IS2150/Tel2810 Introduction to Security
Final,
Tuesday, December 15, 2009

Name:

Email:

Total Time	: 2:15 Hours
Total Score	: 100

There are two parts. Part I has 25 points. Part II has 75 points over 12 questions. Note that scores for each question may be different – *so spend time accordingly on each question*. Be precise and clear in your answers.

Total Score:

Good Luck!!

Part I: Write T for *True* and F for *False* (Total Score 25)

1. [ ] The third generation firewalls have dynamic packet filtering.

2. [ ] A desirable goal of an IDS system is to reduce both *false positives* and *true positives*.

3. [ ] A demilitarized zone (DMZ) contains proxy servers between the internal and external firewalls.

4. [ ] *Asynchronous validation /inadequate serialization* class includes TOCTTOU attacks.

5. [ ] *Emergent Faults* class under Aslam's taxonomy includes *Synchronization errors*.

6. [ ] IPSec cannot be used to create a virtual private network between two networks that are connected through Internet.

7. [ ] Stealth virus provides a clean disinfected file when a read operation is performed on that file.

8. [ ] Macro viruses are application-dependent and architecture-dependent.

9. [ ] Both confidentiality and integrity models can be used to prevent the spread of viruses.

10. [ ] *Speaker recognition* and *Speaker verification* techniques refer to *information verification* and *recognition of speaker's voice characteristics verbal*, respectively.

11. [ ] Security association indicates the bi-directional relationship between the peers and specifies the security services provided to the traffic carried on it.

12. [ ] For race conditions to occur at least two control flows must alter the state of the race object.

13. [ ] *Encapsulating Security Payload* protocol does not provide message integrity service.

14. [ ] Salting uses random value to select an authentication function.

15. [ ] Multipartite virus infects either boot sectors or the executable files.

16. [ ] Penetration testing approach aims at proving the *absence* of vulnerabilities in a system.

17. [ ] Stack smashing attack in *finger*/*fingerd* is the result of buffer overflow problem

18. [ ] One use of *auditing system* is in assessing the damage done by an intrusion.

19. [ ] *Race conditions* vulnerability essentially falls under the Improper Serialization class under Aslam's classification.

20. [ ] The NRL taxonomy uses three schemes one of which is referred to as Emergent Faults.

21. [ ] A Firewall cannot prevent insider attack and is a part of defense in depth solution.

22. [ ] Following is an example of Improper Data Sanitization problem in C programs:

```
sprintf(buffer,
   "/bin/mail %s < /tmp/email",   addr
);
```

23. [ ] Authentication Header protocol provides confidentiality, authentication and anti-replay services.

For 24 - 25, refer to the following exchange

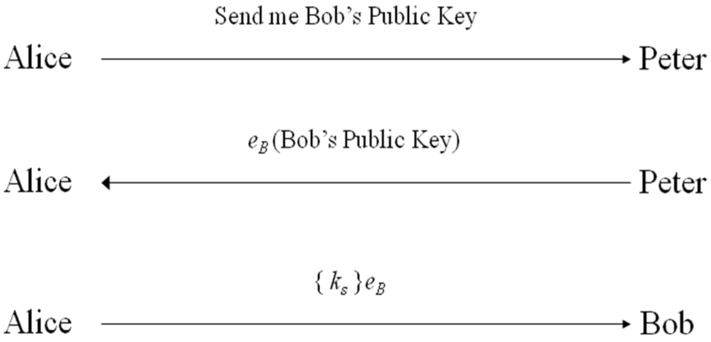
$$\text{Peter} \xrightarrow{\{\text{m}\}k_{\text{s}} \,\|\, \{h(\text{m})\}k_{\text{Alice}} \,\|\, \{k_{\text{s}}\}k_{\text{Bob}}} \text{Cathy}$$

24. [F] k_s is the Data Encipherment Key and k_{Alice} must be Alice’s Private Key

25. [Y] This protocol provides non-repudiation service.

