## 

## [3413CT Network Security](file:///D:\Profiles\user\My%20Documents\Teaching\Courses_2003\6216INT_03\6216inthome.html)

### **Workshop 6B**

**Reviewing the lecture notes, answer the following questions**

1. List and explain the three different types of firewalls.  
   The three types of firewalls include:  
   a. **Packet Filtering**: A set of rules are applied to incoming and outgoing IP packets . Based on these rules the packets are forwarded to the appropriate destination or discarded.  
   b. **Stateful inspection firewall**: Keeps track of the state of network connections traveling across it. Only packets matching a known active connection will be allowed by the firewall; others will be rejected.  
     
   b. **Application Level Gateway**: Acts as a relay for application level traffic. The user contacts the gateway using TCP/IP applications such as telnet or FTP, the gateway asks for user of the remote host. When the user responds with correct authentication information the gateway contacts the user on the remote host and relays the information. A disadvantage is processing overhead on each connection.  
   c. **Circuit-Level Gateway**: Works at the session layer of the OSI model, or as a "shim-layer" between the application layer and the transport layer of the TCP/IP stack. They monitor TCP handshaking between packets to determine whether a requested session is legitimate
2. What information is used by a typical packet-filtering router?  
   Source IP, Destination IP, Source and destination transport level address, IP protocol field, Interface
3. What are some weaknesses of a packet-filtering router?  
   a. Packet filter firewalls do not examine upper layer data, which means they cannot prevent, attacks that employ application specific vulnerabilities.  
   b. Limited logging capabilities due to information available at the firewall level  
   c. Most packet filter firewalls do not support advanced user authentication  
   d. Susceptible to security breaches if improperly configured
4. What is the difference between a packet-filtering router and a stateful inspection firewall?  
     
   Packet filtering looks at the packet and compares it to a set of access control rules then decides to either reject or forward the packet. It has no idea the state of the current connection between host and client. Stateful inspection knows the status of the current connection such as setup request, an existing connection, or a connection teardown request
5. List the three types of firewall configurations and explain, with the aid of a diagram, the differences among them.

a. DMZ network: a firewall placed at the boundary between a local LAN and the external Internet.  
  
[ internet ]   
 |   
 x (router)  
 |  
o-o-o-o-o-o-o-o-o (workstations)  
  
b. VPN: uses encryption and authentication in the lower protocol layers to provide a secure connection through an otherwise insecure network, typically the Internet.  
  
o-o-o-o-o-o-o-o-o (workstations)  
 |  
 x (router)  
 | | (vpn)  
[ internet ]

| | (vpn)  
 x (router)  
 |  
o-o-o-o-o-o-o-o-o (workstations)  
  
c. Distributed Firewalls: Involves a stand-alone firewall as well as a host based firewall working together under a central admin. Provide protection internally and externally.  
  
[ internet ]

|   
 x (router – external firewall)----------y (switch)------ External DMZ  
 |  
 y (switch)  
 |  
 x (router – internal firewall)  
 |  
o-o-o-o-o-o-o-o-o (workstations)

1. In the context of access control, what is the difference between a subject and an object?  
     
   Subject: an entity capable of accessing objects. Generally equates to a process that represents the user.   
   Object: a resource to which access is controlled. An entity used to contain and/or receive information. Examples include records, blocks, pages, segments, files, directories, programs, etc.
2. List four techniques used by firewalls to control access and enforce a security policy.

**Service control**: Determines the types of Internet services that can be accessed, inbound or outbound. The firewall may filter traffic on the basis of IP address, protocol, or port number; may provide proxy software that receives and interprets each service request before passing it on; or may host the server software itself, such as a Web or mail service.

**Direction control**: Determines the direction in which particular service requests may be initiated and allowed to flow through the firewall.

**User control**: Controls access to a service according to which user is attempting to access it. This feature is typically applied to users inside the firewall perimeter (local users). It may also be applied to incoming traffic from external users; the latter requires some form of secure authentication technology, such as is provided in IPSec ( Chapter 22 ).

**Behavior control**: Controls how particular services are used. For example, the firewall may filter e-mail to eliminate spam, or it may enable external access to only a portion of the information on a local Web server.

**Questions for Revision:**

1. Explain the following terms.
   * Computer security: Information security as applied to computers and networks.
   * Network security: Study of usability, reliability, integrity, and safety of your network and data
   * Internet security: branch of computer security specifically related to the Internet, often involving browser security but also network security on a more general level as it applies to other applications or operating systems on a whole.
   * Information systems security: Protection of information systems and the information housed on them from unauthorized use or threats to integrity.
   * Confidentiality: Information transmitted is only accessible for reading by authorized parties.
   * Authentication: Originator of message is identified with assurance the identity is not faked.
   * Integrity: Only authorized parties are able to modify computer system assets and transmitted information.
   * Non-repudiation: Neither the sender nor the receiver can deny the transmission of a message
2. Differentiate between the following terms:
   * Block cipher **/** stream cipher: Block cipher processes plaintext in chunks while a stream cipher will process the data in a bit per bit (sometimes byte).
   * Private-key cryptography **/** public-key cryptography: Private key is hidden from the public and usually used as a signature in asymmetric encryption. Public key is revealed to the public and can be used to encrypt or decrypt messages.
3. Explain the structure and operation of the Feistel cipher.

