideal because 1) increasing server size can still be overflowed by more requests, 2) shorter timeouts disallow slower connections (DoS), and 3) filtering suspicious packet may be hard to determine.

**Lecture 72**

1. Because it prevents some bad packets from getting to the system while letting good ones through. (commonly achieved through a firewall)
2. Intrusion detection analyzes the environment and reacts after the attack has begun, and intrusion prevention systems attempt to block attempted attacks?
3. 1) Have extra servers so they can’t be overwhelmed, 2) filter out the bad packets, 3) slows down the processing, 4) request additional traffic from all requestors.

**Lecture 73**

1. False negative: don’t detect an attack. False positive: wrongly identify behavior as an attack. False negative is probably more dangerous
2. Accurate means that it detects all genuine attacks (false neg), precise means it never reports legit behavior as an attack (false pos)
3. It’s difficult to pick up all attacks and ignore all other behavior perfectly. You have to have a perfect balance. Most systems are either overly protective or open.

4. A formula to determine what probability you would get either false positives or negatives. This is relevant to IDS in that it shows you what percent of the time your flag picks up a false positive

**Lecture 74**

1. Code Red version 1 attempt to cause a DDoS attack on Microsoft IIS servers by using IP addressing collected from the first 20 days of the month
2. Code Red version 1 ineffective  because the attack could only reach the first few machines in a system
3. To say that a worm is “memory resident” means that the attack was in the volatile memory of the machine, which could be removed by rebooting
4. Code Red version 2 much more effective than version 1 because  it used random seeds to reach more machines, and reached other devices such as routers and printers

**Lecture 75**

1. Code Red II was related to Code Red (versions 1 and 2) in that it installed backdoor malware on the system and tries to run itself.
2. Code Red II incorporated its elaborate propagation scheme to remain random and to be more difficult to detect. This also allowed it to reach more machines
3. Code red installed a remote login feature and attempted to run backdoor malware on the machine.
4. There is a large number of unpatched machines still out there, leaving open grounds for the attack to keep occuring
5. The report from Verizon says that 9/10 of compromised customers could have patched the system 6 months before the attack occurred.

**Lecture 76**

1. So that one entity can judge how secure each system is and what its good for. They have a set of requirements and standards

2. They are a methodology for determining that the functional requirements are met, indicating the trustworthiness of the system.

3. Because they each have different functions and have independent compliance/conformance levels

4. 1) basic security functions, 2)improved physical security, tamper evident packaging, 3) tamper-resistant and countermeasures, 4) complete protection including immediate zeroing of keys upon tamerping

**Lecture 77**

1. Common Criteria has been adopted by 26 countries, and compromises of documents and evaluation methods

2. The commonality arises in that the 26 countries use the same evaluation methods, documents and even have country specific requirements to follow by

3. Why would there be any need for “National Schemes”?

4. a protection profile is a set of implementation independent security requirements for a category of products or systems, and a security target evaluates products or systems against a security target

**Lecture 78**

1. The overall goal of the protection profile as exemplified by the WBIS example is a system were ID tags are put in trash containers, and then the trash turcks bills for the trash by weight. Info is transmitted by short radio signal
2. the purpose of the various parts of the protection profile are to insure that the message is transferred with authorization and is trustworthy. The access to the system must be protected, and the operator must check that the transfers are complete (access control of records).
3. the purpose of the matrix is to shows threats/assumptions and the security objectives/system requirements. If every row has an X, then you know that every threat or assumption has some mechanism to counter it

**Lecture 79**

1. The overall goal of the security target evaluation as exemplified by the Sun Identity Manager example is a product for managing user access privileges stored in directory services.
2. a security target evaluation differs from a protection profile evaluation in that a security target evaluation analyzes the system for vulnerabilities and a PP looks at the specific attackers

**Lecture 80**

1. EALs are levels of rigor that the security is assured to be safe, and they are used for certificates of security
2. The government (NIST in the US) performs the Common Criteria evaluations up to level 4
3. Various countries do not necessarily mutually recognize the higher EALs because certain countries see security strength in different terms. It is also difficult to classify the difference between levels when the system is that good.
4. No.  Evaluations are performed for a fee by commercial labs and are certified by the NIST.
5. If you’re performing a formal evaluation, you shouldn’t reverse engineer the model from the code. Only formal mathematical methods should be used