CS535 **Thanga Rani Prabhu** **Week#1 /19496**

Prof.Dr.Henry Chang

Q1.

Categorization of security services
The 1997 IEEE paper "Encryption", which was submitted by Fred Piper in European Conference on Security and Detection, has this statement

Thus anyone sending a message over a public network or storing
it on a database should ask themselves:
** Am I happy for everyone else to know its contents?*
If their answer is YES then there may be no problem, but if it
is not then they may need to ask:
** How much am I prepared to pay to stop them?*
** Am I allowed to stop them?*
For transmitted messages the sender may also ask:
** Do I need ack knolwedgement of delivery?*
Similarly anyone receiving a message over a network will need to ask themselves the following:
** Am I confident to know the identity of the sender?*
** Am I happy that the message I have received is identical to the one which the originator sent?*
** Am I concerned that the sender may later deny sending this message and/or claim to have sent a different one?*

Please answer these questions related to <u>Security Service</u>:

- **Which security service can assure a sender that people other than the receiver cannot see the content of a message sent from the sender?**

  Data Confidentiality

- **Which security service can provide the identity of the sender?**

  Authentication

- **Which security service can assure the receiver that the message the receiver have received is identical to the one which the originator sent?**

  Data Integrity

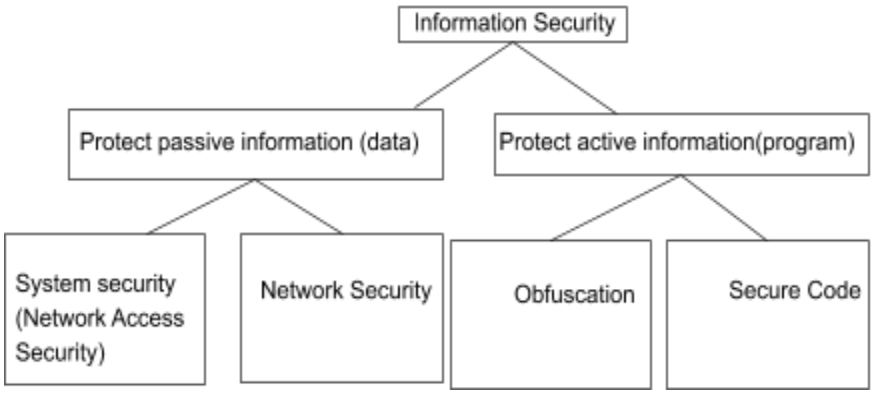
- **Which security service can assure the receiver that the sender cannot deny sending a message and/or claim to have sent a different one?**

  Non-Repudiation

Q2.

Please draw a diagram to show the tree structure relationship among the following security technologies

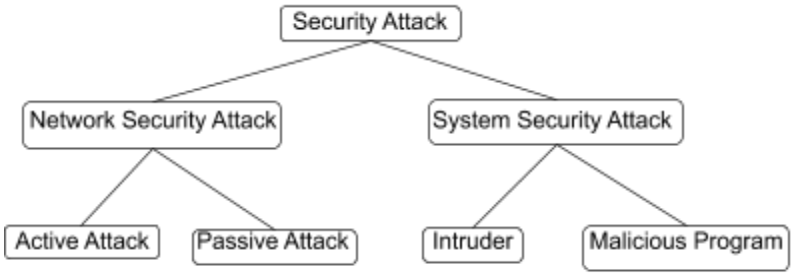
- ***Obfuscation***
- ***Information security***
- ***Network security***
- ***Protect passive information (data)***
- ***Protect active information (program)***
- ***System security (i.e., Network Access Security)***



Q3.

Please draw a diagram to show the tree structure relationship among the following attacks

- ***Intruder***
- ***Malicious program***
- ***Security attack***
- ***Passive attack***
- ***Network security attack***
- ***active attack***



Q4.

Multiple choices

1. Which US government agency is the Big Brother which controls whether a security algorithm can be exported?
    1. FBI
    2. CIA
    3. **NSA**

2. What are the three aspects of information security?
    1. Network Attack, System Attack, and Virus Attack
    2. **Security mechanism, security service, and security attack**
    3. Asymmetric Key Cryptography, Symmetric Key Cryptography and Data Mining
    4. Authentication, Confidentiality, and Integrity

3. What are the two major types of security attack?
    1. Network Security Attack, and Virus Attack
    2. System Security Attack, and Virus Attack
    3. **Network Security Attack and System Security Attack**
    4. None of above

4. Which of the following data does not need to be sent via out-of-band channel?
    1. **public key**
    2. secret key
    3. key for creating MAC

5. Who invented public key cryptography?
    1. Ray Ozzie
    2. **Diffie Whitfield**
    3. Phil Zimmermann
    4. Ron Rivest
    5. Len Adleman

6. Postcard putting inside a see-through windows envelope achieve what service?
    1. Authentication
    2. Confidentiality
    3. **Integrity**
    4. Authorization
    5. Auditing
    6. Non-repudiation

7. Human DNA corresponds to which of the following electronic security mechanism?
    1. Public key
    2. Private key
    3. **Message Digest**
    4. Symmetric key
    5. Digital certificate

8. Passport corresponds to which of the following electronic security mechanism?
    1. Public key
    2. **Digital certificate**
    3. Private key
    4. Message Digest
    5. Symmetric key