Haoshu Yuwen
Hy2892

Assignment 5

Lecture 66:
1. PGP is the closest you will get to military grade security in email encryption and is accessible to all.

2. He did not trust the government.

3. Yes

4. Better support I'm guessing.

Lecture 67:
1. Sender sends a hashed message encrypted with his own private key, hence authenticating the sender.

2. Sender encrypts with receiver's public key, hence only receiver can read the message.

3. Combining 1 and 2.

Lecture 68:
1. Compression, Email compatibility, and Segmentation

2. The encryption process actually expands the message so for efficiency reasons, compression is done.

3. Signing a compressed message would depend too heavily on the compression algorithm.

4. Because many email systems choke on certain bit strings and these must be modified.

5. Many email systems are limited in size.

Lecture 69:
1. Session, public, private and Passphrase based.

2. Unique.

3. Using encryption algorithm E, the previous key, and two n/2 bit blocks generated based on user keystrokes.

4. Odd number is generated. If it's not prime, try again until we get one.

5. With a user passphrase since the security of the whole system depends on the private and public keys.

Lecture 70:
1. Key rings

2. Timestamp, key ID, public key, private key, User ID, all in the rows of a table.

3. Timestamp, key ID, entry public keys, User ID of the owner of the key, all In the rows of a table.

4. PGP uses Key ID field in the message to retrieve encrypted private key from receiver's private key ring, decrypts using prompted password, recovers the session key and decrypts the message.

5. indicates how much an individual trusts that key.

6. Owner issues signed key revocation certificate and receivers update their key rings.

Lecture 71:
1. Consumer problem is basic communication disruption. Producer problem is a denial of availability to the consumer.

2. Attacker forces server to wait for a response, which dries up the server.

3. Could affect legitimate users negatively.

Lecture 72:
1. It's very broad.

2. The detection system still allows the intrusion to happen while theoretically the prevention system does not.

3. – Make it so your server is so robust it can easily handle the massive amount of requests.
- Ignore phony requests
- Makes processing slower which affects the attacker
- Request a response from requestors. Attackers probably wouldn't respond appropriately.

Lecture 73:

1. False positive is a positive when there was nothing. A false negative is an intrusion that goes undetected. False negatives because if there are only false negatives, then you know some actual attacks went through.

2. Accurate: Low amounts false negatives.
Precise: Low false positives

3. It's really hard to be both accurate and precise.

4. Despite accuracy levels of x percent, more than x percent of raised alarms will be false. This shows how difficult it is to be accurate and precise.

Lecture 74:
1. Infect random pcs, disrupt function of whitehouse.gov, and defaced some websites.

2. Static seed -> identical machine lists per infected machine. No compensation for changing of whitehouse.gov IP address.

3. Worm ceases to function upon reboot -> very slow and short term spreading of worm.

4. Random seed -> Different machine lists -> more infected machines.

Lecture 75:
1. Code red 2 is not memory resident, installed a backdoor, and didn't do anything visually disruptive.

2. To increase infection before discovery.

3. Render hosts vulnerable for additional attacks.

4. More vulnerable machines.

5. Update your damn machines.

Lecture 76:
1. So the users know they work.

2. Set of requirements defining security functionality, set of assurance requirements needed for establishing the functional requirements, methodology for determining requirements are met, indication of trustworthiness.

3. Why not.

4. 1 – It works. 2- It’s not easily tampered with. 3- Enhancement of 2. 4- Better than 3.

Lecture 77:
1. An evaluation criteria on a national basis.

2. It’s recognized by countries.

3. Needs vary by country.

4. One’s the goal and one’s the means.

Lecture 78:
1. Provides a systematic way of deciding whether threats and assumptions are being addressed and met.

2. Protect integrity basically.

3. Similar to an ACC.

Lecture 79:
1. Confidentiality.

2. They protect slightly different aspects of security.

Lecture 80:
1. Levels of rigor for a security system used to gauge how reliable and good a system is.

2. The government of a country.

3. Different countries may have different requirements.

4. Nope. That would defeat the purpose of certification by introducing the bias wild card.

5. Inaccuracy?