Inputs of this encryption algorithm are a plaintext block of length 2w bits and a key K. The block is divided into 2 halves L and R. Both halves go through n rounds of processing and then combine to produce a cipher text block. Each round uses the previous round as well as a subkey derived from the overall key K. The subkeys are different from the original key and other subkeys.  
  
During each round a substitution is performed on the left half of the data. The right side goes through a ‘round function’ and then the output is XORed and with the left half of data. Each round is different because they are fed subkeys.  
  
Finally, a permutation takes place that interchanges the two halves of data.

1. Compare DES and AES in terms of data-block length and key size; and explain why AES is more secure than DES.   
     
   DES: Data Encryption Standard: 64 bit blocks with 56 bit keys.  
   AES: Advanced Encryption Standard: 128 bit blocks with 128/192/256 bit keys.  
     
   AES is more secure because it uses larger key sizes and larger block sizes.
2. RSA algorithm is very useful in many commercial systems. Would you think RSA will replace AES? Why or why not? Differentiate between AES and RSA.   
     
   RSA will not replace AES because asymmetric encryption has a larger processing overhead compared to symmetric encryption. Each form of encryption has applicable situational uses and some are better applied than others in certain situations. This is why I do not believe RSA will replace AES.
3. Explain how a pair of users, say, A and B, can exchange a secret session key Kthrough a publicly available channel, making useof public-key cryptography, preventing any unauthorized party from learning the session key.   
   - User A generates a public/private key pair  
   - User A encrypts session key K with private key  
   - User A shares public key  
   - User A sends encrypted session key to user B  
   - User B decrypts session key with public key  
   - User B encrypts message with session key and can now communicate with A
4. Explain the requirements of hash functions for security purpose; and explain how a hash function is used in digital signature creation and verification.

Hash functions are used for message authentication. The hash is generated from the message and encrypted with a private key and then concatenated to the message and sent to the receiving end. Another hash is then generated from the message and then compared to the decrypted concatenated hash, which is decrypted using the public key.

1. Given a piece of message M and a hash function H, briefly describe the processes of signature creation and verification with the ElGamal scheme.
   1. The hash ***m = H(M)*, *0 ≤ m ≤(q-1)***
   2. Choose random integer **K** with **1 ≤ K ≤(q-1)** and **gcd(K,q-1)=1**
   3. Compute the value: **S1 = ak mod q**
   4. Compute **K-1** the inverse of **K mod (q-1)**
   5. Compute the value: **S2 = K-1(m-xAS1) mod (q-1)**
   6. Signature is: **(S1,S2)**
2. Explain how PGP encrypts and decrypts message for data confidentiality.

Message contents are hidden from someone who does not have access to the PGP private key. A session key is generated; the message is encrypted with a session key. Then public key is used to encrypt the session key and concatenated onto the message. Private key is used to decrypt the session key, which is used to decrypt the contents of the message.

1. Answer the following questions on PGP key identifier: (1) Why does PGP associate an identifier with each public key? (2) How does PGP create a key identifier for a given public key? (3) Why isn’t it necessary to associate an identifier with a private key, given an identifier to the corresponding public key?   
     
   1) To differentiate which public key was used to encrypt the session key  
   2) The least significant 64 bits of the public key contain the key ID  
   3) Being able to identify the public key ID, you are able to find the private key because the private and public keys are paired on the private key ring.
2. Answer the following questions on S/MIME: (1) What is S/MIME? (2) Compare PGP and S/MIME in terms of key-management procedures.   
   1) S/MIME stands for Secure Multipurpose Internet Mail Extension and was designed to provide a set of extended features on top of basic 7 bit ASCII e-mailing such as adding attachments, increasing message size, support for full 8 bit ASCII values, etc.  
     
   2) PGP uses a key ID that is attached to the least 64 bits of the public key. SMIME uses a certificate storage/retrieval system to a local list of certificate in order to verify incoming signatures to encrypt outgoing messages.
3. Answer the following questions: (1) What is IPsec? (2) What are some basic security services provided by IPsec? (3) Explain what Security Policy Database (SPD) is in IPsec.

1. Additional transport layer infrastructure that encrypts payload data for safe transmission.  
2. Services provided by IPSec: Access control, connectionless integrity, data origin authentication, rejection of replayed packets, confidentiality, limited traffic flow confidentiality.  
3. The means by which IP traffic is related to specific SAs (or not SA in the case of traffic allowed to bypass IPSec) is the nominal Security Policy Database (SPD). SPD contains entries each of which defines a subset of IP traffic and points to an SA for that traffic.

