ICARFAD: A Novel Framework for Improved Network Security Situation Awareness

Volume 87 - Number 19

Year of Publication: 2014

Authors:
Chanchal Sharma
Vandana Kate

10.5120/15461-4064

Abstract

Networking components and technologies is continuously proving their presence in various core areas of business like IT, Health Care, Stocks, and Emergencies with Military systems. It is possible by applying multiple system phenomenons of compatibility, interoperability and integration of different categories of devices and users. As the usage of information is increasing the transaction and data security needs to be provided effectively. It will serve as a critical and important task which assures data protection. This unexpected and frequent changes in the system is measured which gives a direction of vulnerable behaviour and the criticality of affecting the process. Accessing this information through actual network conditions and changes for improving the security is comes under the area of situational awareness system. This work proposes a novel ICARFAD (Information Collection, Assessment and Response, Feedback and Alerts Decisions) based situation awareness mechanism which gathers current network condition and clearly defines the boundaries by which security solutions can be designed effectively. It reflects all the changes made in configurations and methods taken as a security measures by maintaining a database which later on used to make the decisions for network security improvements. It also makes the visualization of attack conditions by making the graphs and plots which greatly improves the rate and the quality measures of persons or machines decision making.
ICARFAD: A Novel Framework for Improved Network Security Situation Awareness

References

- Bon K. Sy, "Integrating intrusion alert information to aid forensic explanation: An
ICARFAD: A Novel Framework for Improved Network Security Situation Awareness


Index Terms

Computer Science
Security

Keywords

Attack Graphs  Situational Metrics ICARFAD (Information Collection Assessment and Response Feedback and Alerts Decisions);