Summary
HIDE: An Infrastructure for Efficiently Protecting Information Leakage on the Address Bus

Venkatesan Packirisamy
April 11, 2005

1 To be completed before class

What are the problems solved by this paper? (50 words)
Software piracy is a huge issue at present. XOM architecture proposed a way to have hardware support for copy and tamper proof software. But XOM cannot guarantee against information leakage via address bus. Though industry and academia does recognize the problem of protecting address bus, it is very hard because of the high overhead.

What are the approaches attempted by this paper? (50 words)
This paper proposes an infrastructure called HIDE - Hardware-support for leakage-Immune Dynamic Execution. They support chunk level protection of addresses with hardware support. A chunk is defined as one or more pages that are protected and permuted together. Different layers of security is built. Also the HIDE provides an application interface to control the protection mechanism.

What are the main conclusions of this paper? (50 words)
HIDE is able to be guarantee address bus protection that was lacking in XOM. The results show that HIDE guarantee 87% of the address sequence is protected and in which 95% of the accesses to code and static data are hidden. The performance overhead is atmost 1.5% in most cases. Also since HIDE provides a good interface, it makes the protection mechanism more flexible.

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)