Summary
Hide: An infrastructer for Efficiently Protecting Information Leakage on the Address Bus.
Kiran Yellajyosula
April 11, 2005

1 To be completed before class

What are the problems solved by this paper? (50 words)
Inspite of employing various encryption techniques as in XOM, information can be leaked by tracking the addresses on the address bus. The CFG of a program can reveal about 80-90% of a program code due to software reuse and legacy softwares. Some accesses can even reveal secret information about the software and make the encrypting useless.

What are the approaches attempted by this paper? (50 words)
The authors propose to permute every memory location in the address space before it is accessed twice, thereby ensuring that the same address is not repeated twice on the address bus. The authors propose a Hide cache with a fetch queue and a permutation unit which does pre-permutation so as to remove the permutation from the critical path of execution.

What are the main conclusions of this paper? (50 words)
Using Chunks of size equal to a few pages reduces the overhead and the amount of permutations to be performed. Employing compiler guided layout optimizations for code and data further enhances the performance and security of the program. Information loss is prevented upto around 95% by employing Hide caches.

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)