

Sirindhorn International Institute of Technology Thammasat University

Final Examination: Semester 2/2007

Course Title : CSS 322 – Security and Cryptography

Instructor : Dr Steven Gordon

Date/Time : Monday 3 March 2008, 13:30 – 16:30

Instructions:

- ③ This examination paper has 21 pages (including this page).
- ③ Condition of Examination
Closed book (No dictionary, no calculator)
- ③ Students are not allowed to be out of the exam room during examination. Going to the restroom may result in score deduction.
- ③ Turn off all communication devices (mobile phone etc.) and leave them under your seat.
- ③ Write your name, student ID, section, and seat number clearly on the answer sheet.
- ③ 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 do not belong to an open TCP connection
 - c) Allows a firewall to reject (drop) packets that contain malicious HTTP GET requests
 - d) Requires a single homed bastion host
 - e) Requires a dual homed bastion host
 - f) Requires a screened subnet with demilitarized zone (DMZ)

2. When compared to a public key cryptosystem, a symmetric key cryptosystem is:
 - a) Easy to distribute keys, but less computationally efficient
 - b) More computationally efficient, but difficult to distribute keys
 - 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

3. 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

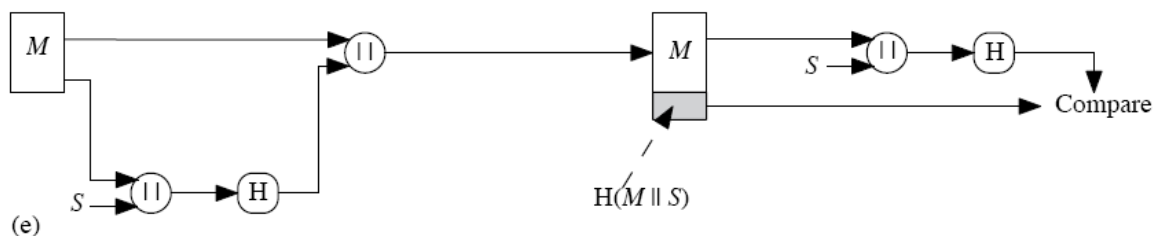
4. If you had access (e.g. login as an administrator) to the SIIT gateway router, for all messages passing through that router, you could:
 - a) Read the contents of the messages if they were encrypted only with TLS
 - b) Read the contents of the messages if they were encrypted only with IPsec (transport 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)
 - e) None of the above.

5. 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) Public key algorithms for key exchange and Diffie-Hellman for data integrity
 - c) Message authentication codes for data integrity and symmetric key algorithms for data confidentiality
 - d) Symmetric key algorithms for key exchange and message authentication codes for authentication
 - e) None of the above.

6. 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

7. 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) It is more efficient to validate certificates signed by different CAs
 - d) Users only need to register and obtain certificates from their local CA, rather than the central CA
 - e) The man-in-the-middle attack can be avoided

8. In the figure illustrating the use of a hash function for authentication, if the following property of hash functions *does not hold*, then an attacker could discover the secret S:
 - a) Hash function produces a small hash value
 - b) Efficient to calculate the hash function
 - c) One-way property
 - d) Weak collision resistant
 - e) Strong collision resistant



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

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

11. A distinct feature of a metamorphic virus (compared to other types of virus):
 - a) A normal application that contains unexpected additional functionality
 - b) Stored in main memory, and hence infects other applications that execute
 - c) Stored on the boot sector of a hard disk, and hence infects applications when the computer starts
 - d) Changes its behavior and appearance when propagating (making copies of itself)
 - e) Changes only its appearance when propagating (making copies of itself)

Part B – General Questions [78 marks]

Question 1 [10 marks]

Using the RSA algorithm, where the ciphertext $C = 146$ and public key $PU = \{e=7, n=187\}$, determine the plaintext P and private key PR . Show your calculations.

(Hint: if you do not have a calculator, the following table gives some selected calculations which may be useful)

a	b	c	a^b mod c	A	b	c	a^b mod c
146	3	187	82	146	15	187	12
146	4	187	4	146	16	187	69
146	5	187	23	146	17	187	163
146	6	187	179	146	18	187	49
146	7	187	141	146	19	187	48
146	8	187	16	146	20	187	89
146	9	187	92	146	21	187	91
146	10	187	155	146	22	187	9
146	11	187	3	146	23	187	5
146	12	187	64	146	24	187	169
146	13	187	181	146	25	187	177
146	14	187	59	146	26	187	36

Question 2 [16 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. [3 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). [3 marks]

d) When the function `getIpFromDns()` in the DNS program is called, an instruction pointer is created that points to a position in memory. Before an attack is performed, 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. [3 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). [3 marks]

