IS-2150/TEL-2810 Introduction to Computer Security
Quiz 2
Thursday, Dec 14, 2006

Name:

Email:

Total Time : 1:00 Hour
Total Score : 100

There are three parts. Part I is worth 20 points. Part II is worth 48 points – you need to answer *eight* questions only. Part III is worth 32 points – you need to answer *eight* questions only.

Be precise and clear in your answers

Score

Part 1 (Total: 20)	**Part II (Total: 48)**	**Part III (Total: 32)**

***Good Luck* !**

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

1. [ ] A *secure telnet* session uses *end-to-end encryption*.
2. [ ] *IPSec* can be used to create a *virtual private network*.
3. [ ] *Authentication header* protocol provides support for confidentiality as well as anti-replay service.
4. [ ] *Salting* uses random value to select an *authentication function*.
5. [ ] *Dimilitarized zone* is an intranet and is separated from the internet (or public network) by one firewall.
6. [ ] *Exploratory programming* approach to software development does not provide high assurance, nor does the *formal transformation* approach.
7. [ ] A *multipartite virus* infects *either* boot sectors *or* the executable files *but* not both.
8. [ ] Encrypted virus is aimed towards preventing detection of a virus signature.
9. [ ] *Macro viruses* are *application-independent* and *architecture-dependent*.
10. [ ] Both confidentiality and integrity models can be used to prevent the spread of viruses.
11. [ ] The *penetration testing* approach aims at proving the *absence* of vulnerabilities in a system.
12. [ ] Java is *by design* a safer language than C.
13. [ ] *Speaker recognition* and *speaker verification* techniques refer to *recognition of speaker's voice characteristics* and *verbal information verification*, respectively.
14. [ ] In *IPSec*, if a packet needs to be dropped, it will be indicated in the *Security Association Database*.
15. [ ] The *misuse detection* approach identifies sequences that violate security policies, while the *specification-model* approach detects violation of system specification. This means it is possible that in certain cases, an attack detected by the *misuse detection* approach may not be detected by the *specification modeling* approach.
16. [ ] One use of an *auditing system* is in assessing the damage done by an intrusion.
17. [ ] TOCTTOU is an example of category "*Inconsistent Parameter Validation*."
18. [ ] A *security association* indicates the bi-directional relationship between the peers and specifies the security services provided to the traffic carried on it.

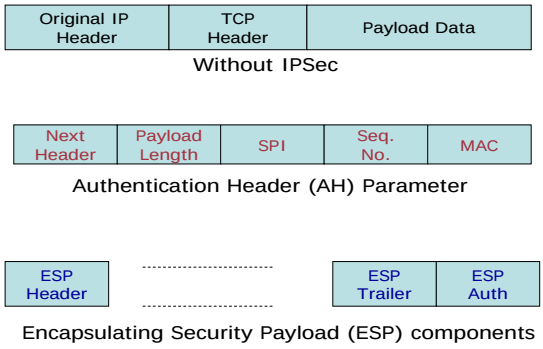
For 19-20, refer to the following protocol used in *Privacy Enhanced Mail.*

$$\text{Alice} \xrightarrow{\{\text{m}\}k_s \,\|\, \{h(\text{m})\}k_{\text{Alice}} \,\|\, \{k_s\}k_{\text{Bob}}} \text{Bob}$$

19. [ ] k_s is the *Interchange Key* and k_{Alice} is a *Data Encipherment Key.*
20. [ ] This protocol provides message *confidentiality* and *integrity*, as well *origin integrity*.

