Abstract

Web applications are the most universal way to make services and data accessible on the Internet. With the increase in the use of these applications, there has also been an increase in the amount and complexity of vulnerabilities and attacks. These attacks target directly the back-end database systems of the web application to achieve information. In this paper, a Dual Safeguard Intrusion Detection and Prevention System was proposed to models the user network behaviors and create normality models of isolated user sessions across both front-end and back-end of the application. To accomplish this, a Lightweight virtualization technique is used to allocate each user’s web session to a dedicated container, providing an isolated virtual computing environment. An Intrusion Detection Model for web applications based on Hidden Markov Model was also proposed.
Dual Safeguard: Intrusion Detection and Prevention System in Web Applications

References


Index Terms

Computer Science

Security
Keywords
IDS  Multitier web application  Normality model  Hidden Markov Model  Container Virtualization