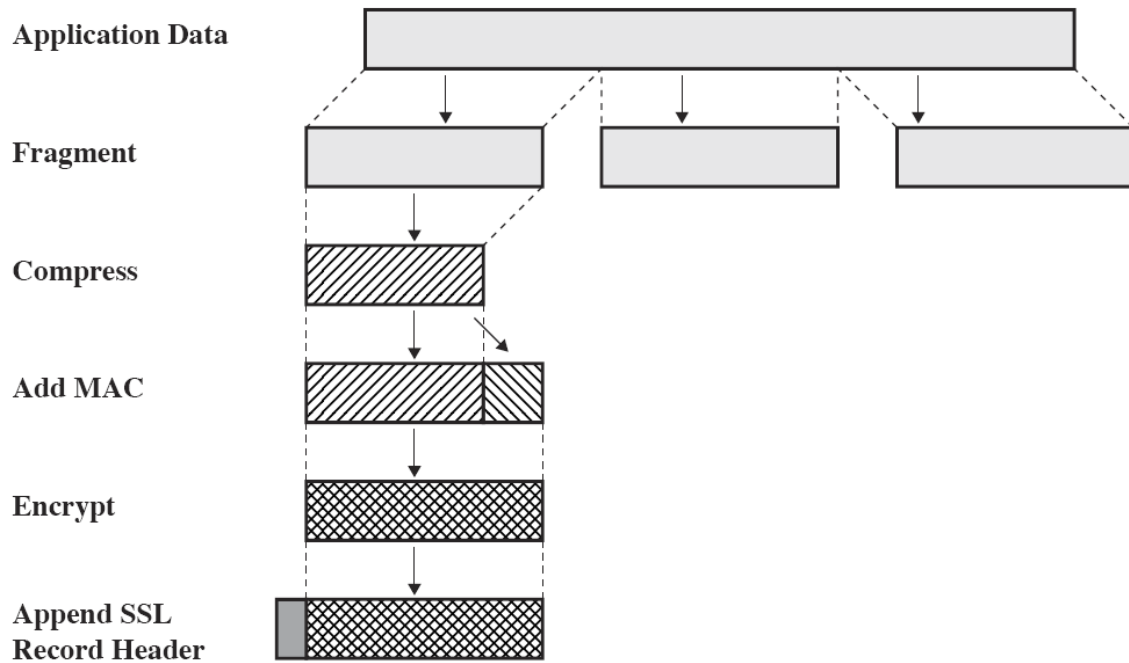
- d) Explain why increasing the salt size from 12-bits to a much larger size (e.g. 24 or 36 bits) *does not* make password guessing (practically) impossible? (Hint: consider part (c)). [4 marks]

Question 4 [8 marks]

Assume a digital signature is applied on the hash of a message (not the message itself), and A sends the message (M_A) and digital signature to B. If the hash function is not weak collision resistant, then explain how an attacker C can forge A's digital signature on a new message from C (called M_C). Make sure you explain why B cannot detect this forgery.

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]

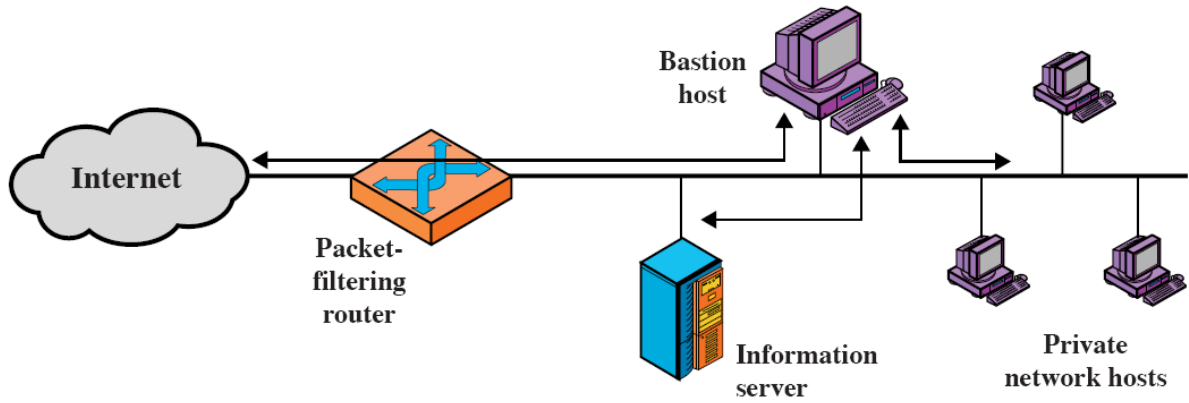
In parts (d) and (e), assume IPsec with Encapsulating Security Payload and Tunneling Mode are used to secure data transfer between the two networks of PCs, with the network gateways being tunnel end-points. PC1 and PC4 communicate via the tunnel.

d) If an IPsec packet is received by Router E, does Router E know that PC1 and PC4 are communicating with each other? Explain why. [2 marks]

e) List and describe an advantage and disadvantage of using tunneling mode (versus transport mode). [2 marks]

Question 7 [10 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. [3 marks]

b) Describe two rules that must be configured on the packet filter router in this configuration. (You only need an explanation of what the rules will do – you do not need to give specific rules) [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]

- c) Explain what happens if C changes both the message M (to N), and calculates and sends the new MAC based on N? (Include an explanation of whether B detects an attack) [3 marks]