Abstract

Spyware is somewhat of a silent killer, because its essential task is secretly and quietly monitoring or sending victim's sensitive information to a separate third party. Unfortunately, existing anti-spyware systems lack the ability to cope with the rapid changes in the spyware signatures and programs.

The main challenge in recent anti-spyware systems is to design efficient system that able to detect new and unknown spywares in a reasonable time. Furthermore, lack of interest in existing anti-spyware systems reusability. This paper introduces an adaptive anti-spyware system that able to deal with unpredictable discovered spywares on run time and improves the detection accuracy. The proposed system adopts design patterns approach in detecting and classifying spyware, in the sense that, reuse existing systems components in detecting new or unknown spywares without performing changes on these systems' designs. The proposed
anti-spyware system can be considered as an engineering product that needs to be verified in terms of performance and maintainability. The aim here is to guarantee the performance of the designed system by defining evaluation methods for assessing the performance and maintainability of this design. Thus, the performance of the proposed system has been evaluated through the adopted data mining evaluation metrics. While, amount of reuse and reusability metrics have been defined to evaluate the proposed system maintainability.

References

6. 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.
14. Mohamed Adel Sheta, Mohamed Zaki, Kamel AbdEl Salam El Hadad, and H.


Index Terms

Computer Science Information Sciences

Keywords

Spyware, Data mining, Design patterns.