CS 491/591 S'09 Homework 2

Due Friday, April 10th before the start of class, either as a hard copy or via e-mail as a PDF or OpenOffice *.odt document (no other format will be accepted). You may send me your answers via email and I'll let you know whether they're correct or not (also must be in *.odt or *.pdf format, not a text file). *These types of questions will be on test 3.* 20 points total.

#1 (5 points)

```
void DoSomething(int w, int x, int &y, int &z);
{
    int temp;

    if (x == 1)
        z = z + 1;
    else
        z = z – 1;

    temp = w + z;
    y = temp;
}
```

Mark these statements as true or false:

- There is an implicit channel from w to y.
- There is an implicit channel from x to z.
- Information flows from x to y.
- Information flows from y to z.
- Information flows from w to z.

#2 (10 points)

Using Kemmerer's Shared Resource Matrix Methodology, fill in the transitive closure of the following matrix (5 points) and answer the questions below (5 points). R = Read and M = Modify.

	File A	File B	File C	File D	Lock 1	Lock 2	Pipe 1	Pipe 2
Alice		R	R,M		R,M			M
Bob	R	R,M					M	R
Cynthia	R							
Darryl	R						R	
Eve	R			R,M	R,M			
Faye				R		R,M		
Gunnar	R					R,M		

- Through a series of covert channels, Eve can read File B. Whose cooperation must she have in order to accomplish this?

- Through a covert channel in which object could this person transmit the information to Eve?

- Which person, via covert channels, can read all but one object in the system (the answer is not Bob, since Bob can only write to pipe 1, not read from it)?

- Is it possible, via covert channels, for Faye to read File B?

- Is it possible, via covert channels, for Gunnar to read Pipe 1?

#3 (2 points)

Which of these best describes, in terms of Wray's definition of timing channels, the following timing channel? The timing channel is one in which the sender sends a 1 by making many hard drive requests within a given time period (therefore adding a lot of entropy to the entropy pool), and a 0 by not doing so during the time period, while the receiver receives information by timing the periods of time in which /dev/random blocks. Both sender and receiver use the system clock for timing purposes.

a. The system clock can be modulated by the sender and read by the receiver, and both sender and receiver can modulate the timing of the completions of hard drive requests.

b. The hard drive completion times are modulated by the sender and read directly by the receiver, there is only this one “clock” involved.

c. The system clock is readable by both the sender and the receiver, and the blocking of the entropy pool can be viewed as a “clock” that can be modulated by the sender and read by the receiver.

d. The receiver modulates the system clock while the sender modulates the blocking of the entropy pool.

#4 (3 points)

Someone tells you that they have built a security extension to the Pentium architecture that will enforce a fine-grained confidentiality policy on the entire system, even for commodity applications without access to the source code or any need for recompilation or static analysis. They claim to have basically implemented Fenton's data mark machine concept on the Pentium architecture. Give three specific and meaningful reasons why they are probably full of %$@#. (Note: my grading on this question will emphasize specific and meaningful, so try to list three major problems with the claim that are indisputable).