1. Explain the two procedures in IP traceback: marking procedure and path reconstruction procedure.   
   Marking procedure:  
   -by routers  
   -add information to packet  
     
     
   Reconstruction Procedure:  
   - by victim

- use information in marked packets

1. Answer the following questions on web security: (1) What is SSL? Explain the protocols that comprise SSL. (2) Explain what SSL connection and SSL session are, and the differences between them. (3) What is SET? (4) Explain what a digital envelope in SET is, and how a digital envelope is produced.   
   1. SSL (Secure Socket Layer) is an encrypted link between a web server and browser. To be able to create an SSL connection a web server requires an SSL certificate. SSL provides basic security services to high layer protocols such as HTTP.  
   2.SSL Connection: A transport that provides a suitable type of service. Every connection is associated with a session. The connection is transient.  
   SSL Session: An association between client as server. Sessions are created using the handshake protocol. Sessions define a set of cryptographic security parameters, which can be shared among multiple connections. Sessions are used to avoid expensive negotiation of a new security parameter for each new connection.   
   3.SET: open encryption and security specification designed to protect credit card transactions on the Internet.  
   4. A digital envelope is a session key that has been encrypted with a public key. It is comparable to an envelope because it must first be opened before the contents of a message can be seen.
2. Answer the following questions on password management and protection: (1) Explain the two useful techniques for password file protection. (2) What is “salt” in the context of UNIX password management? How does it increase security for password authentication? (3) Explain the Markov model for efficient password checking.   
     
   1. Access control list, encrypting the passwords with a hash and a salt.  
   2. Salt is extra data that is fed into a hash function, which:

* It prevents duplicate passwords from being visible in the password file. Even if two users choose the same password, those passwords will be assigned different salt values. Hence, the hashed passwords of the two users will differ.
* It greatly increases the difficulty of offline dictionary attacks. For a salt of length *b* bits, the number of possible passwords is increased by a factor of 2*b*, increasing the difficulty of guessing a password in a dictionary attack.
* It becomes nearly impossible to find out whether a person with passwords on two or more systems has used the same password on all of them.

1. Answer the following questions on intrusion and intrusion detection: (1) On what fundamental assumption do intrusion detection systems work? (2) Explain the two commonly used approaches to intrusion detection.   
     
   1. IDS work on the assumption that the intruder behaves differently from a regular user.  
   2. Anomaly Detection: Counting number of occurrences of a specific event over time. Comparing previous behaviour to current behaviour and seeing if there is a deviation. (Threshold detection, profile-based systems)  
     
   Signature Detection: Signature techniques detect intrusion by observing events in the system and applying a set of rules that lead to a decision regarding whether a given pattern of activity is or is not suspicious.
2. Answer the following questions on virus/anti-virus: (1) Explain the four phases that a typical virus goes through. (2) Explain how a digital immune system works. (3) Name and explain three approaches by which virus scanners work.

a. The four phases include:  
1.Dormant Phase: Virus is idle  
2. Propagation Phase: Places a copy of itself into other programs or copies itself into system areas such as disk or memory. Each infected program contains a clone of the program and can continue the propagation phase.  
3. Trigger Phase: The virus becomes active after a certain condition is met. This could be a number of conditions such as system time, date, certain number of virus infections have occurred, etc.  
4. Execution Phase: Program executes and usually does damage such as deleting certain files or using up system resources for other purposes.  
  
b. A digital immune system works by having a process running on each host machine that monitors the computer looking for suspicious behaviour. The monitoring program forwards a copy of the suspected virus to an administrative machine. Administrative machine encrypts the sample and sends it to a central malware analysis system. The machine creates an environment in which the suspect program can be run in a sandbox environment for analysis. Malware analysis system then creates a prescription for identifying and removing the malware. The prescription is forwarded to other users on the organization. Subscribers from around the world receive anti-virus updates that protect them from the new malware.  
  
c. Scanners first operated by looking for malware signatures to identify the malware. This signature is a sequence of bit patterns in all copies of the malware. Another early generation technique is that the anti-virus software would keep track of the length of a program. If the length increases, it is likely due to a virus. Second generation scanners do not rely on signatures and operate based on behaviour. There are a small set of actions that if satisfied are a good indicator a program is malicious or infected.

1. Explain what firewall is. List and explain three different types of firewalls.  
   A firewall blocks or permits traffic depending on a list of rules defined in an access control list. There are different types of firewalls such as hardware and software. For more details review question #1 on the types of firewalls.

**Hands-on Exercises:**

In the second half of the semester, the hand-on exercises consist of several networking projects to be done by using OPNET IT Guru Academic Edition, with a particular interest in network security issues. Five projects will be provided on the course website. You can spend up to two days (using the workshop times) to complete each project.

**The following is the procedure of downloading and installing OPNET IT Guru Academic Edition:**

* Visit the following website:

<http://www.opnet.com/university_program//itg_panko.html>

* Complete your registration via the following path:
* UNIVERSITY PROGRAM
* [IT Guru Academic Edition](http://www.opnet.com/university_program/itguru_academic_edition/index.html)
* New Users: Register and Download
* Complete the registration table **(providing your email address)**
* You will receive an email including your username and password.
* Go to the following site:

[http://www.opnet.com/itguru-academic/download.html](http://www.opnet.com/itguru-academic/download.html" \t "_blank)

to download the software (presenting your username and password).

* Install OPNET on your computer.

Note that before you can use the OPNET, you will need to activate your license. Please click the OPNET icon and follow the instructions to complete the activation.