IS2150/Tel2810 Introduction to Security
Final,
Thursday, December 13, 2007

Name: 

Email: 

Total Time : 2:15 Hours
Total Score : 100

Note that scores for each question may be different – so spend time accordingly on each question. Be precise and clear in your answers.

Good Luck!!

Total Score:
Part I:

Write T for **True** and F for **False** (Total Score 20)

1. [ ] IPSec can be used to create a virtual private network.
2. [ ] Multipartite virus infects either boot sectors or the executable files.
3. [ ] Encrypted virus is aimed towards preventing detection of a virus signature.
4. [ ] Macro viruses are application-independent and architecture-dependent.
5. [ ] Both confidentiality and integrity models can be used to prevent the spread of viruses.
6. [ ] Java is by design a safer language than C.
7. [ ] Speaker verification and Speaker recognition techniques refer to recognition of speaker’s voice characteristics and verbal information verification, respectively.
8. [ ] In IPSec, if a packet needs to be dropped, it will be known from the Security Association Database.
9. [ ] TOCTTOU is an example of category stack smashing attack.
10. [ ] Security association indicates the bi-directional relationship between the peers and specifies the security services provided to the traffic carried on it.
11. [ ] One weakness of TCSEC is that it is based heavily on **integrity** requirements and ignores availability.
12. [ ] Common Criteria has a component that addresses country specific needs of some nations.
13. [ ] Arc injection is an attack that exploits vulnerability in the use of integer data types.
14. [ ] In two’s complement arithmetic, a signed integer of \( n \) bits ranges from \(-2^{n-1}\) to \(2^{n-1}-1\).
15. [ ] For race conditions to occur at least two control flows must alter the state of the race object.
16. [ ] \( D_k(E_k(D_k(y)))) = E_k(D_k(E_k(z))) \) for \( y = E_k(x) \) and \( z = (D_k(E_k(x))) \)
17. [ ] The product of two relatively prime numbers is a prime number.
18. [ ] Caesar is a transmission cipher and its key weakness is that the key is too short.

For 19 - 20, refer to the following exchange

\[ \text{Alice} \quad \{m\}k_s \| \{h(m)\}k_{Alice} \| \{ks\}k_{Bob} \quad \text{Bob} \]

19. [ ] \( k_s \) is the Interchange Key and \( k_{Alice} \) is the Data Encripment Key
20. [ ] This protocol provides message confidentiality and integrity, as well origin integrity.
Part II

1. Recall that $X<<Y>>$ represents $Y$’s certificate signed by $X$. Consider the following certificates and answer the following [5]
   - Cathy<<Alice>>
   - Dan<<Bob>
   - Dan<<Cathy>>
   - Cathy<<Dan>>

   (a) Show steps (or just write the signature chain) that Alice takes to validate Bob’s certificate:

   (b) Show steps (or just write the signature chain) that Alice takes to validate Bob’s certificate:

2. What is a dictionary attack? Briefly describe the two types of dictionary attack. [5]

   \textit{Answer}: 
3. For the S/Key scheme for password authentication, write the following: [5].
   a. If $h$ is the hash function used, and $k$ is the seed used:
      (i) $n$ keys $k_1, k_2, ..., k_n$ are generated as follows:

      $\quad$ 

      (ii) & the keys are used in the following sequence:

      $\quad$ 

   b. Assuming that $h$ cannot be inverted, the attacker cannot determine the next password because of the following reason:

4. Alice wants to send a message to Bob and she wants to ensure both the confidentiality and integrity. Indicate what encryptions/decryptions you would need to do in the four places indicated by question marks. Use $(pubA, privA)$ as Alice’s public-private key pairs and $(pubB, privB)$ as Bob’s. Use $E_x$ and $D_x$ to indicate encryption and decryption using key $x$ (note $x$ could be public or private key). [5]

Answer:
5. Draw diagrams to show the IPSec packets for the two IPSec protocols in both the models and indicate what security services are included in each. [5, 5]

![Diagram of IPSec packets](image)

