Summary
Secure Program Execution via Dynamic Information Flow Tracking

Kiran Yellajyosula
February 14, 2005

1 To be completed before class

What are the problems solved by this paper? (50 words)
Malicious attacks exploit program bugs to obtain root privileges on a system by either manipulating data that can be used to inject instructions or modify jump addresses. The processor then executes these spurious instructions that may produce other data which might result in a control transfer. The operating system can usually identify these sources of spurious input and take necessary precautions.

What are the approaches attempted by this paper? (50 words)
The authors propose to use the OS to identify the spurious input channels and propose a hardware mechanism called dynamic information flow to identify spurious information flow and restrict their usage. The authors propose to introduce various hardware structures to store the security tags of the data contained in the processors and explain how spurious information flow is tracked and restricted by the OS. The authors propose two security schemes and simulate them using simplescalar.

What are the main conclusions of this paper? (50 words)
The dynamic information flow technique detects the flow of spurious data and can prevent security attacks from taking control of vulnerable programs. Experimental results obtained from the simulation show that the approach is effective in detecting and protecting the system from a variety of security attacks. The mechanism doesn’t effect the performance of the L2 cache significantly.

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)