Summary
Architectural Support for Copy and Tamper Resistant Software
Venkatesan Packirisamy
February 14, 2005

1 To be completed before class

What are the problems solved by this paper? (50 words)
In the year 1998 software industry had lost 11 billion dollars according to the business software alliance. Software piracy can be handled at various levels. But whatever may be the external restrictions, once we run the program in a machine without protection, some other person can run another task in the same machine and access our code and data. So protection is an issue even while executing the program.

What are the approaches attempted by this paper? (50 words)
This paper uses cryptographic techniques to prevent the program code and data values from being read by someone not authorized. In the XOM machine (execute only memory) the user can only execute the code but he can never read it. The XOM machine has a private key which authorizes it to read the program. Using the private key, the machine decrypts the session key of the program and uses it to protect the program. All instructions and data are stored in an encrypted fashion, so if the machine wants to execute an instruction, it first decodes the instruction using its key. And while storing the value also it stores the encrypted value. Thus the machine with the help of encryption techniques is able to protect the instructions and data.

What are the main conclusions of this paper? (50 words)
Preventing the user from reading the code while allowing to execute or copy the code is a challenging problem. The paper solves this problem using the compartments of the XOM machine while incurring modest overhead. The major overhead is the adding of tags to the on-chip cache. The paper uses asymmetric cryptographic algorithms ensuring complete protection of the software.

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)