**Answer:**
6. Describe the replay attack on the Needham-Schroeder key exchange protocol shown below. Assume that $k_s$ is known to the attacker. State why it is possible. [5]

```
Alice || Bob || $r_1$

Alice

{/c

{ Alice || $r_1$ || $k_s$ || { Alice || $k_B$ } $k_A$ }

Alice

{/c

{ Alice || $k_s$ } $k_B$

Alice

{/c

{ $r_2$ } $k_s$

Alice

{/c

{ $r_2 - 1$ } $k_s$

Alice

{/c

Bob

```

**Answer:**

7. Enumerate the key *Risk Assessment* steps [5]

**Answer:**
8. For the risks and the security mechanism indicated below, calculate and insert the values as per the given data: [5]
   - Risks:
     - disclosure of company confidential information,
     - computation based on incorrect data
   - Cost to correct data: $3,500,000
     - @20% likelihood per year: _________
     - Effectiveness of access control software: 60%: _________
     - Cost of access control software: +$55,000
     - Expected annual costs due to loss and controls: _________
     - Savings: _________

9. Write differences among *copyright*, *patent* and *trade secret*. [5]
   *Answer:*

10. Define the following terms [5]
    *Polymorphic virus:*
11. Write in the blank spaces [5]
   i. Two ways of detecting viruses are:
      [a] _____________________________
      [b] _____________________________

   ii. Two general ways to defend against a virus
      [a] _____________________________
      [b] _____________________________

12. Attempt any two of the following: [5]
   a  What is TEMPEST program? Name two ways of protecting against emanations.

   b  Indicate factors that need to be considered before disposing sensitive media.

   c  Identify two natural disasters and factors related to them in terms of protecting information system resources.
Attempt *Three* of the following (13, 14, 15, 16) [Total Score: 15]

13. Recall the buffer overflow program related to the attached program. Describe how the buffer overflow exploit works for the specialized input ‘‘1234567890123456j►*!’’. The contents of the stack after this input has been given is shown below. [5].

```c
bool IsPasswordOK(void) {
    char Password[12];   // Memory storage for pwd
    gets(Password);      // Get input from keyboard
    if (!strcmp(Password,"goodpass")) return(true); // Password Good
    else return(false);   // Password Invalid
}

void main(void) {
    bool PwStatus;               // Password Status
    puts("Enter Password:");     // Print
    PwStatus=IsPasswordOK();     // Get & Check Password
    if (PwStatus == false) {
        puts("Access denied");  // Print
        exit(-1);               // Terminate Program
    }
    else puts("Access granted"); // Print
}
```

---

**Answer:**

| Storage for Password (12 Bytes) |
| "123456789012" |
| Caller EBP - Frame Ptr main (4 bytes) |
| "3456" |
| Return Addr Caller - main (4 Bytes) |
| "j►*!" |
| Storage for PwStatus (4 bytes) |
| "0" |
| Caller EBP - Frame Ptr OS (4 bytes) |
| Return Addr of main - OS (4 Bytes) |
14. Recall the following example of a Trojan horse [5]

Perpetrator does the following
1. cat >/homes/victim1/ls <<eof
2. cp /bin/sh /tmp/.xxsh
3. chmod u+s,o+x /tmp/.xxsh
4. rm ./ls
5. ls $*
6. eof

Describe what happens when Victim1 executes “ls” command while in the directory /homes/victim1/

Answer:

15. Consider the following program [5]:

1. char cresult1, cresult2, c1, c2, c3;
2. c1 = 100;
3. c2 = 90;
4. c3 = -120;
5. cresult1 = c1 + c2 + c3;
6. cresult2 = c1 + c2;

Note that char type uses 8 bit and two’s complement form for negative values. Also they are converted to integer types when they appear in an operations such as those on the right of lines 5 and 6. Will there be a problem in executing lines 5 and 6 – give reasons.

Answer:
16. Describe what you mean by a race-condition. For the following program indicate what is the race condition/window and how it can be exploited. [5]

```c
int main(int argc, char *argv[]) {
    FILE *fd;
    if (access("/some_file", W_OK) == 0) {
        printf("access granted.\n");
        fd = fopen("/some_file", "wb+");
        /* write to the file */
        fclose(fd);
    } else {
        err(1, "ERROR");
    }
    return 0;
}
```

**Answer:**