Name……..….ID……..……..Section…….……Seat No……..….

Sirindhorn International Institute of Technology
Thammasat University

Final Examination: Semester 2/2006

Course Title : CSS 322 – Security and Cryptography

Instructor : Dr Steven Gordon

Date/Time : Monday 12 March 2007, 9:00 – 12:00

Instructions:

- This examination paper has 17 pages (including this page).
- Condition of Examination
  Closed book (No dictionary, no calculator)
- Students are not allowed to be out of the exam room during examination. Going to the restroom may result in score deduction.
- Turn off all communication devices (mobile phone etc.) and leave them under your seat.
- Write your name, student ID, section, and seat number clearly on the answer sheet.
- The space on the back of each page can be used if necessary.

Part A - Multiple Choice Questions [22 marks]

Select the most accurate answer (only select one answer). Each correct answer is worth 2 marks. You receive 0 marks for an incorrect answer or no answer.

1. Stateful packet inspection:
   a) Allows a firewall to reject (drop) packets based on the content of emails (e.g. spam, viruses)
   b) Allows a firewall to reject (drop) packets that contain malicious HTTP GET requests
   c) Allows a firewall to reject (drop) packets that do not belong to an open TCP connection
   d) Requires a single homed bastion host
   e) Requires a dual homed bastion host
   f) Requires a screened subnet with demilitarized zone (DMZ)

2. Web cookies were designed to:
   a) Prevent websites from impersonating (pretending to be) other websites
   b) Provide simple method for submitting username and password
   c) Prevent tracking of user's web browsing habits
   d) Provide state information for web transactions
   e) Provide methods for stateful packet inspection

3. When compared to a public key cryptosystem, a symmetric key cryptosystem is:
   a) More computationally efficient, but difficult to distribute keys
   b) Easy to distribute keys, but less computationally efficient
   c) More secure, but difficult to distribute keys
   d) Easy to distribute keys, but less secure
   e) More computationally efficient, but less secure
   f) More secure, but less computationally efficient

4. A computer virus:
   a) Is a program that searches for other systems to infect, connects to a remote system and copies itself to that remote system and executes.
   b) Goes through the phases of being dormant, propagating, triggering and execution.
   c) Is host independent
   d) Is non-replicating
   e) Is a program modification that contains unauthorized access to functionality

5. If you had access (e.g. login as an administrator) to the SIIT gateway router, for all messages passing through that router, you could:

   a) Read the contents of the messages if they were encrypted only with TLS
   b) Read the contents of the messages if they were encrypted only with IPsec (transport mode)
   c) Read the contents of the messages if they were encrypted with any encryption algorithm/protocol
   d) Not read the contents of the messages if they were all encrypted with IPsec (transport mode)

6. If Transport Layer Security is used to secure data (e.g. web pages) between a client and server, TLS uses:
   a) Public key algorithms for data confidentiality and MD5 or SHA1 for data integrity
   b) Message authentication codes for data integrity and symmetric key algorithms for data confidentiality
   c) Public key algorithms for key exchange and Diffie-Hellman for data integrity
   d) Symmetric key algorithms for key exchange and message authentication codes for authentication

7. John's X.509 certificate (which is signed by the certificate authority Steve) contains:
   a) Only John's private key (and no other keys)
   b) Only John's public key (and no other keys)
   c) John's private key and Steve's public key
   d) John's public key and Steve's public key
   e) John's private key and Steve's private key
   f) John's public key and Steve's private key

8. When compared to using a single certificate authority, an advantage of using a hierarchy of certificate authorities (CAs) is that:
   a) The CA's do not need to trust each other
   b) The lifetime (or validity) of the certificate can be made longer
   c) Users only need to register and obtain certificates from their local CA, rather than the central CA
   d) It is more efficient to validate certificates signed by different CAs
   e) The man-in-the-middle attack can be avoided

9. If sending a Message Authentication Code of a message (as well as the message, M) from A to B, then a man-in-the-middle attack by C can be:
   a) Detected if C sends a modified message P, such that MAC(P) = MAC(M)
   b) Successful if the message M is sent as plaintext
   c) Successful if C knows the MAC function used
   d) Successful if C can discover a message P that such that MAC(P) = MAC(M)
   e) Successful if the MAC function is strong collision resistant

