عنوان مقاله:

A Cooperative GPU-Based Approach for Alert Aggregation

محل انتشار:

مجله بین المللی کامپیوتر و فناوری اطلاعات, دوره 2, شماره 2 (سال: 1393)

تعداد صفحات اصل مقاله: 10

نویسندگان:

Masoud Narimani Zaman Abadi - *IT Security Institute, ICT Department MalekAshtar University of Technology, Tehran*

Alireza Nowroozi - *IT Security Institute, ICT Department MalekAshtar University of Technology, Tehran*

Payam Mahdinia - *Electrical and Computer Engineering Department Isfahan University of Technology*

خلاصه مقاله:

Alert aggregation classified as a similarity-based alert correlation which fuses and clusters similar alerts. Alert aggregation increases meaning of alerts and reduces incoming alerts simultaneously; this process requires lots of computing resources. Limitation of computing resources, like CPUs, makes such systems not satisfactory. Graphic processing units (GPUs) are a potential option to solve this. In recent years, GPUs have been used in various fields, however, due to the dynamic nature of processing and data structures in alert correlation, correlation algorithms have not been implemented on GPU. In this paper, we present a cooperative model that uses the processing power of graphics processing unit (GPU) to aggregate security alerts and transform the time complexity from the second power to the linear one. Evaluations illustrate the proposed method for 600,000 alerts in time window will improve the processing speed by 26 times. In the proposed algorithm, in spite of main algorithm, the system performance at best, average and worst cases are the same

کلمات کلیدی:

Alert aggregation, alert correlation, security alert, graphics processor, time window