Part II: (Total Score 75)

1. Consider the following key exchange protocol where Peter is a trusted party that provides the public keys. Show how you can launch a man-in-the-middle attack on this exchange [5]



Answer:

2. Given the following sequence of **`chdir`** commands, indicate where is the race window and how the race condition can be exploited. Is it a TOCTTOU – why or why not? [5]

```
chdir(“/tmp/a”);
chdir(“b”);
chdir(“c”);
chdir(“..”);
chdir(“c”);
ulink(“*”);
```

Answer

3. Recall that *X*<<*Y*>> represents *Y*’s certificate signed by *X*. Consider the following certificates. Can Alice and Bob validate each other’s certificates - give your reasons and show the signature chains if validations are possible. [5]

   Peter<<Eve>>, *Cathy<<Alice>>*, *Eve<<Dan>>*, *Dan<<Bob>*,
   Cathy<<Peter>>

Answer

4. Consider the following C program. In some compilers this will have undesirable consequences. Elaborate what would be the problem. [5]

```
int main(int argc, char* argv[]) {
    char a[16];
    char b[16];
    char c[32];
    strcpy(a, "0123456789abcdef”);
    strcpy(b, "0123456789abcdef");
    strcpy(c, a);
}
```

***Answer* (on the blank side)**

5. Answer ***two*** of the the following **[10]**

   a. Briefly explain the three types of IDS systems – mainly indicate how they differ.

   b. Differentiate between *System verification* and *Penetration testing.*

   c. Differentiate between *Type I* and *Type 2* dictionary attacks.

***Answer* (on the blank side)**

6. 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
      (i) n keys k_1, k_2, .., k_n are generated as follows:

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

      ----

   b. Given that the attacker can capture a key, he still cannot determine the next password because of the following reason:

Answer:

7. Recall the following example of a Trojan horse [5]

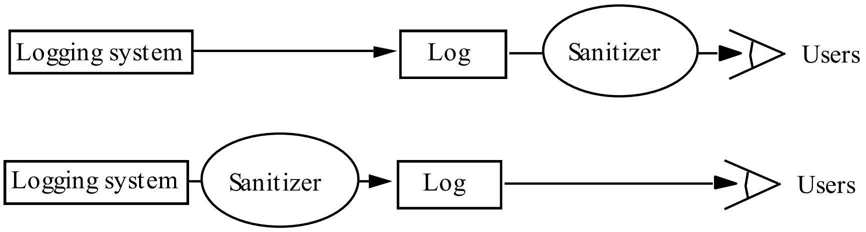
   a *Perpetrator does the following*

```
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
```

Explain how it works. What can Victim1 do to avoid falling into this trap.

***Answer* (on the blank side)**

8. One key issue in Auditing systems is protecting sensitive log information about user activities. Based on the two figures below explain what is achieved by the flows indicated in each figure. [5]



Answer:

9. Elaborate on the ***three*** of the following: [15].

   Goals and/or uses of Auditing

   Intrusion handling activities

   Practical goals of IDS

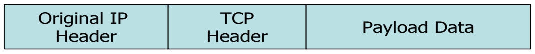
   Defenses against malicious code (virus, worms, etc.)

Answer: **(on the blank side)**

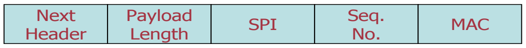
10. Consider an RSA digital signature scheme Alice tricks Bob into signing messages m_1 and m_2 such that $m = m_1 . m_2$ mod n_{Bob}. Prove that Alice can forge Bob's signature on m. [5]

    Answer

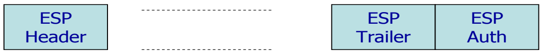
11. Show how the IPSec packets look for the two modes of ESP protocols. [5]



Without IPSec



Authentication Header (AH) Parameter

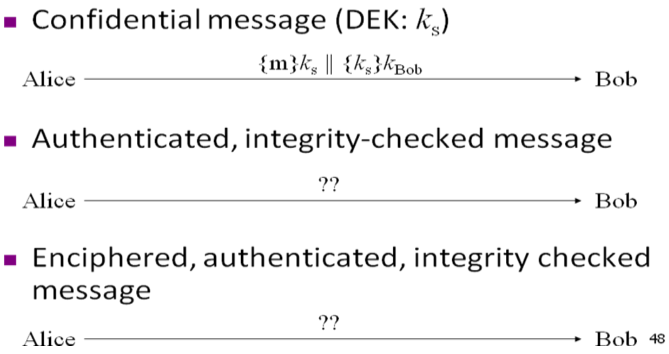


Encapsulating Security Payload (ESP) components

Answer (on the blank side)

12. Recall the *Privacy Enhanced Mail* protocol. Provide the details for the places marked "??". [5]

Answer



- Confidential message (DEK: k_s)

  Alice $\xrightarrow{\{\mathrm{m}\}k_s \,\|\, \{k_s\}k_{\mathrm{Bob}}}$ Bob

- Authenticated, integrity-checked message

  Alice $\xrightarrow{??}$ Bob

- Enciphered, authenticated, integrity checked message

  Alice $\xrightarrow{??}$ Bob 48