10. The security of RSA:
    a) Depends on the difficulty in factoring large numbers into their primes
    b) Depends on the difficulty in multiplying two large prime numbers
    c) Cannot be attacked using timing attacks
    d) Cannot be attacked using a brute force approach
    e) Is much stronger than AES
    f) Is much stronger than 3DES

11. The Diffie-Hellman exchange in Transport Layer Security (TLS/SSL) is used for exchanging:
    a) Secret values between two users
    b) Certificates between two users
    c) Nonce values between two users
    d) Sequence numbers between two users
    e) Encrypted files between two users

Part B – General Questions [78 marks]

Question 1 [11 marks]

a) Describe the TCP SYN flooding attack. Make sure you explain how the attack is started, and how the attack affects the target. [4 marks]

b) What is the difference between slave nodes and reflector nodes in a distributed denial of service (DDoS) attack? [2 marks]

c) Describe an advantage of using reflector nodes in a DDoS attack. [2 marks]

d) Could the TCP SYN flooding attack make use of reflector nodes? If yes, explain how. If no, explain why not. [3 marks]

Question 2 [19 marks]

The following C code shows an example DNS program (`dnsnametoip.c`).

```
#include <string.h>
#include <stdio.h>
char* getIpFromDns(char* strDnsName)
{
      if (strcasecmp(strDnsName, “www.raytheon.com”) == 0)
      {
            return “192.168.0.1”;
      }
      else if (strcasecmp(strDnsName, “www.w3.org”) == 0)
      {
            return “192.168.0.2”;
      }
      else if (strcasecmp(strDnsName, “www.slashdot.org”) == 0)
      {
            return “192.168.0.3”;
      }
      else if (strcasecmp(strDnsName, “www.kerneltrap.org”) == 0)
      {
            return “192.168.0.4”;
      }
      return “Unknown”;
}

int main(int argc, char* argv[])
{
      char strBuffer[255];
      strcpy(&strBuffer[0], argv[1]);
      printf(“%s\n”, getIpFromDns(strBuffer));
      return 0;
}
```

a) Explain what a user needs to do to cause a *buffer overflow* in the above program. Also explain why the buffer overflow occurs. [4 marks]

b) Explain a change to the code that will avoid the buffer overflow. Also explain how the new code avoids the buffer overflow. [3 marks]

The following C code shows an example program that starts a command line shell (`exploitcodeusingExecve.c`):

```
#include <unistd.h>

int main()
{
      char* argv[1];
      argv[0] = “/bin/sh”;
      argv[1] = NULL;
      execve(argv[0], argv, 0);
      return 0;
}
```

c) An attacker wants to perform a buffer overflow attack. Explain the steps the attacker may take for this exploit code to be inserted into memory using the DNS program of part (a). [4 marks]

d) When the function `getIpFromDns()` in the DNS program is called, an instruction pointer is created that points to a position in memory. What is stored in memory at the position the instruction pointer points to? [2 marks]

e) Explain the purpose of the attacker including a new instruction pointer after the exploit code. Include a discussion of the value of the instruction pointer and how it is used. [4 marks]

f) Often the attacker cannot determine the exact position in memory where the exploit code is inserted. What does the attacker do to increase the chance that the exploit code will still be executed, even if the incorrect memory position is used [2 marks]

Question 3 [12 marks]

In some UNIX systems the password file contains a list of usernames for users on the computer system, along with a hash of the password for each user. Assume an attacker has access to the password file.

a) Explain an advantage the attacker has in discovering passwords, compared to an online attack. [2 marks]

As an additional security measure, a *salt* can be included when hashing the password. That is, a 12-bit random value (the salt) is appended to the plaintext password before the hash is applied. The password file then stores the username, the salt, and the hash value (that is Hash(password + salt)).

b) Explain how the addition of the salt helps prevent detection of duplicate passwords in the password file. (Hint: in your explanation, compare what happens if the salt is not used, and then if the salt is used) [3 marks]

c) In addition to preventing detection of duplicate passwords, and despite the salt being known to the attacker, how else does using the salt value increase security of the password file. (Hint: again consider what happens when the salt is and is not used – focusing on the chance of the attacker guessing a correct password). [4 marks]

d) Explain why increasing the salt size from 12-bits to a much larger size (e.g. 24 or 36 bits) *does not* make password guessing (practically) impossible? (Hint: consider part (c)). [3 marks]

