Abstract

Nowadays information systems are very critical and important as their various users are distributed around the world. The role played by the information system in the evolution of the society has led to a new form of economy, the leaders in this economy are those who will be able to master their information system in terms of security issues. Based on the quality of data managed in the information system for decision making, the security issue becomes more and more crucial. Among the challenges that are faced in the information system, it appears that the intrusion detection problem is the major challenge that needs to be discussed first as all attacks start with the intrusion which precedes various malicious activities. Many works had been done in this domain but the intrusion detection problem is still an open research topic in computer science. In this paper, the described problem is considered as an engineering one.
The approach used in this research is based on the workflow theory which allows carrying out an efficient identification in different activities that are able to be performed. The defined approach is focused on a formal and sound description of resources that participate in the execution of identified activities. The result of this paper is the definition of a formal framework for intrusion detection based on workflow execution analysis.

References

Index Terms

Computer Science  
Security

Keywords

Intrusion detection model  
Workflow execution audit  
Information system audit  
Activity categorization