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*.

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

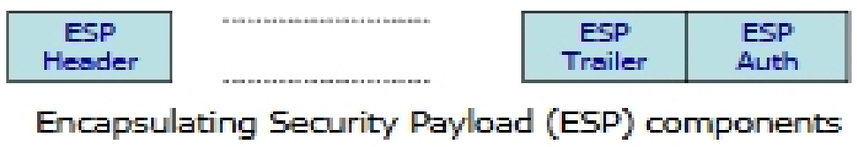
19. [ ] k_s is the *Interchange Key* and k_{Alice} is a *Data Encipherment Key*.
20. [ ] This protocol provides message *confidentiality* and *integrity*, as well *origin integrity*.

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.

Without IPSec

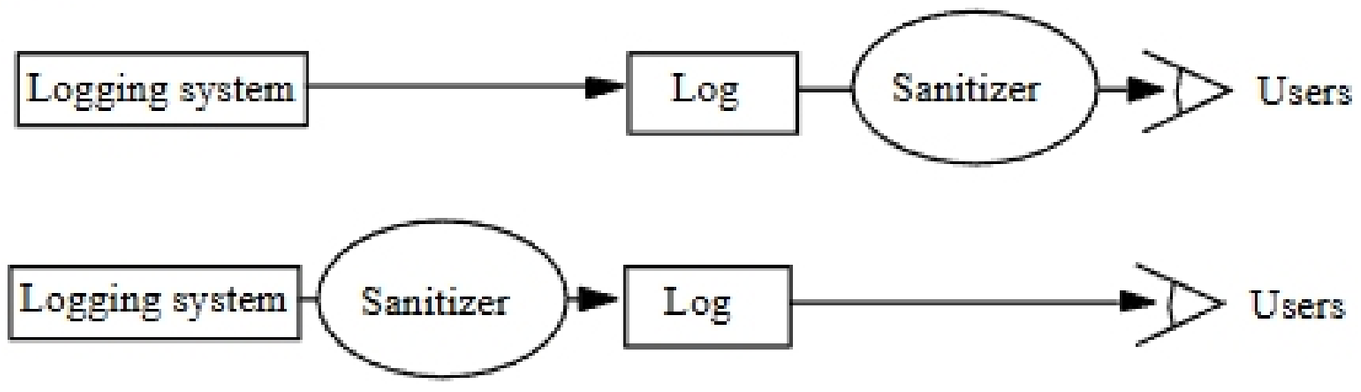
Authentication Header (AH) Parameter



Encapsulating Security Payload (ESP) components

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***)