Question 4 [7 marks]

a) What is the main security problem with HTTP Basic Authentication? [2 marks]

b) How does HTTP Digest Authentication overcome the problem identified in part (a)? [2 marks]

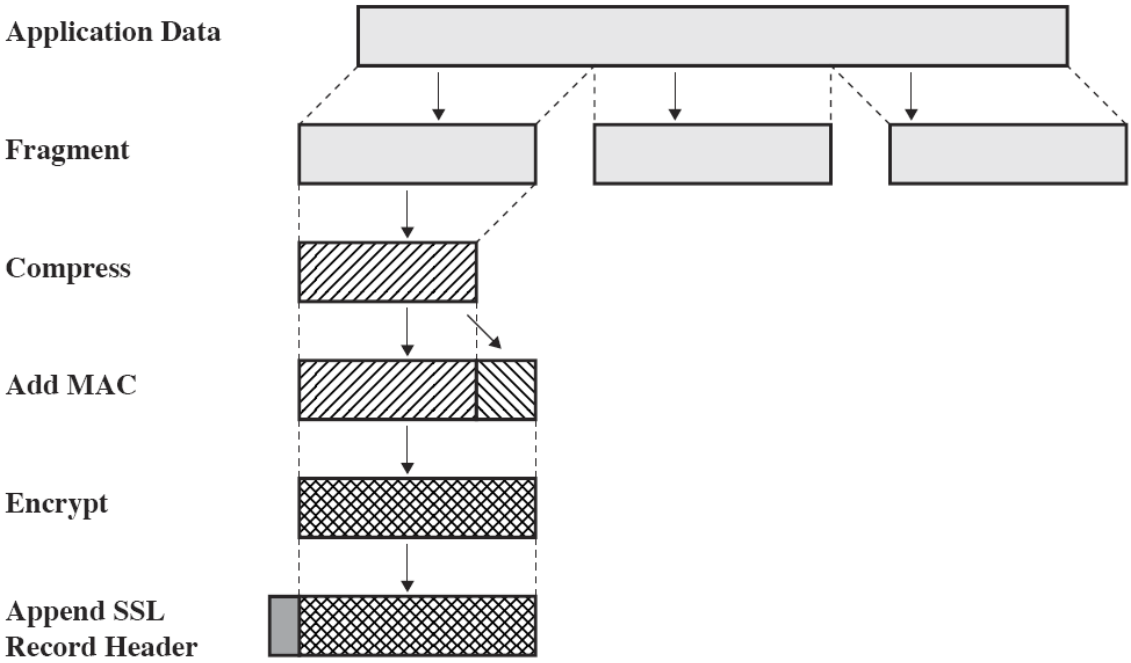
The text below shows an example message sent from client to server for Digest-based authentication. Several important fields are the username, the response (contains the hash of the password), the nonce (which is unchanged in each subsequent request to the same server) and the nonce count (nc).

```
GET /dir/index.html HTTP/1.0
        Host: localhost
Authorization: Digest
        username="Mufasa",
        realm="testrealm@host.com",
        nonce="dcd98b7102dd2f0e8b11d0f600bfb0c093",
        uri="/dir/index.html",
        qop=auth,
        nc=00000001,
        cnonce="0a4f113b",
        response="6629fae49393a05397450978507c4ef1",
        opaque="5ccc069c403ebaf9f0171e9517f40e41"
```

c) How do the nonce and nonce count help prevent/detect replay attacks? [3 marks]

Question 5 [5 marks]

The figure below shows the steps applied to application data by the SSL Record Protocol.

