Emily Ngo

Emn367

Ngo.emily@utexas.edu

Lecture 66

1. A strong encryption to everyone in the form of an email encryption system; PGP is the closest you're likely to get to military-grade encryption.
2. A strong distrust of the government, and believed in right to privacy.
3. Yes, the encryption was difficult to decrypt for several governments due to the high quality algorithms used.
4. Some companies want the option to have maintenance.

Lecture 67

1. A message is hashed and encrypted with a sender's private key and that messaged is sent to receiver; receiver then decrypt with sender's public key and generates a hash to compare message.
2. Take a message, then generate a new message and session key; encrypt message with key and encrypt key with recipient's public key. The receiver can then use his private key to recover the session key to decrypt with.
3. Apply authentication protocol to original message, apply confidentially protocol to result message.

Lecture 68

1. Compression, Email compatibility, segmentation.
2. To save bandwidth
3. Don't want the signature to depend on the compression algorithm; you want the original message to be signed to be authentic and then encrypted.
4. A transformation that takes 3 bytes and expands it into 4 bytes to prevent form feeds to be interpreted as control commands.
5. Breaks message into segments so emails systems can handle the message length.

Lecture 69

1. Session key, public keys, private, passphrase-based keys.
2. It is associated with a single message and is only used once.
3. A new n-bit key is generated by using the previous key and two n/2-bit blocks generated based on the user keystroke and timing. The blocks are encrypted with the algorithm and previous key and combined to form the new key.
4. An odd number n is generated and tested over and over for primality until it is prime.

5. With a passphrase to encrypt the private key with. This way every access to the private key requires the passphrase so not everyone has access to it and is another layer of security for attackers.

Lecture 70

1. Generate an ID likely to be unique for a given user (the last 64 bits of the key) which allows the receiver to verify that he has such key on his “key ring”.
2. Timestamp, key id, public key, private key, user id
3. Timestamp, key id, public key, user id
4. PGP gets key from private key ring using the key id field in the session key component of the message as an index. User puts passphrase in, and session key is used to decrypt the message.
5. The trust or extent of trust PGP has for a public key for a certain user via certificates.
6. Owner issues a signed key revocation certificate which is advising others not to use that key.

Lecture 71

1. Consumer problem is when the attacker gets between the client and service and disrupts the communication. The producer problem is the attacker produces, offers, or request a lot of servicers that the server is overwhelmed.
2. The attacker requests a lot of service which requires the attacker to respond to a protocol, however the attacker does not respond and uses up resources from the server because it is waiting for a response.
3. Either they will use up more resource, throw away possible clients, or disadvantage slower clients which does not solve the problem.

Lecture 72

1. If you can distinguish bad packets from the good you won’t be turning away any potential customers/ legit requestors. However, an overly aggressive filter might turn away too many legit requests.
2. Detection analyzes the patterns and react to fishy patterns, prevention attempts to block intrusion by aggressively blocking attempted attacks assuming they are identified
3. Over provisioning is having a lot of servers so they aren’t ever overwhelmed if there is an attack, filtering attack packets might not be possible but filtering out malicious packets, slow down makes all the requests going in slower so they are manageable, speak up asks legit requestors to increase traffic to outdo the traffic of malicious request.

Lecture 73

1. False negative is an attack not detected, false positive is a harmless behavior that is seen as an attack. It depends on the situation which would be worse.
2. Accurate means the IDS never has a false negative, precise means it will never have a false positive.

3. You can have an IDS that never has any false positives or one that never has any false negatives.
4. If attacks are rare the IDS has to be highly accurate to be useful.

Lecture 74

1. Generated a random list of IP to attack.
2. The static seed made the same list of IP to attack again, hence a static list.
3. It resided in the memory of your machine. A machine can be disinfected by reboot.
4. It had a random seed, it also attacked additional devices like routers or printers which had a effect on the internet.

Lecture 75

1. The author of 2 might not be related to code red 1 at all, but he knew about code red 1.
2. It is made to attack or propagate addresses that are more likely to exist in a subnet.
3. Installs remote access to a machine
4. In that population with high unpatched means the worm will continue to circulate.
5. We should patch and be less vulnerable the more people that are vulnerable overall makes the internet vulnerable too.

Lecture 76

1. To assure the purchaser and it is also a gain for the vendor.
2. A set of requirements defining security functionally, set of assurance requirements needed for establishing the functional requirements, a methodology for determine that the functional requirements are met, and a measure of the evaluation.
3. They don’t want people abusing crypto products, and also there are different levels of cryptography.
4. Level 1 is basic single algorithm, 2 improved package, 3 strong tamper-resistance, 4 complete envelope of protection.

Lecture 77

1. A Criteria that would allow a product to get approved in multiple countries.
2. It unifies the separate evaluation that each country had.
3. At higher levels it might not be as useful but at lower levels it saves time and effort when a scheme can be accepted across multiple countries.
4. ST is the policies that you are evaluating for a system, PP is a set of requirement for a category of products or systems.

Lecture 78

1. The records recorded by the truck to compute the transaction to be accurate and protected from being destroyed.

2. What general classes of mechanisms you need for a class of product or systems, so it tells you want needs to be done but not how.
3. Matrix will show that all the threats have a corresponding counter measure, a systematic way to see if your mechanisms are adequate.

Lecture 79

1. To identify all the threats and what security means for that system and how the system satisfies it.
2. The ST might target threats specifically for that product however might also match the PP evaluation.

Lecture 80

1. Specifies how rigor the evaluation would be; the different level of assurance available.
2. Government of the country or certifying agency (independent party).
3. At higher levels the data gets more sensitive so for governments might feel less ready to accept the common criteria.
4. No then they can just rate it however they want with a bias.
5. Means that it is possible for someone else to reverse engineer it and expose it.