This HW/Lab assignment covers Lectures 8 (IPSec) and 9 (Wireless Security). Please review these thoroughly before starting to work on the assignment.

It is a combination of a hands-on lab exercise and conceptual problems. Problem 9 is a lab exercise while the rest are conceptual problems. You are strongly encouraged to utilize your lab session to accomplish the lab exercise. In fact, to do Problem 9, it is necessary to be in the lab.

All soft copy submissions (with answers to the problems) must be turned in via Blackboard Learn. Name your files as “Lastname_Firstname_HW4”. Please make sure that you have correctly submitted/uploaded the files.

You can submit hand-written hard copies, if you wish. However, we would prefer that you submit soft copies. If you choose to submit hard copies in any case, please turn them into my mailbox in the CS office or hand them in before the lectures. Please also make sure that your hand-written solutions and handwriting is legible and easy to understand.

You must submit by the deadline – 11 am on 12/02/2013. This applies to both soft and hard copy submissions. Late submissions will not be graded.

You will be graded based on the correctness of your answer and also on the steps that you took to come to that answer, whenever possible and applicable. Please try to show all your work, when feasible.

The assignment needs to be solved individually by every student. No collaboration of any sort is allowed, unless stated otherwise. No plagiarism is allowed. Please check the course policies against misconduct (discussed in Lecture 1). When in doubt, please consult the instructor.

Please submit early to avoid any last minute issues.

Please do start working on the homework early and do not wait until the deadline.
A. Lab Exercise and Conceptual Problems

[Please review Section B and C, which will be useful in answering these questions]

1. **[10pts]** IPSec can be used to prevent replay attacks on IP datagrams. How does IPSec accomplish this? Explain your answer in detail.

2. **[5+3+2pts]** Consider the following diagram depicting a VPN network for a company. Assume there are \( n \) travelling salespersons. How many security associations (SAs) will be stored in the Security Association Database (SAD) of the IPSec router in the headquarters? How many SAs will be stored in the SAD of the IPSec router in the branch office? How many SAs will be stored in the SAD of each salesperson’s laptop?

3. **[5pts]** Suppose you are designing a program that sends packets between the client and server using TCP for use in an institution that relies on IPSec to communicate between corporate offices. Would you need to modify your application to suit the needs of IPSec? Explain your reasoning.
4. **[2.5+2.5+5pts]** In which order encryption and MAC are applied in IPSec? In which order encryption and MAC are applied in SSL?

   Are these ordering mechanisms secure (please refer to this paper to answer this question: [http://www.iacr.org/archive/crypto2001/21390309.pdf](http://www.iacr.org/archive/crypto2001/21390309.pdf))?

5. **[5+5+5pts]** Explain the Diffie-Hellman Key exchange protocol. Is this protocol secure against a man-in-the-middle attacker? If not, show a man-in-the-middle attack, and explain how this attack can be fixed.

6. **[5pts]** A wireless network uses MAC address based access control (white lists) to prevent unauthorized hosts from connecting to the network. Explain how an attacker can subvert this access control mechanism.

7. **[5+5pts]** Describe the authentication protocol that WEP employs to authenticate a wireless host to a wireless AP (given that the two have a pre-shared symmetric key). Show an attack on this protocol. That is, show how an attacker, who does not have access to the key shared between a host and an AP, can impersonate the host.

8. **[5pts]** Based on your knowledge of WPA2-Personal and WPA2-Enterprise, which variant is uabwifi-nac relying on?

9. **[30pts]** In the lab, we have a wireless network setup, called netsec-unsecured. Connect to netsec-unsecured and perform a Wireshark trace on the network. Filter your results to show only packets with the following IP address **192.168.1.130**. Analyze the packets sent to and from that IP address, and report your findings. In particular, you should be looking for TCP based traffic.
B. Lab and Tools Description
Like in the SSL lab, we’ll be using wireshark to promiscuously sniff wireless networks.

Connecting to Wireless networks in the Netlab

Select the Networking icon in the upper righthand corner of the screen and select the desired wireless network. Your ethernet connection will be deactivated upon connecting.

Wireshark Wireless Trace
Starting a wireless capture is nearly identical to what we did in Lab 3, however this time we will select the wlan0 interface instead of eth0 (if you’re on a mac, this will be en0/1). Ensure that ‘Capture Packets promiscuously’ is selected and then hit start.

If you want to filter traffic to that involving a specific IP address, in the filter bar, type ‘ipaddr == X.X.X.X’ and hit enter. We will also cover a few other filter options in lab.
C. Lab Background
While the lab itself will focus primarily on wireless security, we will briefly discuss IPSec to give additional insight on the conceptual questions on this homework assignment.