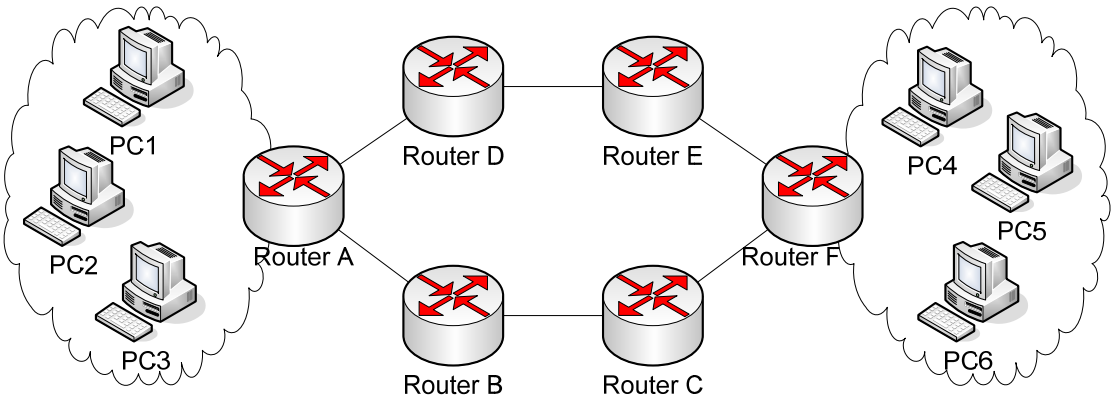


a) What two security services does the SSL Record Protocol provide? [2 marks]

b) List and explain an advantage and disadvantage of using SSL compared to using IPsec. [3 marks]

Question 6 [13 marks]

The figure below shows two networks, each with three PCs, connected across an internet. Refer to the IP addresses of nodes by their name, for example: the IP address of PC1 is PC1.



In parts (a), (b) and (c), assume IPsec with Encapsulating Security Payload and Transport Mode are used to secure data transfer between PC1 and PC4.

a) List three security services provided by the IPsec connection. [3 marks]

b) If an IPsec packet is received by Router E, does Router E know that PC1 and PC2 are communicating with each other? Explain why. [2 marks]

c) If an IPsec packet is received by Router E, does Router E know the application (that is, port number) being used by PC1 and PC4? Explain why. [2 marks]

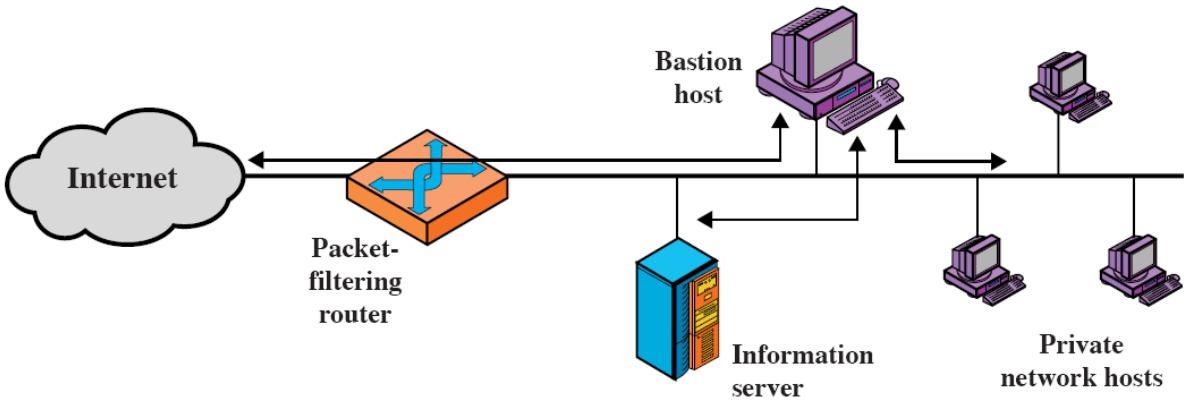
In parts (d) and (e), assume IPsec with Encapsulating Security Payload and Tunneling Mode are used to secure data transfer between the two networks of PCs, with the network gateways being tunnel end-points. PC1 and PC4 communicate via the tunnel.

d) If an IPsec packet is received by Router E, does Router E know that PC1 and PC2 are communicating with each other? Explain why. [2 marks]

e) List and describe an advantage and disadvantage of using tunneling mode (versus transport mode). [4 marks]

Question 7 [11 marks]

A single homed bastion host is one way to configure a network using both a packet filter firewall/router, as well as an application level firewall (bastion host).



a) Explain the difference between a packet filter firewall/router and an application level firewall. Include an advantage of each type of firewall. [4 marks]

b) Describe two rules that must be configured on the packet filter router in this configuration. [3 marks]

c) What is an advantage of using this configuration (as opposed to using only an application level firewall)? [2 marks]

d) What is the difference between this configuration and a dual homed bastion host configuration? Explain how the dual homed configuration provides an advantage over the single homed configuration. [2 marks]