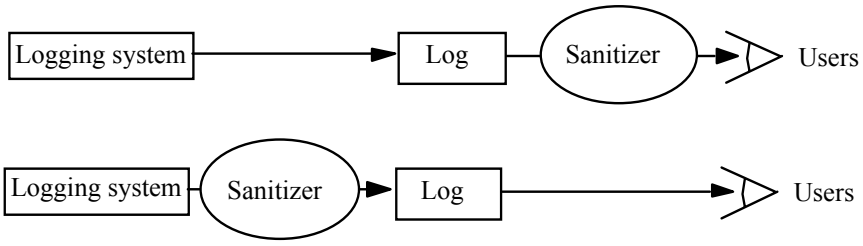
Part II: Answer any *eight* of the following [Score: 8 * 6 = 48]

1. Show how the IPSec packets look for the transport and tunnel modes for both AH and ESP protocols.



Answer

2. Differentiate between the effects of (or the goals achieved by) the following two organizations of auditing systems.



(***provide answer on the back side of the previous page***)

3. What is a *dictionary* attack? Briefly describe and differentiate the two types of *dictionary* attacks. Justify that *salting* makes it difficult to launch dictionary attacks.

Answer

4. For the *S/Key* scheme for password authentication, write the following:
    a. If h is the hash function used, and k the initial seed,
        (i) the n keys, k_1, k_2, .., k_n are generated as follows:

        _____

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

        _____

    b. Explain why this is a good scheme:

    Answer

5. Write briefly on the following issues

    i. Two ways of *detecting* viruses are:

    ii. Two general ways to *defend* against a virus

6. What are the steps involved in the *Flaw Hypothesis* methodology used in Penetration testing approach. Mention what are the drawback(s) of the Penetration testing approach [3]

   Answer

7. Briefly describe the three different approaches to of *intrusion detection* systems and intrusion handling techniques. Briefly differentiate among their capabilities.

   Answer

8. Recall the following example of a Trojan horse [3]
   - *Perpetrator*
     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

   That is, the perpetrator creates a file called ls in *Victim1*'s home directory. When *Victim1* executes the file ls, he will be running a Trojan horse created by the *Perpetrator*.
   (a) Explain what happens when the *Victim1* executes the ls command when he is working in his home directory.
   (b) Suppose *Perpetrator* wants to make sure that once *Victim1* executes the Trojan horse ls, it propagates to *Victim2*. How may he change the above script to achieve it? You can write *pseudo code* and indicate where the additional code needs to be inserted in the script above.

   (***provide answers on the back side of the previous page***)

9. Recall the problem that we discussed in the class regarding the problem with *xterm* program. Note that the following check is done when *xterm* writes to the log_file – i.e., the process checks if the user running the *xterm* program can access the log_file; if yes, then the log_file is opened for writing.

```
if (access("log_file", W_OK) == 0)
        fd = open("log_file", O_WRONLY|O_APPEND)
```

Describe the vulnerability and how someone can exploit it. Suggest a solution for it.

Answer

Part III: Answer any *eight* of the following [8 * 4 = 32]

1. Note that PEM can also provide non-repudiation service. How can non-repudiation service be guaranteed for the PEM protocol in Part I related to statements 19 - 20?

Answer

2. Briefly mention the *four* goals of auditing.

(***provide answers on the back side of the previous page***)

3. Recall that we use constraint p_i: *action* $\Rightarrow$ *condition*. For a system employing the Biba's strict integrity policy, describe what needs to be logged.

   Biba's Model: *Strict Integrity Policy*
   - s **r** $o \Leftrightarrow i(s) \leq i(o)$ (no read-down)
   - s **w** $o \Leftrightarrow i(o) \leq i(s)$ (no write-up)
   - $s1$ **x** $s2 \Leftrightarrow i(s2) \leq i(s1)$

Answer

4. Identify *two* biometric authentication systems and mention possible attacks on them.

Answer

5. Differentiate between the following

   Policy assurance vs. ***Operational assurance***

   Protyping vs ***Extreme programming***

6. What are the three required properties of a *reference validation mechanism*?

Answer

7. Differentiate between the following

   Polymorphic virus vs**. *Stealth virus***

   Trojan Horse vs**. *Virus***

8. NRL taxonomy of software vulnerability includes three schemes. These are:

   1. _____ Example: _____
   2. _____ Example: _____
   3. _____ Example: _____

9. Argue for or against the following statement: *Decrease false positive is more important than decreasing false negatives.*

   Answer