

Autonomic Defense System

by Youssif Al-Nashif

Recently, the need for an efficient cyber defense system has become extremely critical. The Internet is pervading almost every aspect of life and business, and along with this exponential growth comes the critical need to secure these systems from unauthorized disclosure, transfer, modification, or destruction is vital. The increase in the number of attacks and their complexity is due to an increase in the number of applications with vulnerabilities and the number of attackers equipped with fast networks and processing units. Cyber attacks are growing increasingly in complexity and sophistication.

Complex attacks present a significant threat to the security of information infrastructure and can lead to catastrophic results. Attacks typically exploit vulnerabilities in networks, system software, and protocols. For example, some attacks misuse network resources' limitations, protocol vulnerabilities, or application vulnerability to reach their goals. Furthermore, these attacks vary in their speed, complexity, and dynamicity.

We are designing and implementing a multilevel anomaly-based Autonomic Defense System (ADS), which is capable of detecting any type of attacks targeting resources, with low false alerts and high detection rates. The main concept behind the ADS is the zooming in to the correct level of granularity to analyze cyber behaviors. Once the zooming is locked to the correct level of granularity, the cyberspace is monitored, the process of selecting the correct features to improve detection is applied, and then aggregation and correlation is used to reduce the number of analyzed records with minimum loss in information. After that the anomaly based detection technique is used to detect abnormal behavior in the cyberspace. Once an abnormal behavior is detected, the risk and impact analysis process is triggered to recommend the best set of actions to be applied with minimum loss in cyber operation functionality. Finally, the recommended set of actions are either applied automatically or prompted for administrator confirmation in the visualization and management console.

