CSC 439/539 Advanced Information Security, Spring 2013, Question Bank on Module 7 - Network Security

Encryption and VPNs

1) Briefly explain the differences (at least four significant differences) between link-level encryption and end-to-end encryption.
2) Briefly explain the principle of IP-in-IP encapsulation in the context of virtual private networks.

IPSec

1) What is the role of the Diffie-Hellman Key Exchange mechanism and explain the two significant uses of the key exchanged as part of this mechanism during the IPSec security association establishment process?
2) Distinguish between the IPSec transport mode and the IPSec tunnel mode? Explain their operating principle.
3) What is the common characteristic of the IP header fields that are used in the computation of the IPSec authentication data?
4) Assume there are four sites for a corporate network. In each site there are 10 hosts. How many security associations would be formed for secure two-way communication between any pair of hosts in the corporate network under each of the two IPSec (i.e., transport and tunnel) modes?
5) What are the two protocols developed for IPSec? What is the value of the 'Next Header' protocol field for each of them? What features each of these two protocols provide?
6) Briefly explain the sequence of steps to establish a security association from host A to host B?
7) Explain the role of the key-derivation functions in IPSec?
8) What is Internet Key Exchange (IKE) Protocol? What role does it play in IPSec?

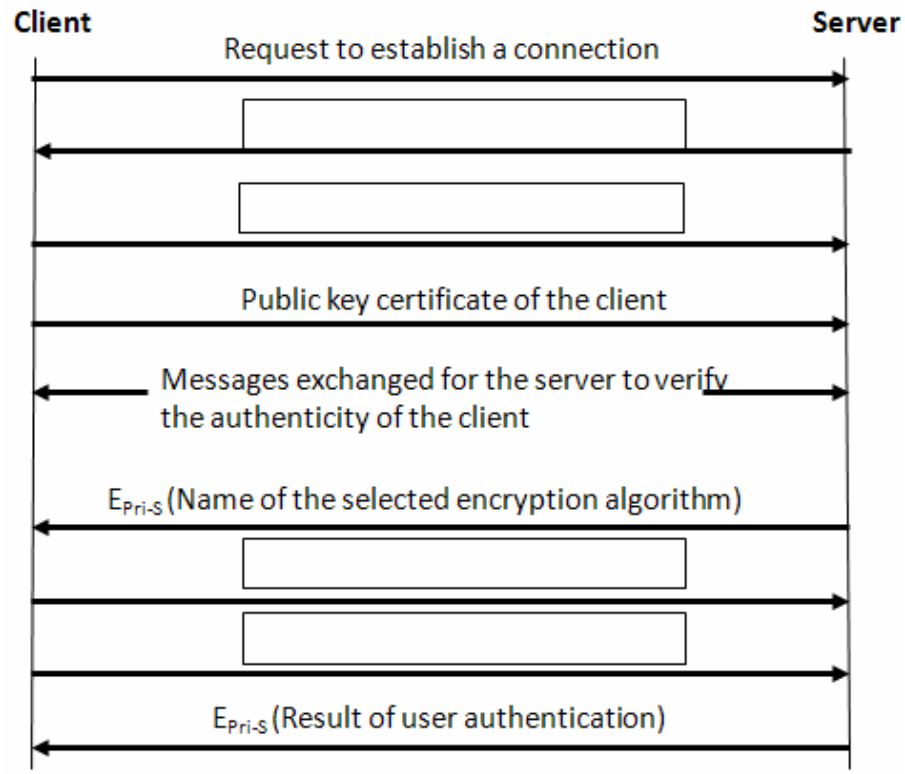
Firewalls

1) Mention two significant characteristics that are unique representative features of a "personal" firewall when compared to the other three categories of firewalls discussed in class?
2) Explain the "default-deny" and "default-allow" options of filtering packets through a firewall.
3) Discuss the pros and cons of using the black-list approach and the white-list approach of filtering packets through a firewall.
4) Explain the three significant attacks (that we discussed in the slides/lecture) that could be prevented by employing a packet filter firewall.
5) Explain how would use a firewall (and what category) for each of the following scenarios. You need to justify your selection:
a. An organization wants to give remote login access for its employers to their office computer. The office computers could differ in the operating system employed and do not have a strong authentication mechanism.
b. A network administrator wants to restrict clients from downloading beyond a certain number of bytes from a file server over a time period.

6) Given the four firewalls: Application proxy firewall, Packet filter firewall, Stateful firewall and the Personal firewall; in what order would you place them from the Internet towards a network and explain why would you place so?

SSH

Complete the following flowchart for the Secure Shell (SSH) Protocol



Wireless Security

1) What is the main weakness of the WEP algorithm and how is it addressed by WPA? Explain.
2) What is the WAP Gap problem? How does the WAP Gateway fix the problem?
3) Briefly describe the encryption process of (i) WEP and (ii) WPA.
4) Describe the challenge-authentication mechanism employed while connecting to a wireless LAN under the WEP standard? Explain the vulnerability involved in it.
5) What are the two modes by which WAP v. 2.0 fixes the WAP Gap problem? Explain both of them.
6) Briefly explain how the Integrity Check Value (ICV) for the data is computed in (i) WEP and (ii) WPA.