Summary
Secure program execution via Dynamic information flow tracking
Venkatesan Packirisamy
February 14, 2005

1 To be completed before class

What are the problems solved by this paper? (50 words)
Malicious attacks on programs are becoming common. The most common way to attack is to make the program control to branch to malicious code which was not supposed to be executed. The programs and the data that is part of the program are usually authentic (unless there is a back door). The problem comes only in the input. A attacker can tailor his input to the program in such a way to force a control transfer to his malicious code. And the attacker can do anything in his code. This is how many viruses and worms are launched. Since there can be a huge loss of money and time due to such attacks, tackling them is very important.

What are the approaches attempted by this paper? (50 words)
There are many ways to prevent such malicious control transfer. In this paper, the OS identifies a input channel as spurious. The architecture will keep track of the data got through these spurious channels. If this data is used to calculate someother value or to do someother execution, the result of such execution is also tagged as spurious. And if the control transfer is done to such spurious address value or if the instruction executed is itself is a spurious location, then an exception is raised. By this the user can never tailor his input to transfer control to his code.

What are the main conclusions of this paper? (50 words)
There has been many techniques that have been proposed to solve this problem, but the one proposed in this paper is widely applicable. Also it has very negligible overhead. For example the first policy caused a performance degradation of 0.02%. The modifications necessary to implement the technique is also very less. The same technique can also be used to implement other security policies like data integrity.

2 To be completed after class

Did this paper address an important issue? Explain. (100 words)

Are the proposed approaches valid? Describe its strength and weakness. (100 words)

Do the results support the conclusions? Explain. (100 words)
Describe the potential future works? (100 words)