CS 491/591 Security and Privacy Spring '09 Test 3

Name:_____Key_____

Answer all questions, you have 50 minutes. 100 points total, the number each question is worth is shown in parentheses. **Open book, open notes, <u>closed anything electronic</u>.** Check right now to make sure you have all pages of the test. All of your answers should be written on page 1, I won't grade anything written on pages 2 through 4.

Part I, Circle "T" for True or "F" for False (75 pts., 5 pts. each, see pages 2 and 3 for questions).

1. F	2. T	3. F	4. T*	5. F
6. T	7. F	8. T*	9. F	10. T
11. F	12. T	13. T	14. F	15. T

#4 is debatable and there was some confusion over the wording on #8, if you missed either of these and want your points back see me.

Part II, Multiple choice, circle the <u>one</u> correct answer for the corresponding questions on pages 3 and 4. (21 pts., 7 pts. each).

16. b

17. a

18. b

19. (1 point, True or false) This statement is false. A*ll answers are incorrect.*

20. (2 points): Who proposed the Turing test of information flow in 1991, which models entropy as uncertainty about the mathematical definition of a system? *Randy Browne*

21. (1 point): What is the name of Sepultura's most recent album?

A-Lex

1. (T/F) Dynamic information flow tracking is a solved problem, you can take any program and track its information flow using Fenton's technique without doing any static analysis on the source code.
2. (T/F) Noninterference is a stronger security property than nondeducability, but sometimes realistic systems that are not noninterference-secure are indeed secure because of cryptography, *etc.*, so that nondeducability is more practical.
3. (T/F) In Shannon's theory of information, entropy (or uncertainty) is the opposite of information. The more entropy a channel has, the less information can be transmitted over the channel.
4. (T/F) Kemmerer's shared resource matrix methodology can only be applied to object storage channels, something like Wray's technique is more applicable for channels with timing characteristics.
5. (T/F) "Covert channel" is another term for "implicit flow," they mean the same thing.

For problems 6 through 10, consider the following pseudo-C++ code (note that i and j are references and can be changed by the function, k is a read only argument):

```
void Funkadelic(int &i, int &j, const int k)
{
    int tmp;

    tmp = k + j;
    if (k < 10)
        i = 1;
    else
        i = 0;

    i = i + tmp;
    return i;
}
```

6. (T/F) Information flows from j to i.
7. (T/F) Information flows from k to j.
8. (T/F) Information flows from k to i.
9. (T/F) Information flows from j to i via an implicit flow.
10. (T/F) Information flows from k to i via an implicit flow.

For problems 11 through 15, calculate the transitive closure of the following shared resource matrix and use the matrix to answer the questions:

	Log files	Log buffer	Auth pipe	/etc/passwd lock
Login		M	RM	RM
Mailer daemon		M	***R***	RM
Audit daemon	M	R	***R***	***R***
SSH daemon		M	R	***R***
Web server		M	R	***R***

11. (T/F) Via covert channels, it is possible for the the login program to read the log files.
12. (T/F) Via covert channels, it is possible for the Web server to read the /etc/passwd lock.
13. (T/F) Via covert channels, it is possible for the mailer daemon to read information passed over the authentication pipe.
14. (T/F) Via covert channels, it is possible for processes other than the audit daemon to read the contents of the log buffer.
15. (T/F) Via covert channels, it is possible for the SSH daemon to read the /etc/passwd lock.

16. Who was Matt Bishop's Ph.D. Advisor, who developed much of the terminology we have been learning and did a lot of the early work on static information flow and the lattice model?
    a. Jeffrey Stewart Fenton
    b. Dorothy Denning
    c. Stephanie Forrest
    d. Max Cavalera
    e. Igor Cavelera

17. Who authored the papers “A note on the confinement problem” and “A comment on the confinement problem,” respectively.
    a. Lampson and Lipner
    b. Gogeun and Mesegeur
    c. Cheech and Chong
    d. Kemmerer and Wray
    e. Karger and Wray

18. Which of these best describes Wray's treatment of covert timing channels?
    a. You need two clocks, one of which can be read by the receiver
    b. You need two clocks, one of which can be modulated by the sender
    c. You need two clocks, both of which must be modulated by the sender
    d. You need three clocks, two of which must be modulated by the sender
    e. You need 1/3rd as many clocks as there are storage objects.