Abstract

Spyware is considered as a great threat to confidentiality that it can cause loss of control over private data for computer users. This kind of threat might select some data and send it to another third party without the consent of the user. Spyware detection techniques have been presented traditionally by three approaches; signature, behavior and specification based detection techniques. These approaches were successful in detecting known spyware but it suffers from some drawbacks such as; the need for updating data describing the system behavior to detect new or unknown spywares, and the high level of false positive or false negative rate. Therefore, in this paper we introduce a proposed anti spyware system design and implementation using design patterns for detecting and classifying spyware. This proposed approach can be reusable and modifying itself for any new or unknown spyware.


12. E. Gamma, R. Helm, R. Johnson, and J. Vlissides, Design Patterns: Elements of Reusable Object-Oriented Software, Boston, Massachusetts, Addison-Wesley Longman Publishing Co., Inc., USA, 1995.


Index Terms

Computer Science  Security
Keywords

Spyware, Design patterns