**IPSec**
IPSec is an end-to-end security suite that is used to authenticate and encrypt IP based communications between two parties at Layer 3, or the Network layer.

Within IPSec there are two different protocol types:
- Authentication Headers - AH
- Encrypted Security Payloads - ESP

The Authentication Header is used to ensure that the message hasn’t been compromised, and that the source of the message is who they say they are.

The Encrypted Security Payload is used to encrypt the actual contents of the message.

IPSec itself can be used in two different modes:
- Transport Mode: Encrypts and/or authenticates upper layer protocols, but not the lower protocols. In this mode, the Source and Destination aren’t hidden. Host-to-host communication.
  - An eavesdropper can potentially see which two machines are communicating.

- Tunnel Mode: The original packet is encapsulated and encrypted within a new packet, which is then sent to another network’s IPSec compliant device. Network-to-network communication.
  - An eavesdropper can only see that two networks are communicating.

IPSec requires mutual authentication between two parties, usually relying on Security Associations and Security Policy Databases in order to dictate the parameters of a given connection.

For additional information on IPSec, refer to Lecture 8.

**Wireless Security**
Wireless networking generally refers to the IEEE802.11 standard, or Wi-Fi. Wireless networking provides a convenient means for machines to connect to existing networks by transmitting traffic over the air to Access Points. These access points, which usually are physically connected to an existing ethernet network, then act as a bridge between wireless clients and wired traffic. However, when broadcasting information over the air, there are a number of security concerns that arise, as eavesdropping becomes a
serious problem. However, wireless routers are generally not high power machines, and therefore encryption methods must be relatively simple in order to allow routers to handle high volumes of traffic.

To counteract this, there are several standard wireless security schemes that are used by routers today. The base mode of a router is unprotected, in which a client simply joins a Wi-Fi network without any form of authentication. This mode is particularly dangerous as traffic sent across the air is not protected in any way, so any eavesdropper can sniff your packets (as we will examine in this lab). Fortunately, this scheme is rarely used by home users, but you might still see this in places that offer unprotected Wi-Fi, such as restaurants or coffee shops. The two popular wireless security schemes are Wired Equivalency Protection (WEP) and Wi-Fi Protected Access (WPA).

**WEP**

WEP was one of the first popular wireless security schemes, however it is now considered to be obsolete due to several security flaws. There are two authentication methods that the client can use to associate with the Access Point. The first, the shared key authentication protocol is accomplished with four simple steps:

1. Client sends authentication request to the AP
2. The AP sends a clear-text challenge
3. The Client encrypts the challenge with the Preshared Key and sends it back
4. AP verifies the decrypted challenge and responds accordingly to the client

After this initial authentication, the client and AP use RC4 (a stream cipher that uses an IV and key to generate a psuedorandom stream of bits that is XORed with data to encrypt it) to transmit encrypted packets.

However, the above protocol is considered unsecure, as an eavesdropper can use the handshake information to determine the RC4 keystream and read the packet stream (the eavesdropper gets a plaintext/ciphertext pair with no effort). Furthermore, the IV value (sent in the clear as a part of the encrypted packet) is only 24-bits, which proves to be a flaw for large networks as IV’s end up being reused with the same key value (making encrypted packets vulnerable).

In the other authentication method, Open System authentication, there is no formal challenge and response. Instead, the client just starts using the WEP key to encrypt traffic, which actually is more secure than the shared key authentication protocol.

Ultimately, WEP is not considered a secure wireless protocol, and has been largely replaced by WPA2.
WPA/WPA2
Due to the large number of flaws in WEP, WPA was quickly proposed as an alternative to replace it. WPA introduced new methods of packet encryption, specifically the Temporal Key Integrity Protocol (TKIP), which still relied on RC4 in order to ensure compatibility with existing routers. In WPA, a preshared key is used to generate the Pairwise Master Key that the AP and Client use to derive the Pairwise Transient key, creating a protected connection between the client and AP.

In the field, you will generally see two variants of WPA2, WPA2-Personal and WPA2-Enterprise. The former is more common on home networks, and relies on Preshared Key values for authentication of clients. The Enterprise variant of WPA2 uses a RADIUS server to authenticate clients individually, instead of using a PSK. WPA2-Enterprise is considered significantly more secure, as each client has unique keys, however WPA2-Enterprise isn’t as practical for home users.

For more information on Wireless Security Technologies, please refer to Dr. Saxena’s slides at http://www.cis.uab.edu/saxena/teaching/cs36-netsec-f13/Lectures/lecture9-Wireless.pdf
And Chapter 7 of Stallings’ Network Security Essentials book.